UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

El ciberespacio, la ciberguerra y los desafíos jurídicos y tecnológicos para el Derecho Internacional

T E S I S

QUE PARA OBTENER EL TÍTULO DE

LICENCIADA EN RELACIONES INTERNACIONALES

P R E S E N T A:

JESSICA GONZÁLEZ HERNÁNDEZ

ASESORA:

MTRA. EVELYN TÉLLEZ CARVAJAL

CIUDAD DE MÉXICO 2020

Índice

El ciberespacio, la ciberguerra y los desafíos jurídicos y tecnológicos para el Derecho Internacional

Jessica González Hernández

Asesora: Mtra. Evelyn Téllez Carvajal

Introducción

El sistema internacional sufre cambios continuos gracias al contexto internacional que, igualmente, está en constantes transformaciones y es quien dirige el accionar de los actores pertenecientes a dicho sistema.

Asimismo, los fenómenos emergen conforme a la transformación progresiva del contexto internacional, como la guerra, aunque ésta no emerge, si no que se presenta en distintas formas de acuerdo a lo que ocurra en dicho contexto, pues se adapta a éste en cuanto a la forma de hacerla y su desarrollo.

Un ejemplo de esto último descrito, es la ciberguerra como una nueva forma bélica que se da entre Estados desde hace unos años solo que en un contexto actual y en un escenario más contemporáneo e influyente como lo es el ciberespacio.

Es por ello que los Estados formulan nuevas herramientas que se adapten a las transformaciones cibernéticas, para con ello adquirir ventajas competitivas por sobre los demás actores, y también, para poder participar de manera firme en las actividades equiparables a la guerra en el espacio cibernético.

De igual manera, se han puesto en marcha estrategias que fomentan la prevención, la disuasión y, en algunos casos, la erradicación de la ciberguerra, pues la idea principal es su búsqueda para evitarla y, en su defecto, afrontarla.

No obstante, todo lo anterior ha dado lugar a grandes vacíos jurídicos, puesto que no existe una normativa internacional homogénea y vinculante con relación a la ciberguerra.

A pesar de que existan tratados, normativas regionales y/o locales, estrategias internas y externas, etc. orquestadas por los propios Estados para afrontar la guerra cibernética no se ha dado pie a una iniciativa integral internacional del tema debido a la intervención con los intereses de los Estados, así como la falta de armonización con sus normas, estrategias y tratados en los que participan.

La presente investigación brindará un análisis de lo anteriormente mencionado, pues su importancia descansa en analizar los constantes retos que enfrenta el Derecho Internacional dentro del ciberespacio para regular los conflictos emergentes del desarrollo tecnológico de la época, como lo es el caso de la ciberguerra, pues dicho espacio no cuenta con una rama del derecho internacional que permita mitigar los efectos derivados de la guerra cibernética.

Se busca desarrollar una investigación concreta respecto a la situación de los Estados que están en constante enfrentamiento cibernético, llevando a la ciberguerra a interferir de manera directa en el plano internacional.

Es así como el objetivo principal de esta investigación es analizar los desafíos para el Derecho Internacional en la creación de una regulación jurídica ante los ataques cibernéticos dentro de los conflictos entre Estados, que se le denomina como ciberguerra. Objetivo que se sustenta de aspectos específicos, los cuales consisten en analizar la concepción referida a la ciberguerra; identificar el ciberespacio como escenario para las operaciones de ciberguerra; explicar el papel de los ciberejércitos en la ciberguerra; reconocer el derecho internacional aplicable a la regulación dentro del ciberespacio y la ciberguerra; y finalmente exponer los desafíos del derecho internacional para la creación de una regulación jurídica ante los ataques cibernéticos dentro de los conflictos entre Estados, todo ello presentando casos de uso para ejemplificar lo presentado.

El capítulo 1 analiza la parte conceptual que el ciberespacio engloba, para así dar pie al análisis de las problemáticas que conlleva el Derecho respecto a los conflictos emergentes como la ciberguerra. La finalidad de dar a conocer la concepción de algunas cuestiones que se albergan en el espacio cibernético, así como algunas referentes a la guerra convencional, derecho de guerra, entre otros, es para comprender el escenario y el contexto jurídico-tecnológico para llevar a cabo acciones que integran la ciberguerra.

En el capítulo 2 se expone la convertibilidad de ciberespacio como escenario para el desarrollo de la ciberguerra. De igual forma, se presenta una perspectiva de los actores de ésta, así como el papel que tienen los ciberjércitos, y las herramientas utilizadas para realizar ciberataques como componentes sustanciales para llevar a cabo las acciones bélicas. Todo ello para mostrar el impacto jurídico, tecnológico y social que se da gracias a la ciberguerra, así como también las implicaciones jurídicas que contrarrestar el sistema internacional para atenuar tales efectos.

Por su parte, el capítulo 3 enfoca un análisis del marco jurídico regulatorio internacional en el ciberespacio, que se presenta para explicar la regulación de la ciberguerra con los desafíos jurídicos que existen para la aplicabilidad de una legislación internacional unificada y de carácter obligatorio en el tema.

En el capítulo 4 se estudia por qué los Estados utilizan la tecnología como una herramienta de adaptación en el ciberespacio como escenario para hacer la guerra. Asimismo, se presentan distintos casos de ciberguerra de México, Estados Unidos, Francia y Reino Unido como ejmeplos de países que se encuentran en ciberguerra o están en guerra latente. Aunado a ello, se dan a conocer las distintas estrategias que dichos países han dado lugar para confrontar la ciberguerra, tanto en lo regional internacional, como en lo internacional, mismas que figuran como cimientos para que junto con la legislación que se ha dado en relación a la guerra cibernética se de la iniciativa para crear una normativa internacional para regular las actividades equiparables a la guerra cibernética.

La importancia de abordar el tema *El ciberespacio, la ciberguerra y los desafíos jurídicos y tecnológicos para el Derecho Internacional*, desarrollado en los capítulos mencionados con anterioridad, desde la perspectiva de las relaciones internacionales recae en que la ciberguerra tiene incidencia directa hacia lo intereses nacionales de los Estados, por ello, éstos tienen mayor interés y necesidad de proteger las actividades cibernéticas que tengan relación con ataques para consumar el accionar bélico y la confrontación de los conflictos entre los Estados, y solo la creación de normas objetivas relativas al ciberespacio.

CAPÍTULO 1. Conceptos sobre ciberespacio y la ciberguerra

La nueva organización política y social basada en la tecnología, ha modificado la forma en que se realizan las comunicaciones, lo que ha provocado, incluso, la generación de nuevos espacios, como es el denominado ciberespacio, en donde se ha dado lugar a cambios que envuelven los medios digitales y herramientas tecnológicas.

Las nuevas tecnologías de la información, han transformado el orden social, ya que suponen una reaparición entre las relaciones existentes de la sociedad, la tecnología y la informática. De este modo, la organización social comienza a verse sometida ante la nueva realidad cibernética, por lo que se comienzan a hacer presentes nuevas comunidades, mismas que se reflejan dentro de las nuevas formaciones sociales, surgiendo, lo que se hace llamar cibersociedad.

La cibersociedad consiste en "una sociedad basada en la información y el conocimiento gestionados por las nuevas tecnologías. Tecnologías que se aplican sobre el conocimiento y no al revés como en las anteriores revoluciones científicas"[1].

Esta nueva sociedad que está inmersa dentro del entorno tecnológico es parte de las transformaciones que de ello proviene, puesto que al adaptarse a éste, creando nuevas estructuras sociales que pretenden liderar los cambios en el nuevo contexto. Además, se considera a la información como un punto de partida para lo anteriormente mencionado, ó sea que la información es el fundamento principal de ésta, debido a que la considera un recurso y la base del desarrollo actual.

Por su parte, los conflictos armados se han posicionado dentro de las relaciones internacionales como una forma para el arreglo de las controversias que no se pudieron solucionar haciendo uso de los medios pacíficos dando paso a la solución de controversias por medio del ordenamiento jurídico que rige a la guerra.

No obstante, con los avances científicos y tecnológicos ha habido cambios en la guerra tanto en el modo de hacerla, como sus modalidades, la posición de los actores y los instrumentos que se utilizan.

---

[1] Fernández, Jesús; Molina, David, *Cibersociedad y ciencias humanas: el caso de la Historia Actual,* [en línea], Argentina, Instituto Argentino para el desarrollo económico, Dirección URL: http://www.iade.org.ar/noticias/cibersociedad-y-ciencias-humanas-el-caso-de-la-historia-actual-0, [consulta: 25 de abril de 2018].

Incluso, el entorno se ha modificado, por lo que las problemáticas bélicas han migrado a estos nuevos espacios, tal como lo es el ciberespacio, mismo que más allá de crear un ambiente moderno, desconocido e inédito, forja una transformación contextual que lleva a una evolución del sistema político, económico, tecnológico y social. Asimismo, es indispensable contemplar todos los elementos que lo engloban, ya que para que se pueda comprender los desafíos a los que se enfrenta, principalmente jurídicos y tecnológicos, es necesario destacar cada componente.

A continuación se abordará de manera conceptual lo que el ciberespacio conlleva para de esta manera analizar la problemática que enfrenta el Derecho en los nuevos conflictos emergentes, puesto que el ciberespacio al ser el escenario para llevar a cabo las acciones que comprenden la ciberguerra, es un lugar con confusa aplicabilidad de una jurisdicción determinada.

1.1. El ciberespacio y los conceptos de soberanía y jurisdicción

El ciberespacio es un entorno virtual sin delimitación geográfica respecto a su alcance. Su concepto fue acuñado por el escritor de ciencia ficción William Gibson, pues creó la idea en su novela llamada Neuromante publicada en 1984, en donde lo definió como *"*el escenario espacial que existía al interior de las computadoras y sus interconexiones, espacio en el cual existen seres ficticios (ciborgs) y el tiempo es algo manipulable*"*[2].

A Gibson se le atribuye la creación del concepto, no obstante, a lo largo del tiempo el ciberespacio ha tenido distintas visiones que se van adaptando y transformando a través del tiempo, por lo que se han dado lugar distintas concepciones.

En la obra *Ciberespacio para principiantes,* se define como "una combinación fortuita y oportuna de tecnologías de información, almacenamiento, y recuperación con las de telecomunicación global"[3], por lo que esta definición describe más el contenido de una computadora, que un espacio en el que se desarrollan actividades cibernéticas, y esto se debe al año en el que fue escrita la obra.

---

[2] Cabrera Mendoza, Elizabeth; y Valdés Godines, Juan Carlos, "Ciberespacio y cibersociedad, su relación con las formas alternativas de socialización para la apropiación social de las TIC´s", Revista Iberoamericana para la Investigación y el Desarrollo Educativo, núm. 10, enero-junio, 2013, [en línea], México, Ride, 2013, Dirección URL: http://ride.org.mx/1-11/index.php/RIDESECUNDARIO/article/viewFile/564/553, [consulta: 16 de diciembre de 2018], p. 3.

[3] Buick, Joanna; Jevtic, Zoran, *Ciberespacio para principiantes,* Argentina, Era Naciente, 2002, p.8.

Por el tiempo en el que fueron escritas las referencias anteriores, se puede incluir la que tiene Pierre Lévy en su obra *¿Qué es lo virtual?,* donde dice que el ciberespacio "designa el universo de redes digitales como un mundo de interacción y aventura, es el espacio de conflictos globales y una nueva frontera económica y cultural"[4]*.* Por lo que de esta manera más allá de hablar de un espacio en donde interactúan las sociedades, lo predetermina como un lugar en el que los conflictos se sitúan por la naturaleza económica, política y cultural que representa.

María del Pilar Llorens en su obra, nos habla de que el ciberespacio hace referencia a la superficie o ambiente compuesto por elementos no físicos, en el que se desenvuelve la red informática la cual está conformada por las conexiones que existen entre todo lo que se realiza dentro de este espacio mediante redes, sistemas y equipos digitales[5].

Joseph Nye, por su parte, enfoca su definición en la electrónica como la base para explotar toda la información posible mediante sistemas interconectados y la infraestructura que el ciberespacio brinda[6]. Además, complementa esta concepción en la terminología de poder, pues considera que los recursos de información son los que en la nueva era tecnológica conceden dominio.

Por otro lado, existe una idea referente al ciberespacio que tiene concordancia con la comunicación que se da en las relaciones entre personas, pues Iván Galvani describe que el internet "nos ofrece un lugar y un tiempo (llamados virtuales) para relacionarnos con los demás, que se denomina "ciberespacio"[7]*,* tomando en cuenta una extensión que se limita no por una dimensión en especifico, si no por las relaciones que se desarrollan dentro de éste, por lo que existe un sentido más humano y social dentro de ésta percepción, que se asocia con la concepción presentada por Gibson.

El Dr. Rafael De Gasperin elaboró una noción del concepto con una comparación respecto al internet, y menciona que, "El ciberespacio es un término vulgar de dominio

---

[4] Levy, Pierre, *¿Qué es lo virtual?,* Barcelona, Paidos Iberica, 1999, p. 22.
[5] Llorens, María del Pilar, "Los desafíos del uso de la fuerza en el ciberespacio", [en línea], México, Instituto de Investigaciones Jurídicas-UNAM, 2017, Dirección URL: https://revistas.juridicas.unam.mx/index.php/derecho-internacional/article/viewFile/11052/13078, [consulta: 26 de noviembre de 2018], p. 787.
[6] Nye, Joseph, *Cyber* Power, United States, Belfer Center for Science and International Affairs, 2010, p. 3.
[7] Galvani, Iván*, La vida cotidiana en el ciberespacio,* Argentina, Universidad Nacional de La Plata, p. 1.

común entre los cirbernautas, esto es, entre las personas que hacen uso de la red de redes sin un conocimiento técnico de la misma. El ciberespacio y la Internet no son lo mismo. Internet es la infraestructura y el ciberespacio es el contenido.

Generalmente los usuarios también forman parte del contenido a través del correo electrónico, la web, los newsgroups, las listas, el Gopher, etcétera. El ciberespacio es generalmente multiusuario aunque no siempre lo es en tiempo real"[8].

De esta manera, Gasperin toca un punto fundamental, acerca de la diferencia que se debe hacer entre el ciberespacio y el internet, distinción que varía de la concepción del tema que tienen diferentes autores.

Debido al papel que está tomando el ciberespacio en el contexto internacional actual, la OTAN lo ha declarado como un territorio al que se le debe poner una atención especial, por lo que declararon que:

"Allies recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. This will enable NATO's military structures to devote specific attention to protecting missions and operations from cyber threats and increase their focus on cyber-related training and military planning for operations conducted in a contested and degraded cyber environment. It will also allow for the streamlining of cyber defense into operations across the other domains of air, land and sea and for achieving joint operational effects"[9].

El ciberespacio al ser declarado como territorio comienza a tener cierto peso respecto a terminaciones como soberanía y jurisdicción. Por lo tanto, es forzoso determinar como la soberanía va a jugar un papel importante dentro del ciberespacio respecto a la aplicabilidad del derecho para regular las actividades de los Estados dentro éste.

El término soberanía se encuentra presente en todos los sistemas jurídicos existentes del mundo, empero, definirlo es complejo, debido a que se encuentran distintas ideas respecto a éste, por lo que a continuación se presentarán algunas definiciones que podrán apoyar en la investigación presente.

---

[8] Gasperin, Rafael, *Adolescencia y ciberespacio,* [en línea], Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura, 2005, Dirección URL: https://www.oei.es/historico/valores2/monografias/monografia05/reflexion04.htm, [consulta: 18 de marzo de 2019].

[9] NATO, *Anual Report 2016,* Bélgica, NATO, 2016, p.24.

Jean Bodin dice que la soberanía es "*el poder absoluto y perpetuo de una republica*"[10]. Con ello el autor de *Los seis libros de la Republica*, habla de la soberanía como una cualidad que debe tener la República, misma que es tomada como un conjunto de familias que tiene poder soberano[11], todo ello basado en un monarca que se encuentra al frente. Pese al tiempo es la definición más acertada y aceptada del término, aunque carece de actualización ya que se centra en la República, pero no existe una explicación de quién es el poseedor del poder, ni de dónde surge y mucho menos quien lo ejecutará.

Por otro lado, se encuentra la siguiente determinación del concepto,

"se refiere al ejercicio de la autoridad en un cierto territorio. Esta autoridad recae en el pueblo, aunque la gente no realiza un ejercicio directo de la misma sino que delega dicho poder en sus representantes. La Soberanía significa independencia, es decir, un poder con competencia total"[12]. En dicha idea ya se plantea la determinación de un territorio, en donde se lleve a cabo el ejercicio de poder dentro de éste, el cual le va a brindar autonomía por sobre la demarcación.

La noción que se tiene de soberanía es aplicable para un territorio que está designado, empero, es difícil comprender el alcance que tiene el poder bajo las condiciones de la soberanía respecto al ciberespacio, es por ello que surge la percepción reciente de la cibersoberanía o soberanía cibernética que es concebida como "el derecho de los Estados a controlar Internet dentro de sus fronteras"[13].

Al conceptualizar de esta manera al dominio cibernético se entra en un conjunto de contradicciones entre las que destaca, en principio, el control del internet, siendo que éste último no es en el que se engloba el contenido del ciberespacio, como se mencionó con las definiciones presentadas con anterioridad; en segundo lugar, se encuentra la idea de control en el territorio de los Estados, retornando al planteamiento que en el ciberespacio no existe un área delimitada para ejercer autoridad.

---

[10] Bodin, Jean, *De la soberanía* en *Los seis libros de la Republica,* Madrid, Tecnos, 1997, tercera edición, p.47.
[11] *Ídem*.
[12] s/a, *Soberanía,* [en línea], Sistema de Información Legislativa, Dirección URL: http://sil.gobernacion.gob.mx/Glosario/definicionpop.php?ID=229, [consulta: 19 de abril de 2018].
[13] Mallol, Eugenio, *La era de la cibersoberanía*, [en línea], El Mundo, 18 de diciembre de 2017, Dirección URL: https://www.elmundo.es/economia/2017/12/11/5a2e6c3546163f552d8b4642.html, [consulta: 19 de abril de 2019].

Con lo anterior, el concepto de jurisdicción toma relevancia, ya que la aplicabilidad del derecho en el ciberespacio depende de la soberanía dentro de éste, que como se mencionó no está delimitada, así como de la jurisdicción que tiene como objetivo llevarse a cabo en dicho espacio, pero que resulta complejo debido a tal falta de delimitación territorial.

De esta forma, es sustancial definir jurisdicción, ya que de ello deriva que el derecho sea aplicable. De acuerdo a la Real Academia Española, define en su diccionario el concepto como el "poder o autoridad que tiene alguien para gobernar o poner en ejecución las leyes o para aplicarlas en un juicio"[14].

La idea anterior es bastante general, puesto que únicamente se enfoca en alguien para gobernar, por lo que es conveniente citar la definición que presenta la Suprema Corte de Justicia de la Nación de los Estados Unidos Mexicanos, en la tesis *Jurisdicción y competencia,* en donde se define lo siguiente:

"La jurisdicción es la potestad del Estado convertido en autoridad para impartir justicia, por medio de los tribunales que son sus órganos jurisdiccionales, pero esa administración de justicia comprende actividades muy diversas, por lo que ha habido necesidad de hacer una clasificación atendiendo a razones territoriales, a la cuantía de los asuntos, a la materia misma de la controversia y al grado, lo cual origina la competencia de determinado tribunal para conocer de un negocio. Así pues, la jurisdicción es la potestad de que se hallan investidos los Jueces para administrar justicia y la competencia es la facultad que tienen para conocer de ciertos negocios, y esa facultad debe serles atribuida por la ley o puede derivarse de la voluntad de las partes"[15].

Con la noción anterior, es menos complejo entender que la jurisdicción es el poder para aplicar y administrar la justicia mediante un actor al que se le va a otorgar cierta autoridad, por lo que ya no solo es de "alguien" como lo planteaba la Real Academia Española, si no que aquí es un actor en especifico que va a tener dicha potestad. Este concepto va a tomar relevancia junto a la idea de soberanía para entender como ambos funcionan dentro del ciberespacio y del poderío que se tiene sobre el concepto de guerra, ya que de

[14] Real Academia Española*, Diccionario de la Lengua Española*, Madrid, Espasa Calpe, 1984, segunda edición, p. 805.
[15] Seminario Judicial de la Federación, *Jurisdicción y competencia,* [en línea], México, Suprema Corte de Justicia de la Nación, 07 de agosto de 1975, Dirección URL: https://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/245/245837.pdf, [consulta: 19 de abril de 2019].

las contradicciones surge aquella en la que debido a la falta de delimitación territorial es complejo intentar definir la soberanía en dicho territorio, así como emprender la jurisdicción en el espacio pues se requiere de la autoridad competente que la lleve a cabo, misma que es difícil de determinar, pues se da lugar una lucha de poder por saber que actores o Estados pretender gobernar tal espacio.

Pese a existir distintas definiciones y visiones respecto al ciberespacio, la mayoría de ellas coinciden en que es una zona no delimitada que se sustenta en una red interconectada, lo que permite la conexión recíproca de las sociedades. Ello también trajo consigo una serie de retos en cuanto a la utilización de los términos soberanía y jurisdicción dentro del ciberespacio.

El progreso del espacio cibernético como escenario, ha dado pie al desenvolvimiento de distintos fenómenos que se han posicionado como agentes de cambio no solo dentro de ese medio, sino también en las estructuras políticas y sociales, tal es el caso de la ciberguerra como un hecho que no solo ha modificado el mismo ciberespacio, sino de igual manera la metodología, las herramientas y los actores para hacer la guerra dentro de éste, siendo la ciberguerra un tema fundamental para la presente investigación.

1.2. Definición de guerra y ciberguerra

El ciberespacio se convirtió en un escenario para que los distintos actores dentro del sistema comiencen a crear relaciones interconectadas para expandir sus redes con distintas ramas.

El desarrollo tecnológico ha creado un margen de conflicto dentro del ciberespacio, ya que lo ha convertido en el campo de batalla de los Estados, pues la amenaza persistente de ataques entre éstos fortalece este nuevo escenario de confrontación, creando una nueva forma de guerra, a la que se le denomina como ciberguerra.

La ciberguerra se deriva de la concepción de guerra, misma que a su vez cuenta con diferentes nociones para describirla, razón por lo cual es necesario delimitar ésta para poder comprender la idea de ciberguerra.

Luis Alfredo Valdés basado en una definición de Carl Von Clausewitz, define la guerra de la siguiente manera:

“Guerra en el sentido literal significa combate, porque sólo el combate es el principio eficaz en la actividad múltiple que en sentido amplio llamaremos guerra… el arte de la guerra en su verdadero sentido, es el arte de hacer uso en combate de los medios dados, y a esto no podemos darle mejor nombre que el de “la conducción de la guerra”… La dirección de la guerra es, por lo tanto, la preparación y conducción del combate”[16].

De esta manera, Valdés nos da a entender que el combate es aquello que se deriva del usar los medios que se tienen para llevar las actividades bélicas que se desenvuelven en lo que es la guerra, por lo que en este sentido, es posible identificar que la relación que existe con la ciberguerra deviene de los medios que se tienen para poder realizar las acciones que de ello se originan.

Respecto a la línea de escritura anterior, es esencial destacar la definición de Clausewitz, quien explica lo siguiente:

“No queremos comenzar con una definición altisonante y grave de la guerra, sino limitarnos a su esencia, el duelo. La guerra no es más que un duelo en una escala más amplia. Si quisiéramos concebir como una unidad los innumerables duelos residuales que la integran, podríamos representárnosla como dos luchadores, cada uno de los cuales trata de imponer su voluntad por medio de la fuerza física; su propósito siguiente es abatir al adversario e incapacitarlo para que no pueda proseguir con su resistencia. La guerra constituye, por tanto, un acto de fuerza que se lleva a cabo para obligar al adversario a acatar nuestra voluntad”[17].

En primera instancia, Clausewitz hace referencia a la parte del duelo, mismo que al extenderse se convierte en lo que llamamos guerra, que tiene concordancia con lo explicado por Valdés, que sustituye la idea de duelo por combate, en donde se usan los medios que se tienen para realizar las acciones.

Por otra parte, Clausewitz hace referencia a que el adversario acate la voluntad que la otra parte impone, por lo que considera la guerra como un medio para lograr obtener el dominio, es decir, el poder como la base para cumplir con los intereses que se tienen mediante el acto bélico.

[16] Valdés, Luis A, *Planeación estratégica integral con enfoque de sistemas: caso de éxito con observaciones* en Planeación Prospectiva Estratégica, México, UNAM, 2015, p. 562.
[17] Clausewitz, Karl, *De la guerra,* Greenbooks editores, 2016, p.4.

La ciberguerra es definida como “El uso de capacidades basadas en la red de un Estado, para interrumpir, denegar, degradar, manipular o destruir información residente en ordenadores y redes de ordenadores, o los propios ordenadores y las redes de otro Estado”[18], con el objetivo de debilitar o desmantelar por completo la infraestructura informática con la que cuenta el Estado, para de esta manera bloquear los flujos de operación cotidianos del país y mostrar superioridad ante el afectado.

Al respecto, el Instituto de Ingeniería de la Universidad Nacional Autónoma de México define el término ciberguerra haciendo una comparación con la guerra común,

“En una guerra convencional, los adversarios generalmente conocen sus capacidades, armamentos y tácticas específicas donde existe un frente de batalla común claramente delimitado por factores geográficos; en la ciberguerra, el ambiente, las estrategias y las armas son totalmente distintas pero con un potencial destructivo similar a las armas físicas. Las fronteras son inexistentes y los atacantes virtualmente invisibles; su objetivo, desmantelar o deshabilitar la infraestructura informática del enemigo con todo lo que ello implica: bloquear accesos, ocasionar retrasos en la red, provocar denegación de servicio, lanzar malware masivamente (spyware, virus, gusanos, troyanos), crear botnets, robar información, entre muchos otros”[19].

Por su parte, Juan Pablo Salazar señala que las “acciones efectuadas por una Organización-Nación-Estado con el propósito de penetrar los sistemas informáticos y redes de computadores de otra Nación-Estado, con el propósito de causar daños o interrupción de los mismos”[20].

Por otro lado, Gema Sánchez Medero en *Los Estados y la ciberguerra* menciona que:

---

[18] Carrillo, Leonardo, Vargas, Paola, *Ciberguerra: descripción de estrategias políticas internacionales y algunos planteamientos jurídicos para afrontarla*, [en línea], Bogotá, Universidad Militar Nueva Granada, 2016, Dirección URL: https://repository.unimilitar.edu.co/bitstream/handle/10654/16043/carrillofarfancesarleonardo2017%20% 281%29.pdf?sequence=3&isAllowed=y, [consulta: 17 de diciembre de 2018], p. 12.

[19] s/a, *Ciberguerra*, [en línea], Instituto de Ingeniería-UNAM, Dirección URL: http://www.iingen.unam.mx/esmx/Publicaciones/GacetaElectronica/Mayo2016/Paginas/Ciberguerra.aspx, [consulta: 16 de diciembre de 2018].

[20] Salazar, Juan Pablo, *La migración de la guerra al espacio digital*, [en línea], Madrid, Universidad Complutense de Madrid, Dirección URL: https://www.sites.oas.org/cyber/Documents/2016%20%20La%20migracio%CC%81n%20de%20la%20guerra%20al%20espacio%20digitalJuan%20Pablo%20Salazar.pdf, [consulta: 17 de diciembre de 2018], p. 25.

“La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático”[21].

En este sentido, es posible realizar una comparación entre la concepción emitida por Sánchez Medero y la que expresa Juan Pablo Salazar, puesto que el segundo hace referencia a distintos actores que efectúan las acciones perjudiciales hacia los sistemas informáticos y de comunicación, y no solo a los Estados, mientras que la primera emite un juicio hacia el Estado, a quien considera como el productor de dichas agresiones.

Ariel Pantano, concibe a la ciberguerra como “el desplazamiento de un conflicto, en principio de carácter bélico, que toma el ciberespacio y las tecnologías de la información como escenario principal, para producir alteraciones en datos y sistemas del enemigo, a la vez que se protege la información y sistemas del atacante”[22], argumentando que la guerra cibernética es una actividad bélica más allá de las fronteras físicas de un territorio especifico.

La ciberguerra funge como el acto bélico en un territorio que no tiene delimitación concreta, lo que deja en incertidumbre cuanto es el alcance de los daños que ésta puede tener para el sistema internacional. Asimismo, la aplicación de cierta normativa jurídica en el tema de la ciberguerra es compleja, puesto que las contradicciones que existen permiten la aparición de un desasosiego en cuanto a que norma debe regir el tema en cuestión.

El pragmatismo en el que vive el sistema ha generado que las concepciones de guerra respecto al entorno estén en constante cambio, ya que debe existir un sentido de adaptación, incluso, dentro del mismo Derecho Internacional, tal es el caso del Derecho de Guerra, presentado en el apartado siguiente.

---

[21] Sánchez, Gema, *Los Estados y la ciberguerra*, [en línea], España, Universidad de La Rioja, 2010, Dirección URL: https://dialnet.unirioja.es/servlet/articulo?codigo=3745519, [consulta: 16 de diciembre de 2018], p. 64.

[22] Pantano, Ariel, *Ci*berguerra, [en línea], Argentina, Universidad de Palermo, Dirección URL: https://dspace.palermo.edu:8443/xmlui/bitstream/handle/10226/1448/Ciberguerra-Pantano%2068586.pdf?sequence=1 [consulta: 14 de abril de 2018], p. 1.

1.2.1 Derecho de Guerra

La guerra ha sido un elemento importante para esa transformación referida con anterioridad, ya que de ella han derivado distintos sucesos que han sido un punto de partida para entender el desarrollo del contexto internacional.

El Derecho de guerra ha sido parte de los reajustes presentados, en cuanto a su concepción se refiere.

En principio, en el sentido clásico, fue definido como tal, como derecho de la guerra, *ius ad bellum,* que pronto se sustituyó por derecho de guerra por lo que se entiende que son "las reglas bajo las cuales deben conducirse las partes que se encuentran en un conflicto armado"[23], es decir, es el derecho que va a regir el control de las disputas bélicas. La importancia de esta idea radica en que no se utiliza el concepto de guerra, sino como se menciona, como conflicto armado.

Los tratados internacionales que rigen el derecho de guerra se basan en el Ordenamiento sobre las Guerra Nacionales de la Haya de 1907, mismos que tienen como base el Convenio de Ginebra para el mejoramiento de la suerte que corren los militares heridos en los ejércitos en campaña de 1864, así como la Declaración de San Petersburgo (prohibición del uso de determinados proyectiles en tiempo de guerra) de 1868. Posteriormente, se concluyeron las cuatro Convenciones de Ginebra de 1949, acompañadas de sus dos protocolos adicionales de 1977. Sin embargo, es importante mencionar otros instrumentos que han sido complemento para los ya mencionados, tales como Convención de La Haya para la protección de los bienes culturales en caso de conflicto armado de 1954; los dos Protocolos adicionales a los Convenios de Ginebra de 1949 que mejoran la protección de las víctimas de los conflictos armados internacionales y no internacionales publicados en 1977; Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados de 1980 y al que se le añaden 3 protocolos adicionales; el Estatuto de Roma de la Corte Penal Internacional de 1998; asimismo, en 1999 se crea el Protocolo a la Convención de 1954 para la protección de los bienes culturales, al que en 2000 le siguió el Protocolo facultativo de la Convención sobre los

[23] s/a, *El DIP de guerra* en Derecho Internacional Público, [en línea], México, Instituto de Investigaciones Jurídicas de la UNAM, Dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/7/3262/21.pdf, [consulta: 19 de abril de 2019], p. 145.

Derechos del Niño relativo a la participación de niños en los conflictos armados; mientras que en 2001 y 2005 se creó la Enmienda al artículo I de la Convención sobre ciertas armas convencionales y el Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la aprobación de un signo distintivo adicional, respectivamente.

No obstante, con la finalización de las guerras mundiales, y la necesidad de acentuar el tema de la paz en los asuntos de la guerra y como ausencia de ésta, así como con la nueva visión de distintos autores como Armando Soto, se da lugar a un Derecho Internacional Humanitario, y se define como "sistema integral de normas que se aplican particularmente en tiempo de guerra o de beligerancia interna, con el propósito de tutelar los bienes jurídicos de las personas ajenas al conflicto e incluso que formaron parte del mismo"[24].

Es así como la ideología contemporánea del ahora Derecho Internacional Humanitario se basa en un centro antropológico en donde se intenta "humanizar" la guerra para de esta manera disminuir el sufrimiento y los daños que se ocasionaron tras los conflictos armados.

El Derecho Internacional Humanitario es basado en que el individuo es el más importante, puesto que considera su protección y cuidado para evitar perjudicarlo durante el enfrentamiento bélico.

Asimismo, es importante destacar que dicho derecho se ha visto adaptado al contexto internacional, mismo que enfoca su visión en la seguridad humana, lo que ha generado que de ello se obtengan las bases en el cambio de concepto del derecho de guerra.

Sin embargo, el entorno no deja de transformarse de manera constante, por lo que es debido preguntarse si el derecho de guerra o Derecho Internacional Humanitario puede ser aplicable a la ciberguerra en un territorio no determinado como lo es el ciberespacio, mismo que no se tiene una idea concreta del alcance jurídico dentro de éste.

[24] Soto, Armando, "Derecho de la guerra = Derecho Internacional Humanitario", [en línea], México, Insituto de Investigaciones Jurídicas- UNAM, 2015, Dirección URL: http://dx.doi.org/10.22201/fder.24488933e.2015.263.59871, [consulta: 19 de abril de 2019], p. 428.

1.3. Conceptos básicos para comprender las acciones reconocidas como agresiones en el ciberespacio y su equiparación a la guerra

Los cambios que ha sufrido el contexto actual han favorecido a que las problemáticas tengan nuevas perspectivas hacia las nuevas situaciones que se presentan.

Los nuevos conceptos han sido adaptados a las circunstancias emergentes que han transformado el desenvolvimiento de los actores dentro del sistema internacional.

La guerra ha cambiado, tanto en su instrumentación como en el modo de hacerla, es por ello que en el presente apartado se van a desarrollar los conceptos básicos para entender las acciones que son reconocidas como agresiones de ciberguerra dentro del ciberespacio y la equivalencia de dicha concepción con la idea clásica de guerra.

Dichos conceptos se encuentran vinculados al entorno en el que se involucra la dinámica del ciberespacio, ya que el ciberespacio se ha convertido en uno de los campos más controversiales para la dinámica que se juega dentro del sistema, puesto que, al no tener un rango de alcance totalmente definido, plantea una serie de retos que lo llevan a carecer de ciertas características que le reconozcan jurisdicción.

De esta manera, es importante determinar ciertos conceptos que van a permitir el entorno que conlleva la ciberguerra dentro del ciberespacio, ya que cada uno de ellos representa un aspecto fundamental.

1.3.1. Infraestructura informática

La concepción que se tiene para comprender términos estatales y jurídicos es fundamental, no obstante, es necesario determinar cuál va a ser su aplicabilidad, pues el campo es el ciberespacio, sin embargo, de éste emanan distintos componentes que conforman distintas estructuras que juegan un papel importante en materia de ciberguerra.

La infraestructura informática, o de acuerdo al nuevo contexto tecnológico, infraestructura tecnológica, es el:

“conjunto de software y hardware sobre el que se soportan los servicios de una organización para responder eficientemente a las necesidades de los consumidores, actualizar los planes de control o supervisión y optimizar la cooperación con proveedores

y clientes. Este conjunto de medios técnicos, que contienen redes o líneas de comunicación"[25]. El segundo, hardware, es referido por parte del Instituto de Ingeniería de la UNAM, como a "la parte física de una computadora, es decir, todo aquello que pueda ser tocado: teclado, ratón, monitor, impresora, cables, tarjetas electrónicas, carcasa, disco duro, memorias, bocinas, micrófono, etcétera"[26]. Por su parte, el software es conceptualizado como "lo opuesto al hardware, es decir, la parte intangible o lógica de la computadora: los programas, los sistemas de información, las aplicaciones (como procesadores de texto, hojas de cálculo o bases de datos), los simuladores, las aplicaciones gráficas y los sistemas operativos"[27]. Pese a ser definiciones contrarias, ambos elementos son dependientes entre sí, pues se requiere de un software especifico y que cumpla con los requerimientos para que la función del hardware sea óptima.

Ello se complementa de una infraestructura Tecnología de la Información, la cual es conocida como "el servicio que ofrece el conjunto de dispositivos y aplicaciones necesarios para una empresa"[28], por lo que es considerado como un sistema base para hacer funcionar de manera adecuada la infraestructura informática, y "se gestiona a través de la monitorización mediante el despliegue de los equipos suficientes, máquinas y software"[29].

La finalidad de ambas infraestructuras es optimizar los procesos que se gestionan y se adaptan a las necesidades de la transformación digital que se vive día con día, en conjunto con sus dos componentes fundamentales hardware y software.

Es conveniente señalar, que dentro de software existe una rama destacable conocida como malware que se refiere a "cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil. Los tipos de malware incluyen spyware (software

[25] s/a, *Cómo aumentar el rendimiento de tu infraestructura informática,* [en línea], España, RCG Comunicaciones, Dirección URL: http://rcg-comunicaciones.com/rendimiento-infraestructura-informatica/, [consulta: 20 de abril de 2019].
[26] s/a, *Hardware y software*, [en línea], Instituto de Ingeniería-UNAM, Dirección URL: http://www.iingen.unam.mx/es-mx/Publicaciones/GacetaElectronica/GacetaNoviembre2013/Paginas/Hardwareysoftware.aspx, [consulta: 21 de abril de 2019].
[27] *Ídem.*
[28] Saavedra, Alberto, *¿Qué es la Infraestructura Tecnológica IT? Beneficios en la Transformación Digital,* [en línea], España, Clavei Expertos en Transformación Digital, 13 de febrero de 2018, Dirección URL: https://www.clavei.es/blog/que-es-la-infraestructura-it/, [consulta: 21 de abril de 2019].
[29] *Ídem.*

espía), adware (software publicitario), phishing, virus, troyanos, gusanos, rootkits, ransomware y secuestradores del navegador""[30].

Dicho componente es manejado por distintas figuras que cuentan con un objetivo perjudicial. Un ejemplo de ello, son los hackers, igualmente conocidos como piratas informáticos, aunque existe un debate respecto a ésta última concepción de estos personajes.

Un hacker es considerado como un programador inteligente, que tiene las capacidades suficientes para poder manipular o modificar desde un sistema hasta una red informática[31], empero, hay la existencia del llamado hacker malicioso quien "es alguien que utiliza sus conocimientos de informática para obtener acceso no autorizado a datos tales como información de tarjetas de crédito o imágenes personales, ya sea para diversión, beneficio, para causar daño o por otras razones"[32], y que son los ejecutantes de las acciones que son equiparables a la guerra en el ciberespacio.

Una situación que se presentó el 8 de noviembre de 2010 y que ejemplifica el modo de actuar de un hacker o pirata informático, fue cuando la página oficial de la Marina Británica había sido hackeada por piratas informáticos, y fue realizado con la introducción de un hacker conocido como TinKode "mediante el método Inyección SQL, un tipo de ataque que introduce código SQL. Inyección SQL es un agujero de vulnerabilidad informática de programas escritos en el lenguaje de programación SQL y que se produce durante la validación de las entradas a la base de datos de una aplicación"[33]. Lo que provocó este ciberataque fue la alteración del funcionamiento de la página y la obtención de información de la Marina Británica por parte de los piratas cibernéticos.

Este ataque fue frenado con la suspensión de la página de la Marina Británica, para de esta manera poder realizar acciones de ciberdefensa y volver a ponerla en funcionamiento.

---

[30] s/a, *Malware y antimalware,* [en línea], Avast, Dirección URL: https://www.avast.com/es-es/c-malware, [consulta: 23 de abril de 2019].
[31] s/a, *Hacker*, [en línea], Avast, Dirección URL: https://www.avast.com/es-es/c-hacker, [consulta: 25 de abril de 2019].
[32] *Ídem.*
[33] BBC, "Royal Navy website attacked by Romanian hacker", [en línea], BBC News Technology, 08 de noviembre de 2010, Dirección URL: https://www.bbc.com/news/technology-11711478 [consulta: 13 de junio de 2019].

Asimismo, existen otras infraestructuras que debido a su relación y su interconectividad con el entorno ciber de cada Estado se ven afectadas por las distintas actividades que pretenden desmantelar y vulnerar a dicho ente estatal, tal es el caso de la infraestructura crítica.

La infraestructura critica, descrita por el Departamento de Seguridad Nacional de los Estados Unidos como "the physical and cyber systems and assets that are so vital to the country that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. The nation's critical infrastructure provides the essential services that underpin society"[34] se ha convertido en un punto focal para los ciberataques, orquestados, en su mayoría por hackers comandados por Estados que buscan desestabilizar dicha estructura, ya que la infraestructura critica de los países está interconectada entre sí gracias a los avances tecnológicos, y también es un epicentro para la seguridad nacional, debido a que si se lleva a cabo un ataque en dicha infraestructura existirá una desestabilidad con daños perjudiciales.

De esta forma, la infraestructura crítica se convierte en un objetivo para fomentar las acciones reconocidas como agresiones dentro del ciberespacio y su equiparación a la guerra, es decir, se convierte en la intención principal de otros actores estatales para llevar a cabo agresiones a dicha infraestructura siendo el ciberespacio como escenario, mismas que podrían desencadenar una ciberguerra entre los involucrados.

Cabe enfatizar, que las infraestructuras mencionadas son la motivación primordial de los actores estatales que se enfrentan durante una ciberguerra, debido a que éstas son la base de la interconexión existente entre el Estado, su sociedad y las nuevas tecnologías, mismas que manejan una gran cantidad de datos, por lo que al transgredir dichas estructuras se crean vulnerabilidades que generan un ambiente inseguro, poniendo en constante amenaza el orden político, económico y social del Estado o los Estados participantes en las actividades bélicas, que podrían llevar a una ruptura en la estabilidad de éstos y, por consiguiente, en la del sistema internacional.

Así es como su puede poner de ejemplo el caso ocurrido en una planta nuclear en Natanz provincia de Isfahan en Irán, en enero de 2010, en la que el gusano malicioso conocido

[34] s/a, *Infrastructure Security,* [en línea], Estados Unidos, United States Department of Homeland Security, Dirección URL: https://www.dhs.gov/topic/critical-infrastructure-security [consulta: 12 de junio de 2019].

como Stunext infectó el sistema informático que controlaba la planta, lo que generó un caos con las máquinas centrifugadoras que contenían grandes cantidades de uranio, lo que las llevo a su autodestrucción. Lo circunstancial del caso no solo fue lo desarrollado que era código utilizado, si no que éste había sido diseñado con una mentalidad bélica[35] . Además, de que la BBC mencionó que "el reconocido experto Ralph Langner dijo que el gusano fue creado en laboratorio por Estados Unidos e Israel para sabotear el programa nuclear de Irán, pero las autoridades no han confirmado esa afirmación"[36], razón por la que se llegó a considerar la base de una ciberguerra entre aliados e Irán.

Con base en los plantemaientos desarrollados hasta este momento, se considera que es posible entender conceptos que sirven para ser aplicables en el tema a tratar en la presente investigación. De igual modo, es sustancial recalcar la concepción que infiere en la cuestión del ciberespacio, ya que con ella se tiene un mayor entendimiento de la problemática en ciberseguridad que ésta presenta y en los distintos elementos que participan, misma que juega un papel elemental para dar una ofensiva y una defensiva en temas de ciberataques, mismos que pueden convertirse en ciberguerra.

1.3.2. El entorno "ciber" en constante amenaza

El software y hardware son parte del entorno cibernético en el que se desenvuelve la sociedad dentro de la era de la transformación digital, misma que se adapta al contexto que se encuentra en constantes cambios.

El ciberespacio ha extendido su entorno y sus actividades en dicha transformación, ello ha generado que la seguridad de éste sea expuesta a riesgos y amenazas que intervienen directa o indirectamente en distintos actores pertenecientes al sistema internacional.

Las nuevas amenazas a las que se enfrenta el siglo XXI son constantes y distintas a las de otras eras, entre ellas destacan las ciberamenazas que se refiere a "aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su

[35] BBC, "El virus que tomó control de mil máquinas y les ordenó autodestruirse", [en línea], BBC News Mundo, 11 de octubre de 2015, Dirección URL: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet [consulta: 13 de junio de 2019].
[36] *Ibíd.*

utilización, manipulación, control o sustracción"[37]. Dentro de éstas se engloban temas que han sido de suma relevancia a lo largo de la historia, pero que han sido acondicionadas al contexto actual, tal es el caso del ciberespionaje, el que Joaquín Ruiz describe como "la obtención de información, de tipo principalmente estratégico, que hoy en día se encuentra almacenada electrónicamente, si bien bajo grandes medidas de seguridad, en los servidores de las instituciones de defensa estratégicas, de la inmensa mayoría de los países"*[38].*

Cabe señalar, que el objetivo principal de este tipo de actividad, como lo es en el espionaje tradicional, es el de obtener cierta ventaja tanto política, económica como comercial y militar, que es clasificado como una herramienta estratégica durante la ciberguerra.

Es imprescindible destacar, que esta clase de ciberataques no siempre son parte de la ciberdelincuencia, empero, tampoco todas son acciones equiparables a la guerra en el espacio cibernético, ya que la ciberdelincuencia es determinada bajo la idea de "delincuencia vía internet"[39], o mayormente descrito en el Convenio sobre ciberdelincuencia promulgado por el Consejo de Europa en 2001, en donde se hace referencia a ésta cuando se "pongan en peligro la confidencialidad, la integridad, y la disponibilidad de los sistemas , redes y datos informáticos , así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio"[40].

Es por esta razón que las acciones realizadas por la ciberdelincuencia no son ciberguerra, pues pese a tener similitudes como el vulnerar los sistemas para extraer y exhibir información sustancial, los ciberdelincuentes son los actores, no los Estados, y los primeros trabajan para objetivos más personales.

---

[37] Ruíz, Joaquín, *Ciberamenazas: ¿el terrorismo del futuro?,* [en línea], España, Instituto Español de Estudios Estratégicos, 19 de agosto de 2016, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf, [consulta: 24 de abril de 2019], p. 1.

[38] *Ibíd.* p. 12.

[39] Ministerio de Defensa, *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, España, Instituto español de estudios estratégicos, 2010, p.52.

[40] Consejo de Europa, *Convenio sobre la ciberdelincuencia,* Budapest, Consejo de Europa, 23 de noviembre de 2001, Preámbulo.

Igualmente, se enlista al ciberterrorismo como una ciberamenaza perjudicial, el cual se precisa en término abstracto como "terrorismo a través de la red"[41], por lo que es complejo obtener una definición completamente aceptada debido a que la concepción de terrorismo no ha sido totalmente aceptadas ni definida de manera unánime, debido a que existe un conjunto de posturas ideológicas respecto a ello. Asimismo, se ha determinado una asociación en cuestión de terminología con ciberguerra, no obstante, pese a tener semejanzas, no es lo mismo, debido a que el terrorismo cuenta, también, con un propósito político, pero busca modificar patrones de comportamiento mediante la fenomenología, ya sea religiosa, política o temática y no busca, casi nunca, un beneficio económico, pero lo que más destaca es que son actores no estatales, por lo tanto, de nueva cuenta no puede integrarse a la idea de ciberguerra, debido a que no hay una confrontación entre Estados, ni tampoco su propósito es el de desmantelar o desestabilizar la infraestructura critica.

Por otro lado, para combatir dichos riesgos y amenazas, que pueden desencadenar en una guerra cibernética, se ha puesto énfasis en la ciberseguridad, la cual es entendida como:

"el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización y los usuarios en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de una organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno"[42].

Por lo que la ciberseguridad pretende proteger de todo aquello que se encuentre dentro de dicho ciberentorno, es decir, en un término más superficial se habla de ésta haciendo referencia a "la seguridad de la tecnología de la información, puesto que engloba un gran número de técnicas y métodos para proteger nuestro sistema, así como otros dispositivos o las redes"[43].

[41] *Ibíd.* p. 52.
[42] *Ibíd.* p. 54-55.
[43] s/a, *¿Qué es ciberseguridad y de qué fases consta?*,[en línea], Barcelona, OBS Business School, Dirección URL: https://www.obs-edu.com/int/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta, [consulta: 23 de abril de 2019].

Con ello, es posible confundir la concepción de ciberseguridad con ciberdefensa, surgiendo la interrogante de si son sinónimos o son cuestiones totalmente diferentes pero que tienen un sentido común dentro del entorno cibernético.

La ciberdefensa es concebida como "el conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición"[44].

Es decir, son las acciones que se realizan para erradicar el problema de inseguridad en el ciberespacio, de esta forma, se expresa la diferencia entre ciberdefensa y ciberseguridad, "la Ciberdefensa, además de prevenir los ataques como hace la Ciberseguridad, da respuesta a los mismos con nuevos ataques con fin de salvaguardar la seguridad"[45]. Cabe destacar, que también existe una noción específica para los ciberataques la cual es:

"la explotación deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología. Estos ataques utilizan códigos maliciosos para alterar la lógica o los datos del ordenador, lo que genera consecuencias perjudiciales que pueden comprometer información y provocar delitos cibernéticos"[46].

Con respecto a lo anterior, se puede interpretar, que la ciberseguridad tiene un carácter preventivo, ó sea que apunta a que el riesgo, el cual es latente pero aún no sucede, no se convierta en una amenaza, o en su caso en una ciberamenaza, mientras que la ciberdefensa si tiene aspecto precautorio, empero, también cuenta con voluntad de replica y resolución para todas dichas actividades que ya están dañan do el entorno.

Las capacidades que tienen los distintos actores para enfrentar las ciberamenazas se engloban internamente en la ciberdefensa. Dentro de las competencias con las que se cuentan, existe la necesidad de enriquecimiento de éstas y llevarlas a un sentido

[44] s/a, *Ciberdefensa-Ciberseguridad Riesgos y Amenazas,* [en línea], Consejo Argentino para las Relaciones Internacionales, noviembre 2013, Dirección URL: http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf, [consulta: 24 de abril de 2018], p. 1.

[45] s/a, *¿Qué es la Ciberdefensa y en qué se diferencia de la Ciberseguridad?,* [en línea], España, Next International Business School, 15 de agosto de 2018, Dirección URL: https://www.nextibs.com/que-es-ciberdefensa-se-diferencia-ciberseguridad/, [consulta: 24 de abril de 2018].

[46] s/a, *¿Qué es un ciberataque y qué tipos existen*?, [en línea], Valencia, Transformación Digital Cámara de Valencia, Dirección URL: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/#Que_es_un_ciberataque, [consulta: 24 de abril de 2019].

mayormente activo, eficaz y eficiente para lograr confrontar los enigmas que surgen, es por ello que se ha optado por la creación de un cibermando militar o ciberejércitos los cuales hacen alusión a la capacidad militar que se posee para la defensa del ciberespacio[47], mismos que pretenden neutralizar las ciberamenazas desde el origen, implementando estrategias que aprovechen las disposiciones que brindan las capacidades de ciberdefensa, además de desarrollar éstas para cuando el entorno cibernético se convierta en un escenario hostil y bélico.

Dichas actividades de defensa se basan en realizar acciones enfocadas en el tema, a lo que se le llama, en un sentido más técnico, ciberoperaciones, las cuales fungen como:

"el empleo de cibercapacidades con el propósito principal de alcanzar determinados objetivos dentro o a través del ciberespacio. Estas operaciones abarcan acciones en redes informáticas y actividades para operar y defender la red y la infraestructura que integra los sistemas de información, servicios, procesos y los datos de defensa para el desarrollo y la ejecución de operaciones"[48].

Es significativo referir que existen diferentes países que han fomentado iniciativas respecto al tema de los ciberejércitos, tales como Estados Unidos, Reino Unido, China, Rusia, Irán, India, Pakistán, Corea del Norte, Corea del Sur, Israel, entre otros[49].

Es posible afirmar que, pese a usar dichos comandos militares como una herramienta de defensa, también se emplean como elementos que enfatizan el poder de éstos Estados, entonces podríamos hablar ya no solo del dominio en el entorno tradicional si no, incluso, en el ciberespacio, que es un nuevo e importante dominio de poder, pues el ciberespacio cibernético se considera como el dominio más moderno, y que se suma a los llamados tradicionales, los cuales son la tierra, mar, aire y espacio, mismos en los que se desenvuelven todas aquellas actividades que convergen en los intereses de los actores participantes en éstos, por lo que durante la guerra cada dominio funge un papel importante, pues de cada uno se requiere realizar una estrategia para poder sacar ventaja de éste mismo y superar o envolver al enemigo, por lo que se puede sugerir la idea de ciberpoder, por la necesidad de tener influencia sobre dicho dominio.

---

[47] Casar, Corredera, *El ciberespacio. Nuevo escenario de confrontación*, España, Centro Superior de Estudios de la Defensa Nacional, 2012, p. 240.
[48] s/a, *Ciberoperaciones*, [en línea], España, Astabis Information Risk Management, Dirección URL: https://www.astabis.com/es/servicios-para-los-gobiernos/defensa/ciberoperaciones, [consulta: 25 de abril de 2019].
[49] Ministerio de Defensa, *Ibíd.*

El poder, en palabras de Joseph Nye, es “the ability to affect other people to get the outcomes one wants. Some people call this influence, and distinguish power from influence, but that is confusing because the dictionary defines the two terms interchangeably”[50], es decir, el poder es la capacidad de influir en las decisiones de los demás. Esta terminología ha tenido que adaptarse a la evolución moderna del contexto y del comportamiento de la sociedad, por lo que basándose en la apreciación del concepto, se plasma la nueva idea de ciberpoder, la cual Nye lo confiere en 2 definiciones diferentes, pero que en conjunto enrolan un solo razonamiento.

La primera parte hace referencia a la actuación de éste:

“Cyber power behavior rests upon a set of resources that relate to the creation, control and communication of electronic and computer based information -- infrastructure, networks, software, human skills. This includes the Internet of networked computers, but also intranets, cellular technologies and space based communications”[51].

Mientras que conceptualmente menciona que el:

“cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. In one widely used definition, cyber power is “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power.” Cyber power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace”[52].

En relación al poder, el ciberpoder también es la competencia que se tiene para poder influenciar en el actuar de los demás, solo que en su caso, el modo de operar es mediante el ciberespacio como medio, y los sistemas tecnológicos de información como su herramienta, es por ello que éste puede utilizarse como una motivación para realizar actividades que se desenvuelvan en la ciberguerra, ya que la idea de los Estados es la adquisición de poder para crear ventajas sobre el resto de éstos en el sistema internacional y, que les permita liderar y tomar el control del ahora llamado quinto dominio para obtener superioridad dentro y fuera de éste.

[50] Nye, Joseph, Cyber Power, United States, Belfer Center for Science and International Affairs, 2010, p.2.
[51] *Ibíd.* p. 3
[52] *Ibíd.* p. 3-4.

Concluyendo la conceptualización

El contexto actual en el que se realizan las actividades ha sufrido alteraciones que se le atribuyen a las innovaciones tecnológicas que acrecientan día con día, en las que los actores participantes dentro del sistema fungen como un punto de partida para habituarse al nuevo entorno basado en las tecnologías de la información.

El ciberespacio se ha convertido en un sitio de suma relevancia para distintos actores que se interrelacionan dentro del sistema internacional. Los distintos ciberataques que se llevan a cabo dentro de éste y que han sido dirigidos a los distintos actores entre los que se encuentran los Estados, las empresas y las distintas cibersociedades que convergen dentro del espacio cibernético, han dado lugar a que la guerra sea uno de los conflictos con protagonismo en éste, por lo que ha sido considerado como el quinto dominio de la guerra[53], posicionándose junto a los otros 4 dominios de suma importancia, la tierra, el mar, el aire y el espacio.

Al ser considerado de tal manera, la OTAN ha establecido el ciberespacio como dominio militar legítimo, lo que conlleva a que se convierta en un espacio de confrontación, puesto que un ciberataque orquestado a cualquiera de los 29 miembros de la organización sería considerado como si éste hubiese sido realizado a todos; asimismo, "podría accionar el artículo 5 del tratado que está relacionado con la defensa colectiva"[54] del Tratado del Atlántico Norte.

Como se planteó con anterioridad, la ciberguerra es entendida como el accionar de un actor dentro del ciberespacio en el que se pretende debilitar los sistemas informáticos de los Estados para poder sustraer flujos de información que, posteriormente, puedan ser usados en su contra.

Las acciones que se consideran como ciberguerra son aquellas que tienen un trasfondo gubernamental o institucional, es decir, que son impulsadas por éstos para cumplir con el objetivo de tomar control de la infraestructura informática con la que cuentan otros

[53] Carracosa, Celia, *Ciberespacio, el quinto dominio de la guerra,* [en línea], GIASP Intelligence & Strategy, 08 de marzo de 2017, Dirección URL: https://intelgiasp.com/2017/03/08/ciberespacio-el-quinto-dominio-de-la-guerra-cyberspace-the-fifth-domain-of-the-war/ [consulta: 11 de junio de 2019].

[54] s/a, *OTAN considera el ciberespacio como un dominio militar legitimo,* [en línea], México, Coordinación de Seguridad de la Información- UNAM, 29 de junio de 2017, Dirección URL: https://www.seguridad.unam.mx/otan-considera-el-ciberespacio-como-un-dominio-militar-legitimo [consulta: 11 de junio de 2019].

Estados o instituciones para de esta manera tomar ventaja por sobre éstos y sacar un provecho que beneficie, ya sea económica, política, social o culturalmente al actor agresor. Es importante señalar, que dichas acciones se llevan a cabo con ayuda de especialistas en el tema, los llamados hackers.

Como se puede apreciar, han surgido una serie de conceptos que han ayudado a la adaptación de la trama que la ciberguerra envuelve, misma que se viene manejando en los últimos años, sin embargo, ello ha sido sede de grandes desafíos que han sido difíciles de enfrentar debido a la complejidad del reciente contexto internacional.

Hay que recalcar, de manera fundamental y, conforme a lo presentado en la terminología básica, la diferencia entre ciberataque, ciberdefensa y ciberseguridad, en especial, de éstos dos últimos, dentro del espacio cibernético.

En cuanto a ciberataque, como se mencionó anteriormente, es el ataque que se realiza mediante códigos maliciosos que vulneran la información y, por consiguiente, la seguridad. Por lo que, el ataque cibernético es la acción que se realiza mediante distintas técnicas informáticas con un objetivo perjudicial.

Por su parte, y rescatando la diferenciación que se hizo entre ciberdefensa y ciberseguridad, hay que destacar que la primera es referente a todas aquellas acciones a manera de defensa que le permiten atacar y erradicar las constantes amenazas en el ciberespacio, mientras que la segunda, también es el accionar mediante técnicas y métodos para prevenir los ciberataques. Ambas, son concepciones similares, no obstante su distinción radica en que la ciberseguridad previene los ataques, y la ciberdefensa también lo hace, pero además erradica y responde con nuevos ataques planeados de manera estratégica, es decir, ataca para defender y salvaguardar la seguridad.

Las sociedades modernas se sustentan de distintos sistemas que les ofrecen servicios y comunicación para mantener un desarrollo sostenible y que con ello exista progreso. No obstante, el ciberespacio es parte de dichos sistemas que crean nuevas estructuras y con ellas infraestructuras que permiten que se dé lugar lo anterior, razón por la cual éstas últimas han sido foco de ataques que potencian la desestabilidad en los países que cuentan con éstas. La infraestructura critica, descrita con anterioridad con base en la definición que brinda el Departamento de Seguridad Nacional de los Estados Unidos, es un elemento concéntrico en el que los ciberataques se centran para dar lugar a la

desestabilización de la estructura y, de esta manera, vulnerar al mismo sistema del Estado, lo que lo lleva a tener fallas y falta de cobertura en las necesidades de su población e, incluso de las mismas del Estado.

La erradicación de las ciberamenazas se realiza mediante la ciberdefensa, sin embargo, el tema de ciberseguridad se ha posicionado como fundamental dentro de las agendas de los Estados para proteger sus intereses nacionales.

La era cibernética o tecnológica, ha generado la necesidad de adaptación por parte del derecho, debido a que se han formulado grandes desafíos para éste dentro del ciberespacio, pues de acuerdo a la naturaleza amorfa de éste, es decir, que no cuenta con una forma física definida, ni una estructura interna concreta, así como tampoco cuenta con un espacio físico ni geográfico determinado, la jurisdicción, soberanía, atribuciones y responsabilidades cuentan con mayores retos para la aplicabilidad de una norma respecto al uso de la fuerza en esta categoría de nuevos conflictos dentro del sistema internacional.

Cabe destacar, que dentro del Derecho Internacional no existe como tal una norma o algún tratado multilateral que establezca reglas especificas para el tratamiento de la ciberguerra, propiciando la controversia de la aplicabilidad del Derecho Internacional en la nueva serie de conflictos cibernéticos.

Asimismo, tanto los Estados como algunas Organizaciones Internacionales han realizado estrategias enfocadas en la seguridad y protección de los países respecto al tema, pero no existe una homogenización dentro del Derecho que cree una normativa para mitigar las disputas en el ciberespacio.

Determinar si existe una ciberguerra es complejo, ya que se puede confundir con un ciberataque provocado por un hacker hacia un Estado, empero, existen casos de ataques en los últimos años considerados como ciberguerra, entre estos se encuentra el caso ocurrido una planta nuclear en Natanz en enero de 2010, arriba mencionado, el cual el modo en el que se llevo a cabo la estrategia para dar lugar al ataque realizado a las maquinaria que almacenaba el uranio, fue razón por la que se llegó a estimar como una acción que sirviera como cimiento de una ciberguerra entre los Estados implicados, sin embargo el que no se haya podido comprobar que el ataque se originó desde el gobierno de los Estados Unidos ha impedido que sea considerado una acción bélica.

Otra situación que tomó relevancia y que también se expuso a lo largo de este capítulo fue la ocurrida en 2010 cuando la página oficial de la Marina Británica fue hackeada por piratas informáticos, y que al igual que la anterior, no fue una acción considerada como tal como ciberguerra, puesto que si fue un ataque dirigido a una institución del Estado, pero fue orquestado por un hacker, que hasta el momento no existe prueba de que la orden fue realizada por otro Estado.

Los planteamientos expresados en el presente capítulo servirán como base como base para continuar con el análisis que se desarrollará en los capítulos siguientes, que van a enriquecer la investigación de lo que el ciberespacio confronta frente al escenario de la ciberguerra y los desafíos jurídicos y tecnológicos, incluso, para el mismo Derecho Internacional.

CAPITULO 2. La ciberguerra: la nueva confrontación entre Estados

Las estructuras y el modo de actuar de los Estados, han sido alterados, modificados y totalmente transformados por fenómenos tecnológicos como la ciberguerra, que se ha visto acompañada del sustento que le otorga las herramientas y los actores que provienen de una especialización en dicho ámbito.

La introducción de la metodología y la praxis, basada en nuevos escenarios e instrumentos que están bajo la idea de la era tecnológica como la nueva revolución industrial, ha impulsado el desarrollo de actividades bélicas en el nuevo medio, que tienen como pilar el desestabilizar las relaciones y la estructura entre Estados y del mismo sistema internacional.

La naturaleza del ciberespacio ha permitido su propio desarrollo en el entorno actual, sin embargo, también las ciberamenazas se han adaptado a éste contexto, lo que ha generado incertidumbre y la necesidad de combatir las deficiencias, en todos los ámbitos.

De igual manera, es de suma importancia contemplar cómo lo tradicional se ha adaptado, pero también transformado, para habituarse al ambiente hostil que ofrece el quinto dominio, mismo que ha caído en una categoría trascendental porque es el dominio que resulta ser superior, al manejar y controlar de manera integral a los ya existentes.

En este capítulo se expone como el ciberespacio se convirtió en un escenario para las operaciones de ciberguerra. Asimismo, proporciona un panorama de los actores, tales como los ciberejércitos, así como de las herramientas que son utilizadas en estas operaciones en el ciberespacio, siendo el internet la principal y los *big data o* macrodatos, que hace referencia al conglomerado de datos masivos que son procesados y utilizados para analizar el comportamiento de los usuarios[55], así como los ciberataques, que son utilizados como elementos esenciales para llevar a cabo dichas operaciones.

Por otro lado, se presenta el impacto jurídico, tecnológico y social que proviene de la ciberguerra directamente en los Estados, pero también las consecuencias jurídicas a las que se enfrenta el sistema internacional.

Todo lo anterior, con el motivo de crear y entender un análisis enfocado en manifestar los desafíos para la aplicabilidad del Derecho Internacional en la guerra cibernética.

[55] s/a, *¿Qué es big data?,* [en línea], Oracle, Dirección URL: https://www.oracle.com/mx/big-data/guide/what-is-big-data.html, [consulta: 10 de septiembre de 2019].

2.1. El ciberespacio como escenario para las operaciones de ciberguerra

El ciberespacio es un lugar en el que el poder juega un papel de suma importancia. Al ser éste considerado como el quinto dominio, llamado de esa manera debido a que se ha convertido en un escenario significativo para distintas acciones de los distintos actores que tratan de velar por sus propios intereses, uniéndose así a los cuatro dominios, tradicionales tierra, mar, aire y espacio ultraterrestre, las amenazas se han convertido en un tema relevante para los distintos actores que los han llevado a dar lugar a acciones de ciberdefensa.

La guerra se ha transformado a lo largo de los años, esto gracias a las herramientas, los actores y los escenarios que se han ido adaptando al nuevo contexto tecnológico internacional. Es por ello que ha habido una migración de los conflictos equivalentes a actos bélicos hacia el espacio digital.

Los escenarios permiten que se definan de manera adecuada las herramientas e instrumentos que serán utilizados para las actividades dentro de éstos. Javier López de Turiso y Sánchez en su obra *La evolución del conflicto hacia un nuevo escenario bélico,* nos describe un escenario como "un lugar donde ocurre o se desarrolla un suceso"[56] y hace énfasis, basándose en dicha explicación, para delinear lo que es un escenario de conflicto, el cual determina como el "lugar donde ocurre o se desarrolla un conflicto"[57]. Es decir, es el área que se va a convertir en zona de conflicto debido a que pertenece a una serie de escenarios que son naturales o han sido creados de manera artificial para llevar a cabo ciertas actividades y, el contexto que los rodea les permite tomar cada uno de sus elementos para dar lugar a los enfrentamientos.

Cabe destacar, que de estos escenarios se destaca el físico[58], que es el tradicional y en el que se reconoce se dan pie los conflictos, entre éstos se encuentran los dominios que se trataron con anterioridad, terrestre, marítimo, aéreo y espacial.

La transformación de éstos ha llevado a cabo el desenvolvimiento de actividades de conflicto en un nuevo escenario que fue establecido en el mundo virtual, el ciberespacio,

---

[56] López de Turiso, Javier, *La evolución del conflicto hacia un nuevo escenario bélico* en *El ciberespacio. Nuevo escenario de confrontación*, España, Centro Superior de Estudios de la Defensa Nacional, 2012, p.128.
[57] *Ídem*.
[58] *Ibíd*. p. 129

al que López de Turiso se dirige de la siguiente manera, “el ciberespacio no es ni una misión, ni una operación. Es un escenario estratégico, operacional y táctico”[59].

La interconectividad que existe en el ciberespacio ha hecho que la operatividad sea la motivación principal para los distintos sistemas informáticos que les permitan la construcción de una infraestructura más extensa y sólida. No obstante, ello ha provocado que se desatienda el tema de la seguridad dentro de éste, abriendo una brecha de vulnerabilidad, la cual se define como “las características y las circunstancias de una comunidad, sistema o bien que los hacen susceptibles a los efectos dañinos de una amenaza”[60], en dichos sistemas, misma que es aprovechada por las amenazas, a la que se distinguirá de una vulnerabilidad como “un fenómeno, sustancia, actividad humana o condición peligrosa que puede ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales”[61], y ambas como factores del riesgo como “la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas”[62], que se presentan de manera constante, las cuales se adaptan a los cambios tecnológicos que se viven día a día, dando lugar a que los mismos Estados no cuenten con las capacidades suficientes de protección, debido a que los agresores siempre están en ventaja respecto al tema, gracias a sus habilidades que se extienden hacia las competencias adquiridas que los convierten en expertos.

Las vulnerabilidades que son aprovechadas por éstos últimos, fomentan la aplicación de técnicas y tácticas estratégicas que les permiten cumplir con sus objetivos deseados que, dependiendo la perspectiva, pueden ser benéficos o perjudiciales.

La conexión cibernética ha creado una infraestructura interconectada con los cinco dominios existentes, tierra, mar, aire, espacio y, ahora, ciberespacio, por lo que dicha conexión ya no solo pone en riesgo al ciberespacio, sino también al resto de ellos, ya que actualmente, todos se encuentran trabajando de manera conjunta dentro de este espacio,

---

[59] *Ibíd.* p. 128
[60] s/a, *Aproximación para el cálculo de riesgo,* [en línea], Centro Internacional para la investigación del Fenómeno de El Niño, Dirección URL: http://www.ciifen.org/index.php?option=com_content&view=category&layout=blog&id=84&Itemid=336&lang=es, [consulta: 10 de septiembre de 2019].
[61] *Ídem.*
[62] *Ídem.*

puesto que las operaciones que se llevan a cabo dentro de éste se complementan de aquellas que se dan lugar en los dominios que son conocidos de manera tradicional.

De esta manera, se puede observar la extensión para actuar con la que cuenta el ciberespacio, razón por la cual se ha convertido en la "primera línea de batalla, el primer escenario de combate de cualquier acción bélica moderna, por delante de las acciones realizadas en los escenarios tradicionales"[63].

La transformación del contexto tecnológico ha modificado los escenarios y, por consiguiente, los medios tecnológicos que se utilizan para crear un entorno de confrontación. En el espacio cibernético existen medios específicos empleados para poder realizar operaciones de guerra dentro de éste, los cuales son distintos a los que se manejan en los escenarios tradicionales, es decir, se omite la utilización del armamento y medios de transporte físicos, no obstante, éstos son parte del manejo de dichos medios, puesto que su manipulación mediante el sistema que los maneja es un objetivo particular.

Los medios que se usan son diseñados, configurados y manejados por especialistas en el tema. Entre estos medios se encuentran computadoras, laptops, tabletas, teléfonos celulares, etcétera, es decir, todo aquel dispositivo que pueda ser modelado para estructurar y manejar un software, que posteriormente sea modificado para convertirse en malware, operado por un especialista, como lo es el hacker[64].

Cabe destacar, que las acciones bélicas llevadas a cabo en el ciberespacio se rigen bajo los principios de guerra, debido a que pese a ser un nuevo escenario, con medios tecnológicos emergentes, el modo de hacer guerra es dirigido por dichos principios como base.

Distintos autores como Sun Tzu, el estratega naval Alfred Mahan, el capitán retirado Wayne P. Hughes, Liddell Hart, y autores más recientes como Carlos de Izcue Arnillas, describen los principios de la guerra, algunos anexando más y otros restándole, no obstante, todos coinciden con los que presenta Karl Von Clausewitz en *De la guerra* de en cuyas ideas apoyamos nuestro punto de vista. Éstos son la estrategia para alcanzar el objetivo, las principales potencias morales, la virtud militar de un ejército, la audacia, la perseverancia, la sorpresa, la estratagema la cual tiene que ver con el engaño,

[63] *Ibíd.* p. 139
[64] s/a, *Hacker*, [en línea], Avast, *Ibíd.*

concentración de fuerzas en el espacio, concentración de fuerzas en el tiempo, las reservas estratégicas, la economía de fuerzas, el elemento geométrico, la suspensión de la acción de la guerra cuando sea el debido momento, acerca del carácter de la guerra moderna, tensión y reposo, el encuentro, las fuerzas militares, la ofensiva y la defensa[65].

De esta manera, las acciones de guerra han migrado a un nuevo escenario bélico, y los principios de la guerra se han adaptado a dicho entorno, a lo que López de Turiso nos aporta una explicación de cómo dichos principios se han desarrollado:

"Disponen de un objetivo único estratégico, operacional o táctico; precisa de la acción ofensiva súbita que le proporcione la iniciativa; demanda concentración de fuerzas con una distribución de recursos eficiente, tanto en ofensiva como en defensiva; se maniobra con seguridad, mediante acciones de ciberespionaje, para obtener una posición ventajosa sobre el adversario y todo ello bajo la dirección de un mando único al más alto nivel"[66].

Los espacios tradicionales y la guerra se han adaptado al contexto actual, por lo que ambos han creado un escenario bélico emergente con base en la transformación tecnológica que se ha presentado en los últimos años. La guerra sigue siendo la misma, lo que ha evolucionado es la manera de hacerla, así como los actores, los métodos y las herramientas.

2.2. Los ciberataques como herramienta de la ciberguerra

Las herramientas son esenciales para llevar a cabo las estrategias mediante los medios, como el internet, los ordenadores, software, etcétera, y técnicas, como el proceso y aprendizaje que se debe llevar a cabo para orquestar un ataque cibernético, que se emplean para poder cumplir los objetivos políticos, económicos, sociales, culturales y más, de quien lo hace.

Dentro del ciberespacio, como se mencionó con anterioridad, se utilizan distintos métodos para llevar a cabo las acciones equivalentes a la guerra en este escenario de confrontación, dichos métodos son herramientas y fungen como instrumentos para facilitar las actividades bélicas.

---

[65] De Izcue, Carlos, *Principios de la guerra* en *Apuntes de estrategia operacional,* Perú, División de publicaciones de la Escuela Superior de Guerra Naval, octubre de 2013, segunda edición, pp. 25-26.
[66] López de Turiso, Javier, *Ibíd.* p. 137.

Los ciberataques definidos en el capítulo anterior como:

"la explotación deliberada de sistemas informáticos, empresas y redes dependientes de la tecnología. Estos ataques utilizan códigos maliciosos para alterar la lógica o los datos del ordenador, lo que genera consecuencias perjudiciales que pueden comprometer información y provocar delitos cibernéticos"[67]

Son una de las herramientas más importantes que se utilizan en la ciberguerra. Dichos instrumentos fungen como un elemento en donde sus manejadores, los hackers, aprovechan las vulnerabilidades en las infraestructuras informáticas para entrar a los sistemas y, de esta forma, obtener información confidencial de distintas instituciones y Estados para usarlos en contra de éstos mismos o para adquirir poder mediante dicha información.

Los ciberataques son empleados por las partes en conflicto dentro del ciberespacio para obtener información confidencial y usarlo como instrumento de poder para sacar ventaja de lo adquirido o usarlo en contra de la victima de estos ataques para vulnerabilizarlo aún más y desmantelar la infraestructura informática.

Los Estados que utilizan los ciberataques mediante la contratación de hackers expertos en el tema, de acuerdo a la Unión Europea, "podrían interpretarse como un acto de guerra"[68], esto debido a que, como se mencionó con anterioridad, se ataca la infraestructura, sobretodo la crítica[69] de los Estados.

Es posible afirmar que, actualmente y, pese a la controversia que existió en donde se afirmaba que la ciberguerra aún no estaba presente en su totalidad dentro del espacio cibernético, este fenómeno ya existe y se encuentra en desarrollo.

El robo de información con el ataque cibernético lanzado por un hacker desde China hacia el Pentágono en Estados Unidos; el realizado a una planta nuclear en Natanz, Irán; así como los ataques de ramsomware ("programa de software malicioso que infecta tu

[67] s/a, *¿Qué es un ciberataque y qué tipos existen*?, [en línea], Valencia, Transformación Digital Cámara de Valencia, Dirección URL: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/#Que_es_un_ciberataque, [consulta: 24 de abril de 2019].
[68] IT User, "La UE declarará los ciberataques como acto de guerra, [en línea], IT User, 09 de noviembre de 2017, Dirección URL: https://discoverthenew.ituser.es/security-and-risk-management/2017/11/la-ue-declarara-los-ciberataques-como-acto-de-guerra [consulta: 10 de julio de 2019]
[69] /a, *Infrastructure Security, Ídem.*

computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema"[70]) WannaCry el cual afectó los servicios de seguridad social en Inglaterra, todos son ejemplos de hechos que han sido considerados como actos de ciberguerra, debido al impacto que éste tuvo en la infraestructura informática de los Estados afectados.

Dentro de la guerra deben existir actos con efectos asimilables al uso de la fuerza, es decir, que se den lugar actos de violencia para poder asegurar que se está en una situación bélica.

No obstante, y de acuerdo a lo expuesto por Antonio Segura en *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio,* se ha dado lugar el debate que consiste en considerar o no a los ciberataques como mecanismo para crear guerra, sin embargo, la resolución 3314 (XXI) de la Asamblea General de las Naciones Unidas respalda que los efectos que estén en consecuencia de comportamientos componentes a la agresión expuestos en el artículo 3 de la misma pueden abarcar medios cibernéticos.

Por tanto, si las consecuencias que se generan gracias a los ciberataques son perceptibles o igualables a lo que los efectos de una agresión mediante el uso de la fuerza en los medios tradicionales generan, es preciso afirmar que los ciberataques si son el método fundamental para llevar a cabo el acto bélico.

Los ciberataques son la herramienta esencial para realizar actos bélicos considerados como ciberguerra, puesto que no solo vulnera la infraestructura crítica de los afectados, sino que también trasgrede la seguridad de éstos, llevándolos a una desestabilidad y a un desequilibrio de poder.

2.3. El papel de los ciberejércitos en la ciberguerra

La ciberseguridad se ha convertido en un tema predominante para los actores que pretenden establecer un entorno de control para enfrentar la problemática en cuanto a los conflictos emergentes que se dan dentro del espacio cibernético. Para establecer las medidas adecuadas de ciberdefensa para el combate cibernético, los actores cuentan con distintas capacidades para enfrentar las ciberamenazas que son los ciberejércitos o

[70] s/a, *¿Qué es el ramsomware?,* [en línea], Kaspersky, Dirección URL: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware [consulta: 10 de julio de 2019].

cibermandos militares, los cuales analizamos con anterioridad, como la capacidad militar que se posee para la defensa del ciberespacio[71] , mismos que buscan la neutralización de las ciberamenazas desde su origen, es decir, implementan las estrategias que se instauran en términos de ciberseguridad para erradircarlas, esto mediante ciberoperaciones, las cuales pueden ser defensivas u ofensivas.

El papel de estos agentes en la ciberguerra es de suma importancia, ya que como en los demás dominios, existen fuerzas entrenadas y especiales para atender cada ámbito, por lo que cuentan con estrategias particulares para el combate dentro de éstos. En el caso de los ciberejércitos, tienen metodologías que se basan en la estrategia que los especialistas en el tema crean para evitar o contraatacar los ciberataques.

El desarrollo de la capacidad informática ha dado las competencias a las tropas cibernéticas para poder crear y ejecutar las estrategias adecuadas para defender y atacar las ciberamenazas.

De esta manera, los ciberejércitos son los protagonistas de la ciberdefensa dentro del espacio cibernético para proteger la infraestructura con la que cuentan los Estados y, para evitar un impacto aun mayor y con consecuencias más graves a futuro.

No obstante y, pese a ser la tarea principal de los ciberjércitos el tema de la defensa de su propia infraestructura cibernética, no todos defienden y contraatacan ante una ciberamenaza o ciberataque dirigido hacia los Estados de manera directa, sino que también existen ciberejércitos que solo se dedican al ataque, tal es el caso del ciberejército iraní.

El caso del ejército cibernético iraní consistió en ataques de *defacement*, que hace referencia al cambio, transformación o cualquier cosa que modifique una página web[72] con el objetivo de perjudicar de manera directa a ésta, hacia algunos portales de la red social Twitter, lo que generó cierto descontrol de éstos.

Los Estados han trabajado para poder crear y fortalecer sus ciberjércitos. Entre los más destacados se encuentran Estados Unidos, quien reunió a un grupo de hackers especializados que han sido entrenados para la lucha en caso de que se presenciara una

[71] Casar, Corredera, *El ciberespacio. Nuevo escenario de confrontación*, España, Centro Superior de Estudios de la Defensa Nacional, 2012, p. 240.
[72] Feliu, Luis, *La ciberseguridad y la ciberdefensa* en *El ciberespacio. Nuevo escenario de confrontación*, España, Centro Superior de Estudios de la Defensa Nacional, 2012, p. 51.

ciberguerra[73]. El ciberejército, o mejor conocido como cibermando estadounidense, es parte de la estrategia de seguridad dentro del territorio nacional, en la que las fuerzas armadas tradicionales como la fuerza área, marítima y el ejército forman parte, en conjunto, de este cibercomando en el que se especializan en ciberseguridad para poder combatir y erradicar las ciberamenazas. Cabe destacar, que es uno de los ciberejércitos que destacan por las capacidades con las que cuenta, pues además de desarrollar el plan integral en el que se plasma la logística y los recursos necesarios para sostener y proteger la infraestructura crítica del Estado, también proporciona asistencia al sector privado, así como la promoción de una armonización con otras agencias del gobierno federal para colaborar de manera conjunta[74].

Las iniciativas de ciberseguridad se sustentan en un presupuesto definido para el FY (Año fiscal) presente (2019) de $15 billones de dólares[75] para todas las actividades relacionadas a la defensa cibernética, entre las que destacan el sustento de los ciberejércitos. Sin embargo, se presume que cada año éste tiene un incremento de acuerdo a las necesidades que Estados Unidos tiene respecto al tema.

China cuenta con un ejército cibernético con el que ha querido ganar terreno dentro del ciberespacio, pues "tienen la capacidad para emplear armas electrónicas y de información para alcanzar a un adversario en otro continente"[76]. La capacidad con la que cuenta dicho ciberejército se basa en el *People´s Liberation Army*[77] que es un plan integral en el que se desarrolla una doctrina enfocada en la ciberguerra, y en el que se plasma la estrategia para el desarrollo de elementos entrenados en el tema para así formar el ejército cibernético correspondiente. Se puede destacar que el alcance de éste va desde la investigación en ciencia y tecnología, que es un complemento para fabricar productos relacionados a las TIC, hasta la cooperación con Rusia con el que se está implementando un programa de ciberguerra.

---

[73] Joyanes, Luis, Estado del arte de la ciberseguridad en *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, España, Instituto español de estudios estratégicos, 2010, p.33.
[74] The White House, *Cybersecurity funding,* [en línea], Estados Unidos, The White House, Dirección URL: https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf [consulta 15 de septiembre de 2019], p. 273.
[75] The White House, *Ibíd.* p.273.
[76] Sánchez, Gema *Ibíd.* p. 70.
[77] Pastor, Óscar, *et al., Seguridad Nacional y ciberdefensa,* [en línea], Madrid, Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones , octubre de 2009, Dirección URL: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf [consulta: 15 de septiembre de 2019], p. 126.

Actualmente, se desconoce de manera precisa el presupuesto destinado por la República Popular China en cuanto a ciberdefensa, no obstante, de acuerdo a lo plasmado en *Seguridad Nacional y Ciberdefensa* y a algunos reportes y declaraciones emitidos por Estados Unidos, se cree que el país de oriente está invirtiendo la mayoría de dicho gasto entre actividades de investigación y en personal técnico que se especialice en hackeo para llevar a cabo distintas funciones, entre las que se encuentra el ciberespionaje[78]

Por su parte, España y su Ejército de Ciberdefensa de las Fuerzas Armadas españolas, crearon el Mando Conjunto de Ciberdefensa (MCCD) el cual:

"es el órgano de la estructura operativa, subordinado al Jefe de Estado Mayor de la Defensa (JEMAD), responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudiera tener encomendadas, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional"[79].

y aplican una metodología más de ciberdefensa, empero, utilizan también el método de atacar los sistemas informáticos de aquellos que consideran como sus enemigos.

Al inicio de 2019, para cubrir todas las necesidades que se requieren en el tema en cuestión, el Ministerio de Defensa español recibió 4.608 millones de euros[80] para defensa, de los cuales una parte se utiliza para los gastos en investigación y renovación tecnológica para mantener en un alto estándar la cuestión de ciberdefensa. De dicho presupuesto, 900 millones[81] fueron destinados a mejorar la profesionalización de los Ejércitos que les permita tener una mayor preparación, dentro de éstos se incluye el Mando Conjunto de Ciberdefensa (MCCD), ciberejército español.

El ciberejército con el que cuenta Corea del Norte está establecido más para ofensiva que para defensa, pues se sabe que tiene a los hacker pertenecientes a su ciberejército trabajando en ataques que van dirigidos prioritariamente a Estados Unidos y Corea del

[78] *Ídem*.
[79] s/a, *Ciberdefensa,* [en línea], España, Estado Mayor de la Defensa, Dirección URL: http://www.emad.mde.es/ciberdefensa/ [consulta: 16 de septiembre de 2019].
[80] Herraiz, Pablo, "Presupuestos 2019: Defensa recibe 900 millones para mejorar la profesionalización del ejército", [en línea], *El mundo,* 14 de enero de 2019, Dirección URL: https://www.elmundo.es/espana/2019/01/14/5c3c79e5fdddff5d078b45a2.html [consulta 16 de septiembre de 2019].
[81] *Ibíd.*

Sur, quienes tienen sus propias fuerzas armadas cibernéticas, respectivamente. Asimismo, cuenta con la capacidad de atacar las infraestructuras financieras de Estados Unidos[82].

En este sentido, "Corea del norte invierte en sus fuerzas armadas aproximadamente una cuarta parte de su PIB. Por lo que parece sus constantes provocaciones y su actitud frecuentemente belicosa continuaran poniendo a prueba las alianzas regionales e internacionales que pugnan por preservar el equilibrio y la seguridad a nivel mundial"[83], por lo que una parte va destinada al ámbito cibernético, que más allá de enfocarse en la defensa de éste, lo utiliza para profesionalizar a su comando en ciberataques.

Otro que destaca es el ciberejército iraní, el cual, como vimos, tiene una estrategia completamente ofensiva, al igual que la mayoría de agentes de países que pretenden desmantelar la infraestructura, de manera particular, estadounidense. Además, cuenta con lazos desde el gobierno con Rusia e India, para evitar un aislamiento económico y tecnológico y, de esta manera, seguirse desarrollando en estos ámbitos. Es por ello que "Irán ha sufrido en la última década un proceso de apertura a las tecnologías de la información en respuesta tanto a necesidades militares como civiles"[84].

Irán con el negocio del petróleo ha destinado sus recursos en armas de destrucción masiva, armas avanzadas dentro de los dominios tradicionales y, sobre todo, en distintas tecnologías para ciberguerra. No obstante, el mayor interés que tiene el país iraní es la inversión a largo plazo en entrenamiento de los ciberejércitos y tener mayor acceso al llamado *know how* tecnológico[85]. Es por ello que se ha convertido en un enemigo potencial para Estados Unidos, debido a que se considera un país que tiene la capacidad de expandir sus herramientas tecnológicas para contender una guerra cibernética.

Muchos Estados, además de los mencionados, cuentan con ejércitos cibernéticos, sin embargo, es importante señalar que hay países que no cuentan con ellos, o bien, tienen sus capacidades limitadas debido a la cantidad presupuestaria que requiere preparar y sustentar este tipo de fuerzas armadas.

---

[82] Mateos, Iván, "Corea del Norte, la última apuesta nuclear", [en línea], *CISDE Observatorio,* 13 de septiembre de 2019, Dirección URL: https://observatorio.cisde.es/actualidad/corea-del-norte-la-ultima-apuesta-nuclear/ [consulta: 16 de septiembre de 2019].
[83] *Ibíd.*
[84] Pastor, Óscar, *et al., Ibíd.* p.137
[85] *Ibíd.* p.137.

Los ciberejércitos son los actores principales dentro de la ciberguerra, puesto que son los que llevan a cabo de manera práctica las estrategias planteadas por los líderes de los Estados, para llevar a cabo las acciones reconocidas como agresiones en el ciberespacio y su equiparación a la guerra.

2.4. Impacto jurídico, social y tecnológico de la ciberguerra en los Estados

El desarrollo del ciberespacio ha experimentado grandes avances, lo que ha generado gran dependencia por parte de los Estados y de las sociedades, llevándolo a tener un alcance global, en donde los ataques dentro de éste pueden ser originados desde cualquier parte del mundo.

La vulnerabilidad de los sistemas informáticos también se ha ampliado, puesto que pese a que exista ciberseguridad con estrategias ofensivas y defensivas, el entorno cibernético está en constante transformación, por lo que los métodos y medios para el ataque varían o cambian, por lo que la seguridad en el y del ciberespacio se ha convertido en uno de los puntos centrales de la comunidad internacional.

La ciberguerra ha modificado el contexto internacional, no solo por el entorno en el que se desenvuelve, sino también por el impacto que tiene en distintas áreas que afectan de manera directa las estructuras sistemáticas de los Estados.

En el apartado presente, se pretende dar a conocer el impacto jurídico, social y tecnológico, con un análisis de manera prospectiva con una relación de causalidad entre las acciones ofensivas y el impacto que se tiene de éstas, mediante hipótesis que se basan en la identificación de los efectos que se tienen cuando se traspasa la seguridad de los sistemas informáticos y que se ven reflejados de forma benéfica o perjudicial, principalmente, en las estructuras económicas, jurídicas y sociales.

La impresión que ha traído consigo los ciberataques que crean un ambiente hostil de ciberguerra, han generado, en palabras de María José Caro Bejarano:

“el temor a las catastróficas consecuencias de un hipotético «ciber-Katrina» o a un «ciber-11S» ha provocado que países como EEUU, Francia, Reino Unido, Israel y Corea del Sur, así como la ONU y la OTAN entre otras organizaciones, hayan tomado conciencia de la

importancia y necesidad de un ciberespacio seguro"[86], creando la exigencia de establecer marcos normativos.

La evolución y la aplicabilidad de distintos conceptos jurídicos ha sido uno de los impactos más notables en la guerra cibernética, pues ideas como soberanía, jurisdicción y uso de la fuerza, han sido adaptados a la regulación que distintos miembros del sistema internacional han propuesto y aplicado de manera interna como acción defensiva para un ordenamiento jurídico de acciones equiparables a la guerra en el ciberespacio.

"Throughout history, the international legal regime has adapted to technological advances, indicating that it both can, and must, continue to adapt and evolve alongside the everchanging realm of technology"[87].

No obstante, el efecto más enérgico al que se enfrentó, se enfrenta y se seguirá enfrentando el ámbito jurídico respecto a la ciberguerra es el enfoque del derecho de guerra y, como tal, del derecho internacional, puesto que es más asequible entender y aplicar su desenvolvimiento en un entorno físico en el que su conceptualización está definida por cuestiones geográficas, físicas y mayormente vinculables, a desarrollarlo y ejecutarlo en un dominio que consta de vulnerabilidades en su definición.

Los conflictos fungen como un elemento esencial para el impacto en el desarrollo de las sociedades presentes y las emergentes que se crean conforme se da el progreso en el contexto.

Socialmente, el efecto que provoca la ciberguerra es de lo más significativo, debido a las repercusiones que se reflejan cuando ésta ocurre.

La infraestructura crítica, a la que se le hizo alusión anteriormente, la cual ofrece los servicios que son elementales para sostener a la sociedad, es una estructura que pese a tener la protección adecuada contiene una serie de vulnerabilidades, por tal razón el impacto que generaría en un Estado debido a una ciberguerra sería representativo, ya que si se da lugar un ciberataque en dicha infraestructura, los servicios que le dan bienestar y estabilidad a la sociedad, tales como lo son lo de salud, educativos,

[86] Ministerio de Defensa, *Ibíd.* p. 80.
[87] Raboin, Bradley, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare", [en línea], Estados Unidos, Journal of the National Association of Administrative Law Judiciary, vol. 31, núm. 2, octubre 2011, Dirección URL: https://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=1013&context=naalj [consulta: 30 de julio de 2019], p. 659.

financieros, económicos, de energía, de transporte etcétera, serían afectados de manera directa la operatividad, interfiriendo en los sistemas que monitorean y controlan al Estado, generando un daño perjudicial no solo a la seguridad de las personas, si no a la seguridad de la nación.

El daño a la infraestructura critica "vulnerará el bienestar y los derechos de la comunidad, perjudicando los intereses particulares y comunes, afectando con ello el funcionamiento de los servicios críticos de la nación, lo que vincula esta infraestructura con el nivel nacional por sus posibles amenazas y efectos"[88]. Las repercusiones de ello pueden derivarse desde la pérdida de vidas humanas, u ocasionar graves daños a la población civil atentando contra su bienestar o el bien común de éstos, llevándolos al quebrantamiento, incluso, de su libertad y la obtención de los derechos básicos que se poseen.

Además, siendo la defensa nacional de todos los países como parte de la infraestructura critica, si ésta es violentada de manera similar que la sociedad, se puede transgredir su operatividad como un sector sensible y sumamente importante para la seguridad nacional.

Por su parte, los sistemas de comunicaciones también se ven afectados por las acciones que se presentan durante la ciberguerra, pues al ser los medios más endebles por la interconexión que existe entre sí, se llega al entorpecimiento para el control de éstos, creando una situación de desorden, lo que lleva a que distintos sectores del país no puedan llevar a cabo sus actividades, dando lugar a un estancamiento en el desarrollo del Estado y a una vitalidad económica afectada.

La tecnología es la base para las operaciones que se llevan a cabo dentro del espacio cibernético, por lo que el impacto es directo cuando se trata de ésta.

Los efectos se ven reflejados en la seguridad de ésta, puesto que al ser expuesta mediante las vulnerabilidades que son aprovechadas por los atacantes, la tecnología, como tal se vuelve insegura, y su operatividad se vuelve compleja y obstaculizada. De esta manera, se demanda el mejoramiento y la creación de infraestructura tecnológica que permita continuar con el desarrollo defensivo de ésta. Aunado a ello, se requiere un

[88] Marowski, Carl, *Efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica* en *La ciberguerra: sus impactos y desafíos,* Chile, Centro de Estudios Estratégicos de la Academia de Guerra Ejército de Chile, 2018, primera edición, p. 114.

entrenamiento más especializado para expertos en ciberdefensa que propicien un entorno sólido y totalmente resguardado de las ciberamenazas.

De esta forma, más allá del impacto tecnológico que se manifiesta en la necesidad de adquirir, mejorar y crear nuevas tecnologías que permitan responder y erradicar las amenazas cibernéticas constantes, también, se interfiere en una desestabilidad económica, debido a que ello exige una inversión aún mayor por el coste que la nueva infraestructura con personal experto requiere y, que en la mayoría de ocasiones, no puede ser sustentado por los Estados y los distintos sectores.

El impacto que genere la ciberguerra afectará en todos los ámbitos, lo que suscitará un panorama de incertidumbre, desconcierto y desestabilidad, que creará necesidades de ciberdefensa, estratégicas, técnicas, tecnológicas y jurídicas, con urgencia para proteger una infraestructura de control y no estancarse en una fluctuación constante de sus sistemas critícos, afectando de manera permanente el desarrollo político, tecnológico, social y económico de los Estados.

2.5. Consecuencias jurídicas de la ciberguerra dentro del sistema internacional

La nueva realidad que se está desenvolviendo en un contexto en cambio constante dentro del sistema internacional, se ha tenido que adaptar a la transformación tecnológica.

La ciberguerra se ha visto como un fenómeno que ha infringido y modificado los sistemas y, por consiguiente, ha alterado el desarrollo de las estructuras de los Estados que son sustentadas por dichos sistemas.

En el ámbito jurídico, estos cambios son sobresalientes, por lo que los requerimientos en dicha esfera se convierten en rigurosos, tal como lo describe Antonio Segura Serrano:

“la historia jurídica demuestra que como ha sucedido con todos los demás sectores, generarán –están generando ya- particulares exigencias jurídicas. Tiene sentido pensar que esas exigencias se aglutinen en torno a una nueva rama del Derecho, propia de Internet como principal elemento impulsor de la sociedad de la información”[89]

El impacto jurídico, como se hizo mención en el apartado anterior, ha sido de los más relevantes en el entorno bélico dentro del ciberespacio, pues se ha visto reflejado

[89] Segura, Antonio, *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio,* Granada, Universidad de Granada, 2013, p. 74.

directamente en el marco conceptual y regulatorio jurídico a nivel internacional, por lo que las consecuencias se derivan de éstos, debido a que el ordenamiento jurídico ha padecido de grandes modificaciones para habituarse al dominio que contiene una serie de retos en su aplicabilidad.

Las ciberoperaciones que se realizan para poder ejecutar, son las que han traído consigo mayores consecuencias en el ramo jurídico, puesto que, dichas operaciones son asimilables a una operación militar tradicional, mismas que se efectúan en la guerra clásica, lo que ha generado que la terminología del Derecho Internacional se adecue. “La existencia de un nexo entre la operación cibernética y una operación militar hará más probable la caracterización de esa ciberoperación como un uso de la fuerza”[90].

El concepto de uso de la fuerza, como se explica de manera precedente, y con base en la resolución 3314 (XXI) de la Asamblea General de las Naciones Unidas, en donde se incluyen todos los medios, incluso, los cibernéticos, es determinado para las operaciones cibernéticas, pues éstas son consideradas una metodología con el fin de ejercer una agresión mediante los ciberataques como su herramienta.

Respecto a lo anterior, María Pilar Llorens afirma lo siguiente, “este criterio busca analizar la vinculación entre el acto y las consecuencias”; por ende analiza la cadena de causalidad. Mientras mayor sea el vínculo entre la ciberoperación y las consecuencias, mayores serán las probabilidades de que sea caracterizada como un uso de la fuerza”[91].

Cabe destacar, que es complejo determinar cuando existe un uso de la fuerza dentro de este dominio, por lo que los efectos que se transmitan de una ciberoperación o, consecuentemente, del mismo ciberataque son los que precisarán de manera vinculante que actividades son uso de la fuerza.

Por otro lado, las operaciones cibernéticas tienen consecuencia en otra cuestión legal, respecto a la legítima defensa, el cual es un derecho que los Estados tienen para defenderse durante las actividades bélicas y, a lo que Llorens refiere como “cuándo los Estados podrán recurrir legalmente al uso de la fuerza para responder a una operación

[90] Llorens, María del Pilar, *Ibíd.* p.804.
[91] *Ibídem*.

cibernética"[92]. Por lo que el Artículo 51 de la Carta de las Naciones Unidas hace referencia a la legítima defensa:

"Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales"[93]

De esta manera, la ciberoperación cuando se considere como uso de la fuerza, dará lugar a que se ponga en pie el derecho a la legítima defensa. "De este modo toda ciberoperación que produzca una destrucción significativa de elementos de trascendencia del Estado atacado puede dar lugar al ejercicio del derecho de legítima defensa"[94].

Sin embargo, surgen ciertas controversias respecto al uso de la fuerza, pues destaca la idea de ataque armado, el cual está definido como:

"un acto o el comienzo de una serie de actos de fuerza armada de considerable magnitud e intensidad (escala) que tienen como consecuencia (efectos) la producción de una destrucción sustancial sobre elementos importantes del Estado atacado, como por ejemplo, la población, infraestructuras económicas y de seguridad, destrucción de aspectos de la autoridad gubernamental, esto es su independencia política, así como el daño a o la privación de su elemento físico, también denominado su territorio"[95].

Esto quiere decir, que se debe determinar a los ataques producidos durante una operación cibernética para poder implementar la aplicabilidad del derecho de legítima defensa, porque "todo ataque armado será un uso de la fuerza contrario a la prohibición, mientras que no todo uso de la fuerza será un ataque armado. Ello a su vez implicará que

[92] *Ibíd*. p. 806
[93] Naciones Unidas, *Carta de las Naciones Unidas,* [en línea], San Francisco, Naciones Unidas, 26 de junio de 1945, Dirección URL: https://www.un.org/es/charter-united-nations/index.html [consulta: 15 de noviembre de 2019].
[94] Llorens, María del Pilar, *Ibíd.* p. 807.
[95] *Ibídem.*

no todo Estado que sea afectado por un uso de la fuerza ilegal tendrá derecho a ejercer el derecho a la legítima defensa"[96].

De este modo, la controversia se enfoca en la infraestructura crítica, debido a que si ésta es afectada como consecuencia de un ataque cibernético derivado de una operación cibernética, entonces se considera como ataque armado, pues su alcance y los efectos que se produzcan concluyen en la destrucción sustancial sobre elementos importantes del Estado[97] , de acuerdo a la definición de ataque armado y, consecuentemente, se puede aplicar el derecho de legítima defensa.

No obstante, es complicado determinar que es o que no es un ataque armado realizado como ciberoperación, o bien, también deducir quién lo realizó, pues si éste fue hecho por un actor no estatal, se le puede atribuir a un Estado específico, dando lugar a poder hacer el uso de legítima defensa.

En otras palabras, el contexto y el desenvolvimiento de la ciberguerra va a delimitar tanto su concepción, como su situación, esto basándose en elementos manejados de manera tradicional.

Otra manera de describir lo anteriormente planteado, es retomar la idea de que el marco existente dentro el Derecho Internacional para regular los conflictos bélicos, es utilizable para las actividades en el ciberespacio que se equiparan a las de la guerra, lo que ha generado que el sistema internacional emplee dicho ordenamiento clásico a un contexto tecnológico emergente y pragmático, provocando un desequilibrio jurídico dentro del sistema.

En conclusión: ¿qué ha traído la ciberguerra al mundo virtual y real?

El ciberespacio ha dado lugar a una infraestructura totalmente interconectada, que ha llevado a una transformación en el modo en el que ésta se desarrolla. El contexto se ha modificado, dando lugar a la creación de uno que está en constante mutación.

Los conflictos también han adoptado el modo de actuar en el nuevo entorno, migrando a un nuevo escenario, el espacio cibernético, el cual les permite, debido a su

[96] *Ibídem*.
[97] *Ídem.* p. 807.

interconectividad, convertirlo en un escenario de confrontación, gracias a su operatividad que permite llevar a cabo acciones basadas en la estrategia y la táctica.

La ciberguerra es un fenómeno que ha estado sustentando los grandes cambios dentro del ciberespacio y dentro del mismo sistema.

Carl Marowski lo explica de la siguiente manera:

"La presencia de riesgos y amenazas de ciberguerra generan situaciones de vulnerabilidad que pueden afectar cualquiera de los componentes esenciales de la infraestructura nacional, perjudicando el funcionamiento de los sistemas de mando y control gubernamental y militar"[98].

En palabras más breves, Marowski supone una crisis de guerra, pues todo el sistema carece de un control que hace que se dé un desequilibrio, y se entra en una situación de inestabilidad, lo que lleva a una crisis en la propia estructura estatal y no se alcanza el desarrollo esperado.

Respecto a lo anterior, el impacto que la ciberguerra produce es significativo, pues como se expuso, se daña la infraestructura estatal y, posteriormente, esto influye en distintos ámbitos.

De manera particular, el efecto tecnológico no solo interviene en la parte técnica, sino también en lo económico.

En tanto, el daño más esencial se da socialmente, pues el Estado y la sociedad dependen de manera elemental de la infraestructura crítica, misma que da las bases de los recursos para sostener a la sociedad y amortiguar las necesidades de ésta. Cuando la infraestructura es quebrantada por la vulnerabilidad que presenta, el sistema colapsa, corrompiendo el bienestar de la población.

De esta manera, la infraestructura crítica se convierte en el principal objetivo de los ataques cibernéticos durante las hostilidades de la ciberguerra, debido al perjuicio que provoca, generando un impacto aún mayor en la sociedad y, por consiguiente, un descontrol estatal, provocando una mayor ofensiva por parte del Estado afectado.

[98] Marowski, Carl, *Ibíd.* p. 125.

Cabe destacar, que la afección a dicha infraestructura repercute de manera directa en la seguridad nacional, lo que crea una exigencia de capacidad de ciberrespuesta.

El 12 de mayo de 2017 se da un ciberataque, que se puede poner como ejemplo de la irrupción a la infraestructura crítica. El Servicio Nacional de Salud de Reino Unido, o mejor conocido como NHS, fue hackeado, utilizando una rama de software malicioso, es decir, un ransomware, el cual no tuvo nombre especifico, pero se manifestó como una variante del malware Wanna Decryptor.

El ataque afectó de manera simultánea tanto a ordenadores como a teléfonos celulares en 16 hospitales y centros de salud, en distintos lugares donde éstos se encontraban, como Londres, Nottingham, Herefordshire, Blackburn y Cumbria.

Lo que provocó la situación fue que "ambulancias fueron desviadas a otros hospitales"[99]; esto último fue la parte más delicada, puesto que esos desvíos era de personas que tenían que trasladarse a urgencias lo antes posible y fueron llevados a otros hospitales, no solo no siendo atendidos con esa calidad de urgencia, si no también que tardaron más en llegar, poniendo en peligro la vida de todos ellos.

Aunado a lo anterior, "el ataque ha obligado a apagar los ordenadores en diversos hospitales y los médicos han tenido que utilizar lápiz y papel, según testimonios recogidos por la BBC. Varios hospitales han tenido que cancelar citas y han pedido a los pacientes que eviten acudir salvo en casos de verdadera urgencia"[100].

Asimismo, un dato importante que es conveniente resaltar, es que en las pantallas de los dispositivos hackeados se mostraba un mensaje en el que se pedía una remuneración económica para poder obtener el acceso al sistema.

El Centro Nacional de Ciberseguridad del gobierno de Reino Unido, en conjunto con el Departamento de Salud y el Servicio Nacional de Salud comenzaron a actuar de manera rápida para controlar y erradicar el ataque.

---

[99] Smith-Spark, Laura, "Hospitales británicos también son blanco de ciberataque", [en línea], CNN, 12 de mayo de 2017, Dirección URL: https://cnnespanol.cnn.com/2017/05/12/hospitales-britanicos-tambien-son-blanco-de-ciberataque/ [consulta: 31 de julio de 2019].

[100] Guimón, Pablo, "Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero", [en línea], El País, 12 de mayo de 2017, Dirección URL: https://elpais.com/tecnologia/2017/05/12/actualidad/1494602389_458942.html [consulta: 31 de julio de 2019].

No obstante, la primera ministra Theresa May aseguró que el ataque no fue dirigido de forma directa al NHS, sino que éste fue canalizado para distintos países y organizaciones que también fueron afectados.

Con lo planteado anteriormente, respecto al ataque cibernético que sufrió Gran Bretaña, como parte de una estrategia para desmantelar un sistema nacional y, como pauta para responder y comenzar una guerra cibernética, se puede verificar que una agresión de esta índole direccionada claramente a la infraestructura crítica puede causar inestabilidad e incertidumbre, ya que el contexto tecnológico ha provocado que los sistemas más importantes en un Estado estén interconectados, de tal forma, que tanto el Estado, la población y su infraestructura informática sean interdependientes entre sí, dependiendo del sistema tecnológico, sin alternativas para el desarrollo lejos de éste y provocando, incluso, pérdidas estructurales y humanas.

La respuesta inmediata por parte de algunos países, como España, para resguardar la infraestructura crítica, dada la importancia de ésta, es la creación de un Centro Nacional de Protección de Infraestructuras Criticas, como responsable de la coordinación y supervisión en la ejecución de políticas y actividades que son planeadas de manera estratégica para preservar la seguridad en la infraestructura critica.

Empero, este tipo de organismos dedicados a ejercer estrategias en materia de ciberseguridad, no están presentes en todos los países, debido a la falta de presupuesto dirigida a estos ámbitos.

Las herramientas y los actores que participan en el desarrollo de una ciberguerra son circunstanciales, debido a que de ello deriva que las estrategias planeadas se den lugar del modo más preciso.

Aunque, contar con una estructura completa, estable y sustentable depende de las capacidades económicas con las que cuenten cada uno de los Estados, puesto que de ello dimana que los instrumentos, el mecanismo y la metodología sea apta para realizar actividades tanto para la ofensiva, como para la defensiva y aplicar el tema de ciberseguridad de manera superior a las amenazas y riesgos que se presenten.

Las operaciones cibernéticas que se llevan a cabo en el ciberespacio y en las que se utilizan los ciberataques como herramienta fundamental, han dado pie a distintas consecuencias jurídicas que la ciberguerra ha provocado y modificado en el modo de

regular de cada Estado, pero que también ha puesto en constantes dilemas y debates el marco jurídico del sistema internacional.

Cada Estado ha buscado combatir las ciberamenazas que suscitan las ciberguerras, pues como se ha descrito, tal como una guerra convencional, éstas traen consigo consecuencias que desestabilizan el desarrollo del Estado mismo y, por consiguiente, crean incertidumbre que genera, a su vez, un poder escaso y limitado para ejercer dentro del sistema internacional.

El combate de los Estados se basa en crear una estrategia jurídica, estableciendo normas internas que buscan ser vinculantes y que permitan reprimir, erradicar o contener los daños que devienen de la guerra cibernética. El marco regulatorio a nivel global, se ha querido adaptar a un ambiente hostil que se encuentra a poco alcance debido a su extensión extraterritorial, pues el ciberespacio existe y el sistema internacional se basa en éste para poder sustentar el desarrollo del mismo.

No obstante, cada Estado ha tenido que modificar su propio marco de regulación jurídica respecto a temas que tengan que ver con las acciones de ciberguerra realizadas dentro del espacio cibernético, ya que no existe una homologación en dicho marco, lo que ha provocado mayores desafíos en la aplicabilidad de éste con bases en el Derecho Internacional.

Asimismo, existe la ciberseguridad como área especialista en el tema y como complemento para apoyar en la aplicación de una normativa respecto al espacio cibernético, pero también se da la existencia de un marco regulatorio internacional basado en el Derecho Internacional deficiente por la ausencia de estandarización global en éste, lo que representa grandes retos para su aplicabilidad.

Lo expuesto en el presente capítulo, va a permitir comprender el entorno jurídico que rodea al ciberespacio con acciones equiparables a actividades de guerra dentro de éste, así como su falta de homogeneidad que representa uno de los mayores retos en el ámbito jurídico. Ello nos servirá de fundamento para continuar en los capítulos siguientes con el tema en cuestión.

CAPITULO 3. Desafíos jurídicos y tecnológicos para la aplicabilidad del Derecho Internacional en la guerra cibernética

La extensión que abarca el ciberespacio como dominio es difícil de delimitar, puesto que éste es un espacio indefinido, con una superficie en el que su alcance es irreconocible.

No obstante, al ser considerado un dominio existe una necesidad de regularlo, pese a los desafíos que éste presente, pues al tener un espacio no delimitado es complejo entender que y como se puede regular.

La regulación del ciberespacio se obstaculiza mayormente con la presencia de una ciberguerra dentro de éste, pues la migración de la guerra convencional a dicho entorno, ha generado un punto de inflexión dentro del sistema internacional, así como para el derecho internacional, mismo al que le ha causado una considerable complejidad para tener potestad sobre éste fenómeno, que si bien no es del todo nuevo, cada vez se desarrolla más, con nuevas tecnologías y, por tanto, con desafíos novedosos que requieren actualizaciones en el derecho internacional para confrontarlos y, si existe la posibilidad para erradicarlos.

Por lo anterior, es de suma importancia comprender el ambiente hostil que generan las actividades bélicas dentro del espacio cibernético, así como también, los retos que se presentan gracias a éstas.

El capítulo 3 se ocupa del estudio del marco jurídico regulatorio internacional en el ciberespacio, mismo que va a ser utilizado para mantener cierto orden en el ciberespacio como un ambiente amorfo. De igual modo, se explica la forma de regulación de la ciberguerra, el cual cuenta con una serie de lagunas jurídicas que van a demostrar su escasez y falta de potestad para tratar el fenómeno en cuestión. Por su parte, se brinda un análisis en relación a si el derecho de guerra tiene su aplicabilidad a la guerra cibernética.

Todo lo anterior para concebir y analizar los desafíos para el derecho internacional en relación a su aplicación respecto a una regulación jurídica ante los ataques cibernéticos dentro de los conflictos entre Estados, retos que han llevado a que la ciberguerra sea una manifestación compleja de confrontar debido a la falta de uniformidad y obligatoriedad de su relativa legislación.

3.1. Marco jurídico regulatorio internacional en el ciberespacio

El ciberespacio se ha convertido en un tema de enfoque para la comunidad internacional, debido al gran impacto que se da gracias a los fenómenos que se presentan dentro de éste.

Actualmente, existe un marco regulatorio que, si bien podría tener efectos importantes para el desarrollo de los conflictos dentro del ciberespacio, también cuenta con una serie de desafíos que se derivan de la falta de homogeneidad en dicho marco. En relación a esto, José María Molina Mateos menciona:

"De la definición de ciberespacio, de su estructura y naturaleza jurídica se deriva que existen normas vigentes que son de aplicación a determinados presupuestos fácticos que se dan en el ciberespacio, pero, al mismo tiempo se pone de relieve la insuficiencia normativa para otros y, en todo caso, se evidencia la ausencia del regulación del conjunto como ente autónomo y global"[101].

La regulación con la que cuenta el ciberespacio es compleja y cuenta con uniformidad nula en cuanto a que todos los países lo lleven a cabo de la misma manera o que al menos tengan alguna regulación universal del tema, como se refirió anteriormente, no obstante, existe dicho marco jurídico a nivel internacional, que está basado en otras regulaciones, que pueden ser base y complemento de éste y que se plasma en tratados internacionales. Asimismo, los países han creado su propio marco regulatorio que ha servido como fundamento para dichos tratados, pero también para crear unificación con otros países.

De esta manera el marco regulatorio que rige en el ciberespacio, como se hizo alusión anteriormente, tiene sustento, en su mayoría, en documentos que ya han sido escritos y que de manera precisa, algunos de ellos, no tienen enfoque en el ciberespacio pero pueden abarcarlo y, de esta forma, que definan la jurisdicción con ciertos limitantes en dicho espacio cibernético.

[101] Molina, José María, *Aproximación jurídica al ciberespacio,* [en línea], España, Instituto Español de Estudios Estratégicos, 08 de junio de 2015, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO57-2015_Aproximacion_Juridica_Ciberespacio_MolinaMateos.pdf [consulta: 15 de agosto de 2019], p. 11.

La regulación del espacio cibernético se establece desde que se creó una normativa de telecomunicaciones en distintas regiones y varios países del mundo, sobre todo en la Unión Europea.

Los tres elementos que se destacan de dicho ordenamiento y son descritos por Pablo García Mexiá en *El Derecho de Internet* dentro de *Ciberseguridad global: oportunidades y compromisos en el uso del ciberespacio,* pues se describe como una regulación totalmente imperativa, en donde su sustancialidad radica en:

1. La garantía de la libre competencia en la que se busca "salvaguardar los mercados de las telecomunicaciones, y con los que los operadores de internet deben necesariamente interactuar"[102].
2. La ordenación de recursos limitados en el que se considera como "patente, a la vista de la creciente escasez del ancho de banda o del espectro radioeléctrico, como consecuencia de la expansión de usos altamente intensivos de Internet"[103]. En este caso se contemplan los recursos limitados para video o música, por ejemplo.
3. Por su parte, como tercer elemento al que se le da alta relevancia, se toma a consideración la protección de los usuarios "especialmente si son finales y personas físicas, y aún con mayor motivo si, en este último supuesto, sufren algún tipo de desventaja social"[104]; respecto a esto último se toma en cuenta las discapacidades, por ejemplo. Con ello tomado como objetivo para crear medidas que han sido generalizadas por parte de la Unión Europea y algunas otras regiones que son avanzadas en el mundo, como el servicio universal de telecomunicaciones, la previsión de estatutos del usuario de servicios de telecomunicaciones, o la imposición a los operadores de determinadas obligaciones[105] que se realizó por motivos de interés general.

Haciendo referencia a las comunicaciones, en febrero de 1996 el Congreso de los Estados Unidos aprobó la Ley de Decencia en las Comunicaciones (Communications Decency Act), que tenía intención en cuanto a la protección de la infancia que "pretendía establecer un código de conducta en Internet en Estados Unidos, tratando de evitar la

[102] García, Pablo, *El Derecho de Internet* en *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio,* Granada, Universidad de Granada, 2013, p. 80.
[103] *Ibídem. p.80.*
[104] *Ibíd.* p.81.
[105] *Ibídem.*

presencia en la red de material que pudiera considerarse obsceno o violento. Entre otras cosas, se pretendía crear una lista de «palabras prohibidas» que no podían emplearse en chats, publicarse en páginas web"[106]. Sin embargo, ésta se interponía con la libertad de expresión, y distintas organizaciones de derecho cibernético, así como de derechos civiles llevaron a la ley ante un tribunal, misma que fue revocada poco tiempo después. Ello trajo consigo la creación, con la unión de grupos de defensa, del Global Internet Liberty Campaign (Campaña Global por la Libertad en Internet), o mejor conocido como GILC.

De igual forma, por iniciativa de John Perry Barlow, se creó la Declaración de Independencia del Ciberespacio, un manifiesto que "suponía una ruptura radical entre Internet y el sistema económico-político del mundo real"[107], pues declaraba una petición de libertad y de resistencia en cuanto a la autonomía del espacio cibernético con las palabras siguientes:

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear"[108].

Dicha declaración, junto a la Ley de Decencia en las Comunicaciones, marcaron la pauta para que se diera pie a estimular la creación de mayores regulaciones hacia el Internet, para que éste estuviese restringido y protegido y, posteriormente, ello se extendiera hacia el ciberespacio, siempre protegiendo a los usuarios, como objetivo fundamental.

De esta manera, ya existen normas procedentes de organizaciones internacionales, como las formuladas por el Consejo de Europa; normas que fueron emitidas por organismos

[106] s/a, *La ley de decencia en las comunicaciones y GILC,* [en línea], Estados Unidos, Biblioweb Sin Dominio, Dirección URL: https://biblioweb.sindominio.net/telematica/republica/node12.html [consulta: 13 de octubre de 2019].
[107] *Ibídem.*
[108] Perry, John, *A Declaration of the Independence of Cyberspace,* [en línea], Estados Unidos, Nomadas y Rebeldes, 08 de febrero de 1996, Dirección URL: https://nomadasyrebeldes.files.wordpress.com/2012/05/manifiesto_de_john_perry_barlow-1.pdf [consulta: 13 de octubre de 2019], p. 3.

supranacionales como la de la Unión Europea; así como también, normas creadas por distintos Estados, tanto por sus instituciones como entes territoriales.

Respecto a lo anterior, en noviembre de 2001 en Budapest, Hungría se creó el Convenio sobre ciberdelincuencia del Consejo de Europa, el cual entró en vigor hasta 2004, y plasma en su preámbulo el objetivo principal, el cual es:

"prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable;"[109].

Es así como tal Convenio es considerado como "un ejemplo de iniciativa regional y numerosos países prefieren aplicarlo únicamente como referencia dado que siempre será un instrumento de origen europeo"[110], para de ello impartir un marco mundial con una serie de normas que estén homologadas y armonizadas con las leyes de los Estados.

La Cumbre Mundial sobre la Sociedad de la Información (CMSI), fue parte de un proceso el cual provino de las iniciativas pensadas para la regulación en el ciberespacio, mismo que fue propuesto por el Consejo de la Unión Internacional de Telecomunicaciones (UIT) e impulsada por la ONU mediante patrocinio. Un rasgo importante a destacar es que se "incluyó por primera ocasión al sector privado como un actor esencial en el proceso"[111]. También, radica la importancia de distinguir los objetivos de la Cumbre como tal, los cuales consisten en:

"identificar visiones compartidas por los diversos actores, adoptar voluntades políticas, así como delimitar planes de acción tendientes a desarrollar la denominada sociedad de la información, ello, con el fin de establecer un marco global que permitiera hacer frente a los retos y desafíos que implica la sociedad de la información, de igual manera, también

[109] Consejo de Europa, *Ibídem*. Preámbulo.
[110] Touré, Hamadoun, *La búsqueda de la confianza en el ciberespacio,* Suiza, Unión Internacional de Telecomunicaciones, 2014, p. 20.
[111] s/a, *Fortalecimiento del marco de trabajo legal y regulatorio relativo al subcomponente de revisión del marco de trabajo regulatorio a la etapa de monitoreo 2011, Asociación Mexicana de Internet,* 2011, p. 33.

se pretendía identificar las oportunidades que la misma representa y aprovecharlas a fin de alcanzar diversas metas sociales enfocadas en el desarrollo de los Estados Miembros"[112].

Por lo que de esta manera se estableció una base ofensiva para todo aquello que impulse una desestabilización dentro de la sociedad de la información, misma que se desarrolla en el ciberespacio.

Asimismo, es importante señalar que la Cumbre se llevó a cabo en dos fases, la primera fue realizada del 10 al 12 de diciembre de 2003, en Ginebra, Suiza, en donde se planteó una Declaración de Principios y un Plan de Acción, que tiene como objetivos:

"construir una Sociedad de la Información integradora, poner el potencial del conocimiento y las TIC al servicio del desarrollo, fomentar la utilización de la información y del conocimiento para la consecución de los objetivos de desarrollo acordados internacionalmente, incluidos los contenidos en la Declaración del Milenio, y hacer frente a los nuevos desafíos que plantea la Sociedad de la Información en los planos nacional, regional e internacional. En la segunda fase de la CMSI se tendrá la oportunidad de evaluar los avances hacia la reducción de la brecha digital"[113].

Por su parte, la segunda fase tuvo sede dos años después, del 16 al 18 de noviembre de 2005, en la capital de la República Tunecina, en la ciudad de Túnez. El propósito de esta etapa era la de dar seguimiento a los temas de desarrollo pendientes y pactados durante la primer fase en Ginebra, en especial, los relativos a "la gobernabilidad de Internet y al financiamiento para la difusión y uso de las tecnologías de la información y las comunicaciones, con el fin de disminuir la brecha digital, principalmente, abordar la propuesta africana de un fondo de solidaridad digital"[114].

Derivado de lo anterior, y con la necesidad imperante de llevar a cabo los objetivos y el cumplimiento de lo plasmado en la CMSI, la Asamblea General emitió la resolución 63/202, en donde expresa:

---

[112] *Ibíd.* p. 33.
[113] Cumbre Mundial sobre la Sociedad de la Información, *Declaración de Principios y un Plan de Acción,* [en línea], Ginebra, Consejo de la Unión Internacional de Telecomunicaciones, 12 de mayo de 2004, Dirección URL: https://www.itu.int/net/wsis/docs/geneva/official/poa-es.html [consulta: 13 de octubre de 2019].
[114] s/a, *Fortalecimiento del marco de trabajo legal y regulatorio relativo al subcomponente de revisión del marco de trabajo regulatorio a la etapa de monitoreo 2011, Ibídem.* p.37.

“Recordando la Declaración de Principios y el Plan de Acción aprobados por la Cumbre Mundial sobre la Sociedad de la Información en su primera fase, celebrada en Ginebra del 10 al 12 de diciembre de 2003, que hizo suyos la Asamblea General, así como el Compromiso de Túnez y la Agenda de Túnez para la Sociedad de la Información, aprobados por la Cumbre en su segunda fase, celebrada en Túnez del 16 al 18 de noviembre de 2005, y hechos suyos por la Asamblea General,

Recordando también el Documento Final de la Cumbre Mundial 2005”[115].

Referente a ello, se destaca el propósito antes mencionado, en el apartado 9 de dicha resolución, que menciona lo siguiente:

“Alienta la cooperación reforzada e ininterrumpida entre las partes interesadas para garantizar la aplicación eficaz de los resultados de la Cumbre Mundial sobre la Sociedad de la Información en sus fases de Ginebra y Túnez, entre otras cosas, mediante el fomento de asociaciones nacionales, regionales e internacionales entre múltiples partes interesadas, incluidas las asociaciones públicas-privadas, y la creación de plataformas temáticas nacionales y regionales formadas por múltiples partes interesadas, en un esfuerzo común y un diálogo con los países en desarrollo y menos adelantados, los asociados para el desarrollo y los agentes del sector de las tecnologías de la información y las comunicaciones;”[116].

La idea de esta resolución, es fomentar el uso de las tecnologías de la información y las comunicaciones para utilizarlas a favor del desarrollo de lo convenido en la Cumbre. De esta forma, se convierte en un punto de inflexión para crear un entorno digital con mayor afluencia, sin embargo, esto plantea el punto de partida para crear un marco regulatorio del ciberespacio debido a tal concurrencia, puesto que, pese a ser una resolución con carácter no vinculante, es una opinión formal por parte de un cuerpo legislativo importante como lo es la Asamblea General, por tanto, se puede tomar como una base para fomentar el compromiso de llevar a cabo los propuesto en la Cumbre.

[115] Asamblea General de las Naciones Unidas, *Resolución 63/202. Las tecnologías de la información y las comunicaciones para el desarrollo*, [en línea], Naciones Unidas, 19 de diciembre de 2008, Dirección URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/63/202&Lang=S [consulta: 14 de octubre de 2019], p. 1-2.
[116] *Ibíd.* p. 3.

En 2003, durante la 32va. Conferencia General de la UNESCO, se aprobó la Carta sobre la Preservación del Patrimonio Digital, con la intención de preservar dicho patrimonio, el cual se entiende como "recursos únicos que son fruto del saber o la expresión de los seres humanos. Comprende recursos de carácter cultural, educativo, científico o administrativo e información técnica, jurídica, médica y de otras clases, que se generan directamente en formato digital o se convierten a éste a partir de material analógico ya existente."[117], por lo que la idea principal de dicha carta es la de preservar el patrimonio digital a través de la regulación[118].

Es decir, los datos que se manejaban con ambigüedad de manera análoga, migraron hacia lo digital, envolviéndose del contexto de la transformación que han tenido los medios hacia el entorno cibernético, por lo que de ello surge la necesidad de proteger lo migrado hacia éste, y al no tener una normativa vinculante de manera directa, se creó la carta para regular dicho patrimonio, puesto que al ser segmentado y solamente dirigirse a como tal el patrimonio digital, es una parte destacable y que forma parte de crear fundamentos para regular y, posteriormente, buscar la homologación de ello, misma que es inexistente.

Al respecto, de la limitante existente, y de la necesidad de enfocarse en un marco legal que se aborde para cuestiones referentes dentro del ciberespacio, se escribió una propuesta de Tratado Internacional en 2009, por el juez Stein Schjolberg y por la profesora S. Ghernaouti, la cual fue presentada mediante una publicación literaria llamada *A Global Treaty on Cybersecurity and Cybercrime* y expuesta en el Foro para la Gobernanza de Internet en Sharm El Sheikh. Dicha proposición plantea que es "A generic and global approach on main cybersecurity issues is presented from a strategic perspective"[119] que tiene como objetivo:

"to give a broad understanding of what kind of concerns should be addressed and what sort of measures should be taken within a national cybersecurity policy. This part also identifies some basic and non-exhaustive needs that should be taken into consideration at

[117] Conferencia General, *Carta sobre la Preservación del Patrimonio Digital,* [en línea], UNESCO, 15 de octubre de 2003, Dirección URL: http://portal.unesco.org/es/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html [consulta: 15 de octubre de 2019].
[118] *Ibíd.*
[119] Schjolberg, Stein; Ghernaouti-Helie, Solange, *A Global Treaty on Cybersecurity and Cybercrime,* AiTOslo, 2011, segunda edición, p. iii.

national and international levels when dealing with the establishment of a Global Protocol on Cybersecurity and Cybercrime"[120].

Para cumplir con lo anterior, se señala una primera parte que se determina como *Proyecto de Código de paz, justicia, y seguridad en el ciberespacio-un Tratado Global sobre ciberseguridad y cibercrimen (Draft Code on peace, justice and security in cyberspace- a Global Treaty on cybersecurity and cybercrime),* y en la que se plantea una serie de artículos tomados como medidas en derecho penal sustantivo y procesal, en relación a términos, acciones criminales, así como cuestiones de ciberseguridad dentro del ciberespacio.

De esta manera, esta formulación debe armonizar con la legislación de los países, así como con sus intereses, por lo que considerarlo como un Tratado internacional es complejo, sin embargo, se ha convertido en un punto crucial para poder crear un instrumento de gobernabilidad dentro del ciberespacio dirigido hacia la comunidad internacional.

El marco jurídico regulatorio internacional en el ciberespacio, como se presentó con anterioridad, es una legislación que, en su mayoría, está fundamentada en otras normativas, pero también ha servido como base sustancial para considerar la creación de una que sea uniforme y armónica con los miembros pertenecientes al sistema internacional, pues si bien existe, no es del todo vinculante, ya que se resaltan resoluciones, declaraciones, propuestas, etc. que tienen consistencia moral, pero no cuentan con obligatoriedad jurídica.

Es así como se genera la necesidad de crear normas que se vean directamente relacionadas a temas específicos, para darle un enfoque más directo y que de ello exista una mayor imposición, como lo es el de la ciberguerra, misma que requiere una legislación enfocada en prevención, combate, erradicación y, que también va a tener sus cimientos en el marco regulatorio internacional expuesto anteriormente, así como en otras legislaciones enfocadas en la guerra tradicional, pero igualmente, en la guerra desarrollada dentro del ciberespacio.

[120] *Ibíd.*

3.2. Regulación de la ciberguerra

La ciberguerra como una manifestación de la transformación tecnológica que afectó las relaciones de los Estados, es un suceso que pone en constante incertidumbre a los gobiernos y a la sociedad. Además, es un fenómeno que está en incesante cambio y genera un entorno de amenaza, lo que fomenta una necesidad de crear una reglamentación que se enfoque en regularla, puesto que de ello derivaría un mayor control de sus efectos.

Es importante destacar, que la regulación de la ciberguerra es más específica, respecto al marco jurídico regulatorio internacional, puesto como se indicó, éste último aún no cuenta con uniformidad a nivel internacional.

Los ciberataques como el del virus Stunext, que afectó directamente una planta nuclear iraní, así como la afectación al sistema eléctrico de Ucrania, incrementaron la necesidad de prevenir y erradicar los conflictos en el ciberespacio.

De esta manera, en 2001 se promulgó el Convenio sobre ciberdelincuencia por parte del Consejo de Europa, referido en el primer capítulo del presente trabajo, el cual es el primer tratado que se encuentra en la búsqueda de combatir los delitos cibernéticos y, que tiene como punto de enfoque principal el de crear "una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional"[121].

Asimismo, lo convenido en dicho documento lo consideran necesario:

"para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas , redes y datos informáticos, así como el abuso de dichos sistemas, redes, datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable;"[122].

[121] Consejo de Europa, *Ibídem.* Preámbulo.
[122] Consejo de Europa, *Ibídem.*

Es decir, el Convenio de Budapest busca enfrentar los delitos cibernéticos de manera legislativa, mediante la sanción cuando el delito ya ha sido cometido, pero también a través de la prevención para poder frenarlos a tiempo, para de esta forma entablar un entorno más seguro para la comunidad cibernética.

No obstante, el Convenio no es aplicable directamente a la ciberguerra, puesto que se enfoca en ciberdelitos y ciberdelincuencia, pues como se refirió con anterioridad, la ciberdelicuencia no es ciberguerra, a pesar de sus semejanzas, los actores son diferentes.

Sin embargo, el Convenio es un punto de partida para crear una normativa específica para la ciberguerra, pues no solo enfoca en erradicar los peligros que puedan exponer lo que existe en los sistemas, las redes y los datos informáticos, sino que también plantea una perspectiva en la que se dé lugar la cooperación internacional y, por ende, exista uniformidad en la reglamentación de la guerra cibernética. Esto último se puede apreciar en el Capítulo 3, sección 1 determinada como principios generales, el cual relata los Principios generales relativos a la cooperación internacional el cual dice:

“Las Partes cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capítulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos"[123].

Por lo que la cooperación internacional es un punto de inflexión para la normativa de ciberguerra, así como el Convenio de Budapest, como un fundamento, pero también como complemento para la misma legislatura.

Por su parte, el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (CCDCOE) publicó en 2013 el *Manual de Tallín*, o como su nombre en inglés lo indica *Tallin Manual on the International Law applicable to cyber wafare,* el cual fue realizado en 2008 en Tallin, Estonia, de ahí la derivación de su nombre.

El *Manual de Tallín* es una compilación de investigaciones, estudios y opiniones de un grupo de expertos reflejados en una normativa propuesta por estos mismos. Empero, es

[123] *Ibídem.* p. 14.

importante destacar que no es un documento vinculante, pero expresa la aplicabilidad del derecho internacional a los conflictos cibernéticos, así como a la ciberguerra, ello lo hace con un enfoque en el que, en primera instancia, identifica dicha aplicación del derecho internacional y, por consiguiente, plantea 95 normas que se brindan como propuesta para regir dichos conflictos cibernéticos. Cabe destacar, que éste se basó en la aplicabilidad de distintos tratados, entre ellos el Convenio de Budapest, previamente mencionado, así como también la Declaración de San Petersburgo de 1868 y la Convención de Ginebra de 1949.

De manera general, versa en el tema de soberanía y jurisdicción, así como en materia de derechos humanos, la responsabilidad de los Estados, la Ley de Neutralidad, lo referente al *ius ad bellum* y *ius in bello*, entre otras cuestiones que se relacionan con temas de guerra enfocados al ciberespacio.

Respecto a la idea de soberanía, es importante destacar el papel importante que se presenta en el *Manual,* pues como se mencionó en capítulos precedentes, en el ciberespacio no existe un área delimitada para ejercer autoridad, por lo que el alcance que tiene el poder bajo las condiciones de soberanía respecto al ciberespacio se basa en la idea de cibersoberanía o soberanía cibernética, la cual se mostró, de igual manera, con prelación, misma que es referida como "el derecho de los Estados a controlar Internet dentro de sus fronteras"[124], a lo que el Manual expone en el Capítulo 1, sección 1, la primer regla concerniente a como ejercer soberanía respecto a la infraestructura cibernética que se encuentra en su territorio, la cual dice:

"This Rule emphasizes the fact that although no State may claim sovereignty over cyberspace per se, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infraestructure"[125].

Es así como un Estado puede ejercer control sobre la infraestructura cibernética y las actividades siempre que se encuentren dentro de su soberanía territorial, por lo que en cuestiones de ciberseguridad y ciberguerra , el Estado puede actuar de forma ofensiva o

[124] Mallol, Eugenio, *Ibidem.*
[125] Schmitt, Michael, Tallin Manual on the International Law applicable to cyber warfare, [en línea], Cambridge University, 2013, Dirección URL: http://csef.ru/media/articles/3990/3990.pdf, [consulta: 28 de noviembre de 2018], p. 25.

defensiva para proteger su territorio soberano, mismo que en el ciberespacio es aquella extensión utilizada por cada Estado dentro del espacio cibernético.

En relación a la soberanía de un Estado y el cómo pueden ejercer su poder para lidiar con las actividades referentes a la ciberguerra, no obstante, para ello se debe atribuir relevancia a la jurisdicción que se tiene para poder impartir justicia por parte de los Estados dentro del espacio virtual que ocupan dentro del ciberespacio.

De este modo, el *Manual de Tallin* dedica la regla número 2 del Capítulo 1, sección 1, para explicar la aplicabilidad de la jurisdicción de los Estados respecto al espacio cibernético, en donde plantea lo siguiente:

"Without prejudice to applicable international obligations, a State may exercise its jurisdiction:

Over persons engaged in cyber activities on its territory

Over cyber infrastructure located on its territory; and

Extraterritorially, in accordance with international law"[126].

Asimismo, la extensión que abarca dicha jurisdicción es descrita en el artículo 2 de esa misma regla, que menciona:

"The principal basis for a State to exercise its jurisdiction os physical or legal presence of a person (in personam) or object (in rem) on its territory. For instance, pursuant to its in personam jurisdiction a State may adopt laws and regulations governing the cyber activities of individuals on its territory. It may also regulate the activities of privately owned entities registered (or otherwise bases as a matter of law) in its jurisdiction but physically operating abroad, such as internet service providers (´ISPs´). In rem jurisdiction would allow it to adopt laws governing the operation of cyber infraestructure on its territory"[127].

Como se puede apreciar, el ejercicio de esta jurisdicción se refiere a que toda acción que implique alguna actividad realizada por alguna persona, en este caso, comandada por un Estado para realizar actividades ilícitas en la infraestructura cibernética de otro Estado, éste último como afectado tiene la jurisdicción para llevar a cabo la regulación de dicho

[126] *Ibíd*. p. 27.
[127] *Ibíd.* p.27.

ejercicio anticonstitucional, debido a que dicha infraestructura le pertenece y, por consiguiente, es de su territorio y tiene la potestad para llevar a cabo las sanciones pertinentes.

Por otro lado, es circunstancial señalar que cada ciber operación que conlleve a una actividad ilegal dentro del ciberespacio y, que de ello deriven acciones equiparables a la guerra cibernética, son considerados ilegales y, por ende, se brinda la prohibición del uso de la fuerza pues se expone la integridad e, incluso, la independencia política de los Estados[128].

No obstante, para considerar que existe uso de la fuerza, el *Manual de Tallin* determina lo siguiente en la regla 11, Capítulo 2, alusivo al uso de la fuerza:

"A cyber operation consitutes a use of force when its scale and effects are comparable to non-cyber operations rising to level of a use of force"[129].

Por lo tanto, los efectos políticos, sociales, económicos y psicológicos que conllevan el desarrollo de una ciberguerra son equiparables a la escala y los efectos que las ciber operaciones, que son llevadas a cabo durante la guerra en el ciberespacio, a los que lleva una guerra convencional, por el alcance y la magnitud de sus consecuencias.

De tal manera, se puede actuar bajo la normativa que utiliza cada Estado para erradicar y sancionar el uso de la fuerza durante la guerra tradicional.

Es así como las ciber operaciones se posicionan como una estrategia de guerra en la ciberguerra. En referencia a esto, Schmitt en el Manual dedica la parte B, Capítulo 3, *The law of cyber armed conflict*, en especifico en *The law of armed confict generally,* a una propuesta de legislación para la ciberguerra. Empero, él lo nombra como conflicto armado, explicándolo de la siguiente forma:

"It has today replaced the term "war"for law of armed conflict purposes. As used in this Manual, armed conflict refers to a situation involving hostilities, including thos conducted using cyber means. The term takes on a different meaning for the purposes of characterizing international and non-international armed conflict"[130].

[128] *Ibíd.* p. 45.
[129] Ibíd. p. 47.
[130] *Ibíd.* p.68.

Ello lo específica para inferir en el papel de las ciber operaciones dentro de la guerra cibernética o conflicto armado, pues las "cyber operations executed in the context of an armed conflict are subject to the law of armed conflict"[131]; por lo cual, se afirma que "the law of armed conflict applies to cyber operations as it would to any other operations undertaken in the context of an armed conflict"[132].

Sin embargo, es fundamental enfatizar que el *Manual* engloba el precepto del conflicto armado, pues se declara que "the law of armed conflict does not embrace activities of private individuals or entities that are unrelated to the armed conflicto"[133], debido a que la ciberguerra se lleva a cabo solo entre Estados, de tal modo que la interferencia de una entidad privada debilitaría la jurisdicción y aplicación de la normativa directamente hacia la ciberguerra.

Asimismo, se deja en claro que la aplicabilidad de dicha legislación en cuanto a los conflictos armados, no va a depender de la calificación que se tenga de la situación bajo el principio de *ius ad bellum*, sino que debe existir una aplicación equitativa con la ley de conflicto armado[134], es decir, que la idea que plantea el *ius ad bellum* de hacer una guerra justa mediante razones legitimas de un Estado para poderse involucrar en cualquier guerra, se desvanece pues se debe estar sujeto a la ley de conflictos armados.

El Convenio de Budapest, así como el *Manual de Tallin*, entre algunas otras propuestas que hacen alusión a una regulación de la ciberguerra, son ejemplo de que hay una posibilidad desmesurada de que ello sea así. No obstante, el reto no está en que no exista la necesidad o que ésta se pueda cubrir, el desafío deriva en su armonización y posterior aplicabilidad de dicha normativa para cada una de las entidades estatales que conforman el sistema internacional.

De manera que, para que ello ocurra es fundamental comprender si la legislación tradicional vinculante o no vinculante compagina con la formulación de una legislación internacional para regular la guerra cibernética, tal es el caso del derecho de guerra y si su aplicabilidad hacia los conflictos en el ciberespacio.

---

[131] *Ibídem.*
[132] *Ibídem.*
[133] *Ibíd.* p. 69.
[134] *Ibídem.*

3.3. El derecho de guerra ¿aplicable a la guerra cibernética?

El derecho de guerra, como se hizo mención en el primer capítulo, se refiere a "las reglas bajo las cuales deben conducirse las partes que se encuentran en un conflicto armado"[135], es decir, que es la normativa que va a regir la guerra, y que tiene como fundamento el principio *ius ad bellum.*

Posterior a lo proclamado en el Ordenamiento sobre las Guerra Nacionales de la Haya de 1907, a los Convenios de Ginebra de 1949 y las dos guerra mundiales que ha vivido el entorno global, ha generado la evolución del derecho de guerra hasta convertirse en el Derecho Internacional Humanitario (DIH), mismo que hoy en día rige los conflictos armados.

Sin embargo, es de vital importancia acentuar en si el derecho de guerra o Derecho Internacional Humanitario es aplicable a la guerra cibernética, puesto que Laurent Gisel, especialista y asesor jurídico del Comité Internacional de la Cruz Roja (CICR), señala que "en el Manual de Tallin, los expertos jurídicos y militares afirman que el DIH se aplica a la guerra cibernética"[136], debido a que considera que es importante la reafimación que dichos expertos realizan respecto al DIH en relación a las nuevas tecnologías, ya que se estima de forma sustancial determinar las maneras en las que se limitan el potencial costo humanitario[137] que conllevan las operaciones cibernéticas durante los conflictos armados.

Basando tal análisis del *Manual de Tallin*, es imperante señalar la declaración de Gisel, ya que el Manual en el Capítulo 3, correspondiente a la Ley general del conflicto armado, expresa en la primer regla de manera decisiva que:

"despite the novelty of cyberoperations and the absence of specific rules within the law of armed conflict explicitly dealing with them, the International Group of Experts was unanimous in finding that the law of armed conflict applies to such activities in both international and non-international armed conflicts"[138].

---

[135] s/a, *El DIP de guerra* en Derecho Internacional Público, *Idem.*
[136] Gisel, Laurent, *El derecho de la guerra también impone límites a la guerra cibernética,* [en línea], Comité Internacional de la Cruz Roja, 01 de julio de 2013, Dirección URL: https://www.icrc.org/es/doc/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm [consulta: 02 de noviembre de 2019].
[137] *Ibíd.*
[138] Schmitt, Michael, *Ibídem.* p.68.

Es así como las actividades cibernéticas que deriven en un conflicto armado o ciberguerra, deben ser tratadas bajo el derecho de los conflictos armados, ó sea que se debe regir bajo el Derecho internacional Humanitario, debido a que, recapitulando, Schmitt en el Manual presenta a la guerra cibernética como sinónimo de conflicto armado y, por tanto, éste se rige con el derecho de guerra moderno o DIH.

Los principios generales del Derecho Internacional Humanitario establecidos ejercen su aplicabilidad a los conflictos armados tradicionales, sin embargo, también pueden y son aplicados ante la ciberguerra, esto debido a que en ambos casos las circunstancias, las necesidades y las consecuencias lo permiten.

Razón por la cual se destacan el Principio del derecho de Ginebra, Principio de inmunidad, Principio de prioridad humanitaria y Principio de distinción, los cuales concuerdan en la protección total de la población civil y la prioritización humanitaria, por lo que los ataques cibernéticos por parte de los Estados solo deben tener objetivos militares, tal como en la guerra convencional, en donde los ataques armados deben dirigirse hacia lo militar y, no deben comprometer, en lo absoluto, a la población ni bienes civiles[139], pues al embestir la infraestructura cibernética de un Estado, existe la probabilidad mayoritaria de afectar de manera directa a la comunidad civil.

Asimismo, el Principio de igualdad entre los beligerantes, el Principio de necesidad militar y el Principio de proporcionalidad tienen un nexo, pues en conjunto dan lugar al tomar ventaja sobre el Estado enemigo sin causar un mayor daño que el exigido por las propias hostilidades. De igual forma, debe existir una proporcionalidad cuando se lance el ciberataque, ya que debe ser correspondido cuando otro Estado haya realizado o amenace con hacerlo, todo ello bajo la normativa previamente establecida de que dicho ataque debe ser dirigido solo a objetivos militares.

De esta manera, es fundamental destacar el papel que tienen los hackers y si estos se convierten en objetivos militares al actuar a favor de una de las partes, pues la mayoría de los hackers son civiles, por lo que el Derecho Internacional Humanitario les da la protección como tal durante un conflicto, empero, al proceder a favor de una de las partes en conflicto dicha protección desaparece contra los ataques directos, puesto que, al

[139] Comité Internacional de la Cruz Roja*, Principios generales básicos del Derecho Internacional Humanitario,* [en línea], Comité Internacional de la Cruz Roja, Dirección URL: http://www.cruzroja.es/portal/page?_pageid=878,12647079&_dad=portal30&_schema=PORTAL30 [consulta: 02 de noviembre de 2019].

ejecutar acciones de ataque cibernético directas bajo dirección de una de las partes en conflicto y donde las consecuencias desemboquen en muertes de ciudadanos (otros civiles) o existan daños graves a las infraestructuras estatales se convierte, en automático, en un objetivo militar, ello basándose en el reconocimiento del *Manual de Tallin* de la legítima defensa , en este caso, de ciberataques.

Finalmente, el Principio de limitación de la acción hostil acentúa la toma de ventaja sobre el adversario, lo cual se puede realizar a través de los ciberataques pero éstos no pueden tener un alcance ilimitado, es decir, bajo algún arma o método, en este caso tecnológico, que pueda causar consecuencias o daños colaterales que afecten fuerte o permanentemente al otro Estado.

En conclusión, el derecho de guerra u, hoy Derecho Internacional Humanitario, si es aplicable a la guerra cibernética, empero, ello no limita del todo los ciberataques dentro de un conflicto armado, ya que aún se requiere una normativa específica, por lo que ésta se podría proponer *de lege ferenda*[140] para los conflictos armados en el ciberespacio, por lo cual el *Manual de Tallin* es el más asertivo en el tema, debido a que es una propuesta de *lege ferenda*[141] que incorpora el derecho convencional con las actividades bélicas que se generan en el espacio cibernético.

No obstante, al no ser un escrito vinculante carece de imperatividad legal. De este modo, surgen los desafíos para el derecho internacional, en relación a la aplicabilidad de una regulación jurídica ante los ciberataques dentro de la ciberguerra.

3.4. Desafíos para el derecho internacional para la aplicabilidad de una regulación jurídica ante los ataques cibernéticos dentro de los conflictos entre Estados

La ciberguerra ha marcado un punto de partida para tratar de comprender los nuevos conflictos en el entorno que, actualmente, se basan en la tecnología, misma que ha dado pie a nuevas herramientas de ataque y defensa que son utilizadas en las relaciones de los Estados, lo que permite realizar actividades bélicas tradicionales dentro del espacio cibernético.

---

[140] *De lege ferenda:* Con motivo de proponer una ley. La locución se usa por la doctrina para expresar la reforma o mejora aconsejable en una institución a través de la obra legislativa o parlamentaria. Cabanellas de Torres, Guillermo, *Diccionario Jurídico Elemental,* Perú, Libros Derecho, 2006, p. 133.

[141] *Idem.*

Es así, como el ordenamiento jurídico internacional se ha tenido que adaptar a los conflictos armados llevados a cabo en el afamado nuevo quinto dominio.

De acuerdo a apartados anteriores, se ha podido analizar y verificar que la normativa internacional, que rigen los conflictos armados en los cuatro dominios tradicionales, ha sido sometida a un ajuste para adaptarla a tales conflictos que han migrado al ciberespacio.

Sin embargo, tal regulación es una base para dicho ajuste, puesto que realmente no hay una legislación internacional específica para las cuestiones de ciberguerra en el ciberespacio, pese a que hay documentación como el *Manual de Tallin,* presentado con anterioridad, como una propuesta jurídica para las actividades bélicas equiparables a la guerra convencional en el ciberespacio. Es por eso que de ello derivan una serie de retos para el derecho internacional en cuanto a la aplicabilidad de una regulación jurídica ante los ataques cibernéticos en los conflictos que se dan entre los Estados, es decir, ciberguerra.

En primera instancia, uno de los retos que es fundamental para inferir en la aplicabilidad del derecho internacional en asuntos de guerra es lo referente a la concepción y definición de soberanía y jurisdicción dentro del ciberespacio.

En relación a la soberanía dentro del ciberespacio, es donde surge uno de los principales retos para poder aplicar una legislación, puesto que para exista la potestad de hacerlo se debe tener delimitado el alcance de ésta y eso se obtiene con la delimitación del territorio, sin embargo, como se hizo mención anteriormente, en el ciberespacio no hay determinación territorial, razón por la cual ninguna normativa puede interferir en algo que no existe de manera tangible. No obstante, si existe la posibilidad, de ser aplicada, pues al tener tal dificultad, la infraestructura critica funge como el territorio del Estado en el ciberespacio, pero no lo es, solo para efectos aplicativos, por tanto, si ésta es agredida, si puede existir una sanción, la cual va a ser regida bajo los Principios del Derecho Internacional Humanitario, empero, no va cubrir todo aquello que no esté dentro de éste y solo se refiera a cuestiones de ciberespacio y ciberguerra.

Aunado a lo que la soberanía refiere, es importante señalar la jurisdicción, misma que va de la mano con la falta de delimitación territorial, por lo que surge el desafío de

comprender como y en dónde aplicar dicha jurisdicción por las cuestiones de su alcance en un territorio que no tiene una soberanía explicita.

Por otro lado, la atribución y la responsabilidad que se tienen en un ataque cibernético durante la ciberguerra es complejo, debido a que se presentan dos situaciones en las que está implícita la responsabilidad del Estado. La primera, es aquella en la que las operaciones cibernéticas son llevadas a cabo por un órgano del Estado, el cual puede ser "un miembro que forme parte de un cuerpo o división cibernética de las fuerzas armadas de ese Estado o bien por un miembro de una empresa privada o una entidad paraestatal contratada por el Estado"[142]; en segundo lugar, tiene lugar cuando se da la contratación de una persona o grupo de personas[143]por parte del Estado para efectuar un ciberataque, que aunque no es producido directamente por el ente estatal, los contratados han recibido instrucciones o están bajo la dirección del Estado, por tanto, el suceso es atribuible a éste.

Sin embargo, de ambos casos surge el reto, pues si bien está explicito el modo de actuar del Estado, en el caso de la persona o grupo de personas contratadas, como lo son los hackers, el cual si bien se convierte en un objetivo militar de acuerdo a su actuar directo y a favor de una de las partes, como se expuso con anterioridad, no hay una definición concreta de que grado es requerido el control de éste para atribuirle la responsabilidad correspondiente, ya que su actuar debe ser comprobable, porque si ello no existe, entonces es sumamente amplio y subjetivo las responsabilidades atribuibles para el Estado y, en dado caso, para el ente contratado.

La Carta de Naciones Unidas en su artículo 2, apartado 4, hace hincapié en lo siguiente: "los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas"[144], de ahí que derivé la siguiente imposición para determinar la aplicabilidad del derecho internacional, puesto que existe un problema de entendimiento y mal interpretación, ya que no existe una definición del uso de la fuerza en dicha Carta, pese a que es un punto central dentro de ésta. Sin embargo, el artículo 39 declara que "El Consejo de Seguridad determinará la existencia de toda amenaza a la paz, quebrantamiento de la paz o acto de agresión y hará recomendaciones o decidirá

[142] Llorens, María del Pilar, *Ibíd*. p. 795.
[143] *Ibíd.* p. 796.
[144] Naciones Unidas, *Carta de las Naciones Unidas, Ibíd.*

qué medidas serán tomadas de conformidad con los Artículos 41 y 42 para mantener o restablecer 1a paz y la seguridad internacionales"[145], lo que da pie a que pueda existir una regulación basada en la idea del uso de la fuerza y lo estipulado en la Carta dentro del ciberespacio, pero las malas interpretaciones, como se recalca, aunado a que el Consejo de Seguridad solo emite recomendaciones, sustenta la idea de falta de coerción dentro del espacio cibernético.

Por su parte, uno de los desafíos más relevantes para el derecho internacional en cuanto a la aplicabilidad de una regulación jurídica ante los ataques cibernéticos dentro de los conflictos entre Estados es el que se ha estado mencionando durante el desarrollo del presente trabajo y es el de la falta de una regulación específica, homogénea y vinculante en la ciberguerra desarrollada en el espacio cibernético. Pues si bien existen documentos y tratados que son base para una legislación dentro de dicho entorno, no hay uno que sea uniforme para cubrir las demandas y necesidades que se requieren para enfrentar, controlar y erradicar una ciberguerra.

Destacándose, de esta manera, el *Manual de Tallin*, que si funge como un escrito que trata de cubrir los menesteres existentes en relación a la legislación de la ciberguerra, empero, solo es una propuesta por parte de especialistas en temas de legalidad, por lo que se requiere que ello se vuelva un documento que sea válido para el derecho internacional y, por consiguiente, para los Estados miembros del sistema internacional.

De lo anterior deriva que la legislación debe ser homogénea, esto quiere decir, que no esté dispersa en distintos documentos y que esté bien explicada para evitar malas interpretaciones, y que todos los Estados la lleven a cabo de manera uniforme, además, de que se trate de armonizar de manera general con la normativa de los Estados y del Derecho Internacional Humanitario, o al menos, sea acatada por cada uno de éstos, pues es complejo que los Estados acepten y se adhieran a una regulación que se interponga ante sus propios intereses.

Asimismo, que la regulación de la ciberguerra, como la propuesta del *Manual de Tallín,* o las resoluciones por parte de la Asamblea General de las Naciones Unidas, no sea vinculante, expone un reto para la aplicabilidad del derecho internacional en el tema, debido a que puede hallarse, pero al no ser vinculante impone un obstáculo para confrontar y sancionar las hostilidades, lo que en consecuencia podría frenar los efectos

[145] *Ibíd.*

irreparables que derivan de la guerra, lo que generaría una apertura mayor a continuar con las actividades bélicas, así como también consecuencias cada vez más graves de acuerdo al desarrollo de la tecnología con el paso del tiempo.

Es así que es conveniente señalar, que al no existir tan aclamada regulación, es necesario reconocer la importancia al tema de la ciberguerra y su legislación por parte de la comunidad internacional, puesto que con las nuevas tecnologías, la migración de la guerra se está convirtiendo en una situación comprometida para los Estados y otros actores que toman del ciberespacio las ventajas imprescindibles para dar lugar a acciones que puedan desequilibrar al sistema internacional, mismas que traen consigo desafíos para la aplicabilidad de una regulación jurídica ante los ataques cibernéticos dentro de los conflictos entre Estados.

Conclusión: Las necesidades de los desafíos en relación a la ciberguerra

El ciberespacio se ha convertido en el escenario idóneo para migrar los conflictos armados, utilizando nuevas herramientas mediante la tecnología que está en constante desarrollo, y que ha permitido que se tenga un fácil acceso a un entorno que puede llevar a un desequilibrio dentro de los Estados pertenecientes al sistema internacional.

Al ser considerado un dominio más, es indispensable que se determine un ordenamiento jurídico internacional que permita dar pie a una dinámica más estable dentro de este ambiente que se está posicionando como uno de los más cambiantes, pero sumamente indispensables para el contexto internacional actual.

La ciberguerra es un fenómeno que se ha posicionado como una nueva guerra, pues se adapta al entorno cibernético que se ha planteado en los últimos años, por lo que ésta es la manera contemporánea de hacer guerra. No obstante, de ello ha derivado un ambiente mayormente rígido, debido a las necesidades que han surgido por tratar de confrontar y solventar a la guerra cibernética y a sus consecuencias.

De esta forma, se han establecido una serie de normativas referentes al ciberespacio, la cual comenzó desde el establecimiento de la reglamentación en telecomunicaciones por iniciativa de la Unión Europea, a lo que se le sumó la expuesta por el Congreso de Estados Unidos con la aprobación de Ley de Decencia en las Comunicaciones que, a diferencia de la propuesta europea, ésta interfería con derechos como el de libertad de

expresión, que afectaban de manera directa a su aplicación, y que pronto tendría su revocación.

Aunado a ello, la Declaración de Independencia del Ciberespacio brindó una mayor autonomía a este entorno, lo que bien pudo disipar la idea de aislar la libertad, pero también trajo consigo una mayor exigencia para establecer regulaciones fundamentales para el su control.

Con la creación del Convenio sobre ciberdelincuencia del Consejo de Europa expedido en 2001, y entrada en vigor en 2004, se dio lugar a un proyecto de regulación internacional que pretendía mermar los delitos en el ciberespacio. Sin embargo, la problemática con la que cuenta es que solo se enfoca en ciberdelincuencia y los ciberdelitos llevados a cabo, omitiendo otro tipo de fenómenos y actividades que se pueden presentar dentro del espacio cibernético, como la ciberguerra.

De manera más asertiva, la Cumbre Mundial sobre la Sociedad de la Información, celebrada en dos años, junto a la resolución 63/202 emitida por la Asamblea General, funcionan como un punto de partida para fomentar un marco regulatorio del ciberespacio, pero su ausencia de obligatoriedad generan que solo sean fundamentos para un marco vinculante.

La ciberguerra como fenómeno dentro del ciberespacio y con consecuencias que provocan una gran transformación del sistema internacional, carece de un marco específico para la regulación de ésta, puesto que si existen ciertas normativas, que de igual derivan de otras reglamentaciones no vinculantes del ciberespacio, sin embargo, no hay una que trate el tema de manera directa y consistente.

No obstante, se dio lugar una propuesta de regulación, el *Manual de Tallin,* realizada por expertos jurídicos que brindan un panorama respecto a los conflictos armados en el espacio cibernético, y que buscan una normativa que regularice el asunto en cuestión, y que sea acatada por los Estados, así como unificada para su aplicación. Empero, ha subsistido meramente como proposición, por lo tanto, es requerido que se traslade a un documento que figure en un escrito que tenga legitimidad, así como que sea vinculante.

De igual manera, y aunado a lo anterior, es importante resaltar la idea de delimitaciones concretas en el tema, es decir, que en cuanto conceptos, ideas y aplicaciones de las normas se debe ser completamente claro y concreto a través de una determinación

exacta de todo ello, puesto que al carecer de delimitaciones precisas, se recae en redundancias y malas interpretaciones, por lo que la aplicabilidad se entorpece y se realiza a conveniencia de los actores estatales.

Un ejemplo de lo explicado en el párrafo anterior es el tema del uso de la fuerza, que de acuerdo al Manual de Tallin, no existe una definición acertada de la terminología, pero expresa lo siguiente:

"some cyberactions are undeniably not uses of force, uses of force need to involve a State´s direct use of armed force, and all armed attacks are uses of force"[146]

Por tal razón, se debe realizar un análisis detallado que se base en una previsión de las consecuencias que tendría la ciberguerra de acuerdo a los ataques cibernéticos empleados, para poder determinar si hay aplicabilidad de la terminología uso de la fuerza, basándose en ciertos criterios que deben ser fundamentados y definidos por la potestad correspondiente.

Asimismo, el Manual de Tallin explica que:

"it should be noted that the application of the law of armed conflict to cyber operations can prove problematic. It is often difficult to identify the existence of a cyber operation, its originator, its intended object of attack , and its precise effects. Still, these questions of fact do not prejudice the application of the law of armed conflict"[147], por lo que volvemos al tema de la delimitación de las actividades equiparables a la guerra en el ciberespacio.

Como se planteó con anterioridad, las propuestas de regulaciones hacia la ciberguerra han sido fundamentadas en ordenamientos presentados para espacios convencionales, es por ello que surgió la duda si el derecho de guerra como base para el control de los conflictos bélicos tradicionales, puede ser aplicable o no a la guerra cibernética, por lo que, dado el análisis planteado en este capítulo, se dedujo que si es posible su aplicabilidad gracias a las bases fundamentales del Derecho Internacional Humanitario, aunque solo puede ser de manera general, pues hay cuestiones de los ciberataques que no pueden ser regulados por el derecho consuetudinario que ofrece el DIH, si no que debe ser regulado por una normativa específica para ciberataques y ciberguerra.

[146] Schmitt, Michael, *Ibíd.* p. 49.
[147] *Ibíd.* p. 70.

Dicho marco es complejo y cuenta con una falta de homologación entre las propuestas y el derecho tradicional en el que se fundamentan, razón por la cual se ha convertido en un gran reto al derecho internacional en cuanto a la aplicabilidad de una regulación jurídica ante los ataques cibernéticos dentro de los conflictos entre Estados.

CAPÍTULO 4. Ciberguerra entre Estados: la estrategia de adquisición de poder

Durante décadas, los Estados han tratado de crear escenarios para llevar a cabo estrategias que los lleven a la adquisición de poder como una herramienta para la obtención de liderazgo dentro del sistema internacional, la ciberguerra es una manifestación por parte de los Estados para dar pie a dicha obtención.

De esta manera, la guerra cibernética que se da entre Estados es una estrategia de adquisición de poder, pues se crea para planificar el actuar de los actores y de esta forma medir los métodos y el impacto de las acciones derivadas de la situación bélica en el ciberespacio.

Debido a lo anterior, recae la importancia de comprender el modo de actuar de los Estados durante la ciberguerra, así como también la manera en la que actúan para prevenirla y disuadirla.

El capítulo 4 expresa un análisis que brinda una perspectiva del por qué los Estados usan la tecnología para hacer guerra, pues en ello recae el panorama que se vive en el contexto internacional gracias a los avances tecnológicos usados como herramientas para llevar a cabo acciones equiparables a la guerra en el ciberespacio.

Por su parte, se dan a conocer los casos de ciberguerra explicita y tácita de México, Estados Unidos, Francia y Reino Unido por ser los más conocidos en el ámbito cibernético y por la calidad y cantidad de ataques que han recibido y realizado respectivamente.

Asimismo, se presentan las estrategias de seguridad relacionadas al ciberespacio, así como las de ciberseguridad para afrontar la ciberguerra. Algunas de estas estrategias son expuestas en el ámbito internacional y regional, sin embargo, la investigación se centra en México, Estados Unidos, Francia y Reino Unido propiamente, debido a que son los más distinguidos en el tema en cuestión, y sirven para enlazar lo mencionado en los casos expuestos.

Lo anteriormente indicado se da lugar para analizar a los Estados en su accionar durante la ciberguerra y que de ello derive la idea de que existe una carencia sustancial de una regulación jurídica internacional, uniforme y vinculante, debido a que las estrategias son nacionales y regionales, pues como se presenta, las internacionales existen, pero no son como tal una legislación exclusiva para la ciberguerra.

4.1. ¿Por qué los Estados usan la tecnología para hacer guerra?

La guerra ha tenido una gran evolución en los últimos años, no solo por los distintos actores que convergen en ella, si no también, por el modo de realizarla, es decir, la estrategia, la táctica y las herramientas han impactado de manera directa en el modo en el que se realiza la guerra, ello gracias a la tecnología, misma que ha sido la base fundamental para la sofisticación de éstas.

No obstante, es imprescindible identificar el por qué los Estados usan la tecnología para hacer guerra, pues eso va más allá de la sofisticación mencionada con anterioridad, ya que de ello se va a determinar el modo de hacer guerra contemporáneo.

En principio, para responder a lo anteriormente planteado, se destaca la transformación en cuanto a transportes y armamento, pues la idea de ambas es para tener mayor movilidad, respecto al primero, pero también para tener un mayor alcance, precisión y potencia en cuanto a destrucción, aunque ello aplica más para el segundo.

Sin embargo, en la ciberguerra los transportes y el armamento, se mueven de manera diferente, pues si bien la tecnología se desenvuelve en el ciberespacio, éste va a ser el ambiente en el que se va a desarrollar el modo en el que se van a utilizar estos, puesto que, en este espacio se van a dar lugar una serie de movimientos técnicos, basados en codificaciones que van a utilizar las bases de datos para poder hacer uso del transporte y armamento en beneficio de quien lo lleve a cabo, por lo que a diferencia de la guerra tradicional, en la ciberguerra los Estados van a utilizar la tecnología a través del ciberespacio como un escenario para la estimulación de dichas herramientas.

En relación a lo anterior, con los avances tecnológicos en transportes, armamento y comunicaciones, los Estados buscan sacar ventaja de la tecnología para hacer la guerra y de ésta manera, tomar control en ésta. Lo hacen controlando cada una de esas herramientas a través del espacio cibernético. Ello se realiza para poder tener una estrategia y una táctica, pues se consideran importantes para poder sobrellevar y sacar ventaja durante la guerra. A lo que Fernando Pinto Cebrián señala:

“el uso militar de algunos avances tecnológicos de final de siglo en cuanto a transportes, comunicaciones, armamento y explosivos, estuvo presente en el pensamiento profesional

relativo a la estrategia y a la táctica, aprovechando las experiencias más recientes de su aplicación bélica"[148].

La estrategia es definida de dos maneras por la Real Academia Española, la primera hace referencia al "arte de dirigir las operaciones militares"[149] y, la segunda, menciona que es el "arte, traza para dirigir un asunto"[150]. Ambas hablan de un arte como capacidad para poder dirigir asuntos relevantes, no obstante, en la primera se enfoca de manera determinante en operaciones militares en donde la estrategia funge como algo fundamental para éstas.

De esta manera, Emigdio Contreras señala la estrategia como a "aquellas actitudes o acciones que están dirigidas a establecer una forma de pensar o de hacer las cosas"[151]. Por lo que tal definición es menos rígida, pues más allá de considerarlo como un arte, se enfoca en lo que se hace para el establecimiento de ideas pensadas para realizar acciones congruentes y asertivas.

Por su parte, la táctica es referida como el "procedimiento o método que se sigue para conseguir un fin determinado o ejecutar algo"[152], pero también existe la que se refiere a los fine bélicos, la cual dice que es el "conjunto de reglas y procedimientos que se utilizan para dirigir las operaciones militares que se llevan a cabo en una guerra"[153].

Por lo que hablar de estrategia en la guerra es apuntar a las habilidades, actitudes y capacidades que se tienen para dirigir y tomar decisiones desde la perspectiva militar, mientras que la táctica es el método con el que se van a realizar las actividades planteadas en la estrategia para llevar a cabo ésta con éxito.

Cabe señalar, que conforme al paso de los años y con los avances tecnológicos, tanto la estrategia como la táctica han ido evolucionando para adaptarse al nuevo contexto que está sumamente influenciado por dichos cambios tecnológicos, por lo que los Estados,

---

[148] Pinto, Fernando, *El concepto de "guerra moderna" y las nuevas ciencias y tecnologías de aplicación militar (siglos XIX y XX)* en *Guerra y tecnología. Interacción desde la antigüedad al presente,* Madrid, Centro de Estudios Ramón Areces, 2017, p.271.

[149] Real Academia Española, *Diccionario de la lengua española,* [en línea], Real Academia Española, 2019, Dirección URL: https://dle.rae.es/estrategia [consulta: 06 de diciembre de 2019].

[150] *Ibídem.*

[151] Contreras, Emigdio, "El concepto de estrategia como fundamento de la planeación estratégica", Pensamiento y Gestión, núm. 35, Colombia, Universidad del Norte, julio-diciembre, 2013, p. 158.

[152] Léxico, *Diccionario Léxico by Oxford*, [en línea], Léxico, 2019, Dirección URL: https://www.lexico.com/es/definicion/tactica [consulta: 06 de diciembre de 2019].

[153] *Ibídem.*

hoy en día, usan ésta para mejorar y crear sus estrategias y sus tácticas para aplicarlas de la mejor manera y a su conveniencia durante la guerra, así como también para hacer la guerra cibernética, pues de ello se puede sacar una ventaja aun mayor para poder enfrentar la guerra de manera exitosa sobre el enemigo, es decir, el otro u otros Estados.

En la guerra convencional y en la guerra cibernética siempre existe una razón por la cual los Estados las llevan a cabo, pues de ello deriva la motivación de continuar desarrollando estrategias, técnicas y tácticas para poder vencer al que consideran como su enemigo.

La tecnología es usada por los Estados para ejecutar grandes avances en armamento, comunicaciones, transportes, y todo tipo de herramientas para de ello modificar y perfeccionar de manera constante su estrategia y técnica usadas durante la guerra.

No obstante, una de las motivaciones principales es el poder, descrito en el capítulo 1 de esta investigación y, con base, en lo dicho por Joseph Nye como "the ability to affect other people to get the outcomes one wants. Some people call this influence, and distinguish power from influence, but that is confusing because the dictionary defines the two terms interchangeably"[154], el cual podría ser tomado como la capacidad o habilidad de influir en las decisiones que toman los demás.

Y si bien, se relaciona con temas de ciberespacio y ciberguerra, éste poder se transforma en cuanto a su desenvolvimiento, descripción y terminología, pues es llamado ciberpoder, que en dicho capítulo, Nye lo refiere de la siguiente manera "cyber power behavior rests upon a set of resources that relate to the creation, control and communication of electronic and computer based information -- infrastructure, networks, software, human skills. This includes the Internet of networked computers, but also intranets, cellular technologies and space based communications"[155], así como también, conceptualmente, lo menciona como "cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. In one widely used definition, cyber power is "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power." Cyber power can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace"[156]. Por lo que también

[154] Nye, Joseph, *Ídem.*
[155] *Idem.* p. 3.
[156] *Ídem.* p. 3-4.

existe una capacidad de influencia en cuanto a las decisiones pero en el entorno cibernético.

De esta forma, los Estados utilizan el poder en la guerra convencional, o ciberpoder para la guerra cibernética, para poder sacar ventaja competitiva antes, durante y posterior a éstas, ya que con la adquisición de poder los actores estatales pretenden conseguir superioridad por sobre el resto de los actores pertenecientes al sistema internacional, esto para que puedan liderar y tomar el control conforme a la protección de sus propios intereses y, de esta manera, tener supremacía en dicho sistema.

Los Estados usan la tecnología para hacer guerra porque pueden adquirir mayores conocimientos para el desarrollo de sus herramientas y metodologías, sin embargo, el motivo principal es la adquisición de poder como estrategia, pues de ello se tiene mayor preeminencia en el contexto internacional y así se da lugar una jerarquización dentro de éste basada en el poder, pues existe la competencia de dirigir e influenciar dentro de éste.

4.2. Casos de ciberguerra: México, Estados Unidos, Francia y Reino Unido

Los Estados pertenecientes al sistema internacional hacen la guerra con apoyo de la tecnología y lo que ésta les brinda.

La ciberguerra es un fenómeno proveniente de ello, desarrollado en un ambiente contemporáneo como lo es el ciberespacio, y que se desenvuelve gracias al progreso que ha tenido la tecnología.

En la actualidad han ocurrido casos de ciberguerra que se han dado gracias al desarrollo tecnológico enfatizado a lo largo de la investigación presente.

En el caso de ciberguerra en México es nulo, puesto que no existe como tal una guerra cibernética en la que el país sea protagonista, debido a que ello no se ha presentado, no obstante, si es vulnerable de que ello ocurra, ya que el país no se encuentra realmente preparado en materia de política y desarrollo tecnológico, pese a su esfuerzo por actualizarse en ello. A lo que se menciona que “el país, abundan en su justificación, es altamente vulnerable a ataques cibernéticos porque no existe un ente operativo de alto

nivel que coordine operaciones de ciberdefensa ante amenazas extranjeras o dentro del mismo territorio"[157].

En 2011 se habló de la posibilidad de una ciberguerra en México, la cual sería liderada por un grupo de hackers denominados como Anonymus Iberoamérica, quienes lanzaron un mensaje mediante la plataforma Youtube, en la que amenazaron a los integrantes de la organización criminal de Los Zetas, originada en Tamaulipas, donde darían a conocer todas sus operaciones así como todos aquellos vinculados externos a dicha organización.

Los ataques cibernéticos que se realizarían para cumplir con la amenaza, mismos que no estaban realmente sustentados ni cuidadosamente planeados, fueron determinados como Operación Cartel[158], misma que tuvo que ser cancelada debido a que uno de los hackers fue secuestrado por el mismo cartel, mientras que el resto del grupo recibieron una serie de amenazas.

Cabe señalar, que esta situación se llego a considerar como la probabilidad de una ciberguerra contra el narco[159], sin embargo, esa apreciación es errónea, puesto que la ciberguerra, se da únicamente entre Estados, de tal manera no podría considerarse así, ya que el narcotráfico es un actor no estatal, además de que, según el caso presentado, el Estado tampoco es quién hizo la declaración de la iniciativa Operación Cartel, si no fue un grupo de hackers, que hasta donde se conoce, son independientes.

Determinar una ciberguerra en México es complejo, puesto que pese a que se considere como tal, no lo es, porque hasta el momento no se ha dado de manera directa, en donde sea el Estado protagonista. No obstante, las vulnerabilidades con las que cuenta el Estado en su estructura cibernética lo hacen un objetivo fácil para cualquiera que quisiera atacarla.

A lo largo de la historia, México siempre ha fungido como intermediario y/o aliado de otros Estados, por lo que su papel es fundamental para todos los fenómenos ocurridos dentro del contexto internacional.

---

[157] s/a, "México se arma contra ciberataques", [en línea], México, Vanguardia, 20 de enero de 2016, Dirección URL: https://vanguardia.com.mx/articulo/mexico-se-arma-contra-ciberataques [consulta: 10 de diciembre de 2019].

[158] De los Reyes, Ignacio, "Lo que se sabe de una posible ciberguerra contra el narco en México", [en línea], México, BBC News Mundo, 02 de noviembre de 2011, Dirección URL: https://www.bbc.com/mundo/noticias/2011/11/111101_mexico_anonymous_zetas_opcartel_irm [consulta: 10 de diciembre de 2019].

[159] *Ibíd.*

Lo mismo ocurre cuando tiene lugar la ciberguerra en otros países. Un ejemplo de ello es el papel relevante que México tuvo y tiene en la ciberguerra entre Estados Unidos y Rusia, debido a su importancia como socio comercial y vecino de la nación estadounidense, ya que éste al ser blanco de ataques cibernéticos a su infraestructura, así como también a sus empresas, se dan lugar descensos económicos que afectan de manera directa a México, puesto que muchas de estas empresas tiene su base de producción en el país, lo que generaría una baja económica y comercial, perjudicando la inversión extranjera y, por consiguiente, la economía mexicana.

La ciberguerra referida con anterioridad entre Estados Unidos y Rusia está presente y comenzó con el ciber ataque a la red eléctrica ucraniana en 2015 comandado por piratas informáticos rusos donde un gran número de personas fueron afectadas al quedarse sin electricidad, por lo cual este ataque fue considerado como "el primer hackeo exitoso contra una red eléctrica en todo el mundo"[160].

Ello no tardo mucho en extenderse hacia Estados Unidos, donde en 2017 distintas compañías eléctricas, así como la planta nuclear Wolf Creek, ubicada en Kansas City, padecieron ataques cibernéticos rusos, lo que provocó que el país estadounidense comenzará un contraataque contra la red eléctrica de Rusia, aunque es importante señalar, que tales ataques no fueron reconocidos por el gobierno estadounidense, pero si se sabe que fue dirigido por el cibercomando de Estados Unidos, que está bajo la dirección del Departamento de Defensa desde su creación en 2009, tras una penetración imponente y exitosa a los sistemas del Pentágono en 2008 por parte de Rusia, y que se encarga de planear y ejecutar las estrategias de ciberdefensa y ciberataque de la nación.

No obstante, en 2018 se reportaron importantes ataques cibernéticos dirigidos a instalaciones estadounidenses, en especial a estados de la unión americana y empresas que se encuentran en el sector eléctrico y de agua, así como de energía nuclear, aviación, manufactura e instituciones comerciales, lo cual fue llamado como campaña de intrusión de múltiples etapas[161] la cual trataba de "insertar en redes de pequeñas instalaciones comerciales, colocar virus, realizar el reconocimiento de la red y recopilar información

[160] Lima, Lioman, "Estados Unidos vs Rusia: cómo el hackeo de las redes eléctricas se convirtió en un nuevo campo de batalla entre Washington y Moscú", [en línea], BBC News Mundo, 19 de junio de 2019, Dirección URL: https://www.bbc.com/mundo/noticias-internacional-48668879 [consulta: 15 de diciembre de 2019].

[161] *Ibíd.*

relacionada con los sistemas de control industrial estadounidense"[162]. Todo ello, dirigido bajo mando del gobierno ruso.

De esta manera, el gobierno estadounidense mediante su cibercomando y, apegándose a la Ley de Autorización de Defensa Nacional de 2018 que concede autoridad para la realización de actividades clandestinas militares, comenzó el contraataque a la infraestructura critica de Rusia, introduciendo un malware a través de ataques cibernéticos realizados a las redes eléctricas de las empresas e instituciones rusas del sector. Movimientos hostiles que hasta el año 2019 siguen vigentes y se espera su continuación.

Aunado a lo anterior, y lo que ha provocado un aumento de hostilidades entre ambos países, es la intervención de Rusia durante las elecciones de 2016 de Estados Unidos, donde Donald Trump resultó el candidato electo, misma que consistió en la irrupción en el sistema electoral estadounidense, lo que generó que los hackers informáticos lideraran las campañas que se realizaron en redes sociales, lo que impulsó a la victoria del ahora presidente estadounidense. Asimismo, hubo un pirateo de los correos electrónicos del Comité Nacional Demócrata, lo cual figuró para poder realizar una campaña que desprestigió a Hillary Clinton y a su equipo ante sus oponentes. Hecho que marcó no solo un punto importante de inflexión en la ciberguerra entre estas dos potencias, si no también dentro de Estados Unidos y su sistema político, así como de su posición ante el sistema internacional.

Cabe destacar, la importancia que hay entre la ciberguerra ocurrida entre estas dos potencias mundiales, no solo por el papel de suma relevancia que juegan dentro del sistema internacional, sino que también cuentan con dos de los sistemas energéticos más grandes del mundo, Estados Unidos solo por detrás de China como el mayor sistema y Rusia como cuarto detrás de India. Por lo que

"la red eléctrica de EE.UU., por ejemplo, es altamente compleja: está formada por unas 3.300 empresas de servicios públicos que trabajan en conjunto para proveer de energía a sus usuarios a través de unas redes de más de 320.000 kilómetros de líneas de transmisión de alto voltaje"[163].

[162] *Ibíd.*
[163] *Ibíd.*

Por su parte Rusia “cuenta con 20 empresas independientes de producción de energía, unas 440 instalaciones de generación, 496.000 subestaciones y unos 2,3 millones de km de líneas eléctricas”[164].

Es así como un ataque cibernético, mayor a los que se han ido presentando entre ambos actores, pueda llegar a controlar la magnitud de tales sistemas y podría tener consecuencias a gran escala, afectando no solo la infraestructura critica, sino también a la población, generando un desequilibrio no solo interno, también con sus Estados aliados, así como con sus socios políticos y comerciales.

Por otro lado, se habla de una ciberguerra fría, en la que las hostilidades no están declaradas de manera explícita entre Estados, como lo es la guerra fría cibernética de Estados Unidos y China, tal es el caso de Rusia, en donde ya existen una serie de ataques para desprestigiar, manipular y perjudicar la infraestructura critica de los involucrados.

El caso chino-estadounidense comenzó en junio de 2007, cuando la cuenta de correo electrónico perteneciente del ex secretario de Defensa de los Estados Unidos fue hackeada para sacar la mayor información correspondiente a lo relacionado con temas de seguridad del país norteamericano. El incidente fue investigado por las autoridades correspondientes del Pentágono, con un resultado negativo y sin haber pruebas contundentes, se concluyó de manera cuestionable que el ataque había sido realizado por el Ejército de Liberación Popular de China, a lo cual su gobierno negó el ciberataque.

A partir de entonces y con la creación del cibercomando estadounidense, el cual fue considerado como una amenaza por parte de los chinos, así como el Informe Mandiant emitido en 2013 por la empresa estadounidense de ciberseguridad, creada en 2004 con el mismo nombre, en el que plantearon que la Unidad 61398 del Ejército Popular de Liberación Chino[165] estaba estrechamente relacionada con el grupo de ciberdelincuencia ATP1, conformado por hackers, así como el ciberespionaje aplicado por ambas naciones, fueron el punto de partida en el comienzo de la ciberguerra fría entre Estados Unidos y

[164] *Ibíd.*

[165] Lejarza, Eguskiñe, *Estados Unidos- China: equilibrio de poder en la nueva ciberguerra fría,* [en línea], España, Instituto Español de Estudios Estratégicos, 01 de julio de 2013, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO60-2013_Ciberguerra_Fria_EEUU-China_E.Lejarza.pdf [consulta: 20 de diciembre de 2019], p. 7.

China basada en una carrera armamentística virtual[166], en donde ambos Estados han ido incrementando sus capacidades cibernéticas, que si bien aún no es oficialmente declarado, pueden verse como una preparación para una futura ciberguerra entre ambos.

La cuestión entre Estados Unidos y China es compleja, pues como lo describe Fernando Martínez Laínez, "China es un rival económico de EEUU, pero también principal proveedor y cliente, además de ser uno de los mayores acreedores de la deuda pública estadounidense"[167], por lo que hacer la guerra entre estos dos países traería un daño, no solo para sus infraestructuras criticas, sino también para sus balanzas económicas, pues los activos que ambos tienen como aliados podrían ser directamente perjudicados.

La situación de ciberguerra ruso-estadounidense, así como la chino-estadounidense son un claro ejemplo de cómo el avance tecnológico ha proporcionado herramientas que dan ventaja a los Estados para ejercer poder por sobre los otros y, de esta forma, llevar a cabo una lucha de poder dentro del sistema internacional en el contexto más reciente.

Francia junto con Alemania cuenta con una de las infraestructuras críticas más importantes del continente europeo, por lo que además de Estados Unidos se han convertido en objetivos relevantes para Rusia, pues para ésta "Europa es un objetivo más interesante, política, económica e ideológicamente"[168], dadas sus estructuras gubernamentales que influyen para crear estrategias de defensa rápidas para su ejecución y combate de las amenazas.

En 2015, la cadena televisiva TV5 monde, de porte mundial, fue hackeada por piratas informáticos, lo que provocó la caída de su señal durante un par de horas, así como también la afectación de su página de internet y sus redes sociales. El hackeo consistió en que mediante las pantallas se emitieran mensajes yihadistas, mientras que en las redes sociales se filtraron documentos que mostraron la identidad de varios miembros pertenecientes al ejército francés que supuestamente tuvieron participación en la guerra contra el Estado Islámico (IS). El daño palpable fue el económico, pues para reparar los

[166] *Ibíd.* p.18.
[167] Martínez, Fernando, "La guerra silenciosa", [en línea], España, Revista Española de Defensa, núm. 294, abril 2013, Dirección URL: https://www.defensa.gob.es/Galerias/documentacion/revistas/2013/red-294-ciberguerra.pdf [consulta: 20 de diciembre de 2019], p. 46.
[168] Martínez, Salvador, "Europa y sus elecciones, objetivo de la ciberguerra rusa", [en línea], El español, 10 de enero de 2017, Dirección URL: https://www.elespanol.com/mundo/europa/20170109/184732377_0.html [consulta: 20 de diciembre de 2019].

equipos perjudicados, así como el tiempo televisivo perdido, se utilizó un aproximado de 5 millones de euros[169].

Sin embargo, pese a que los piratas se identificaron como yihadistas las investigaciones de la Dirección General de Seguridad Exterior, la cual es la agencia de inteligencia de Francia, desembocaron en un grupo de hackers comandados por el gobierno ruso, quienes habían estado trabajando anteriormente mediante el ciberespionaje.

Aunado a lo anterior, la injerencia de Rusia en las elecciones de Francia de 2017, donde se emitieron los votos de manera electrónica, fue un punto clave para crear un ambiente hostil entre Rusia y Francia, pues el primero actuó de la misma manera que lo hizo con las elecciones presidenciales de Estados Unidos, hablando, incluso, de una "manipulación de resultados"[170].

Es importante destacar que Francia no está en una ciberguerra explicita con Rusia, pero los actos que se han suscitado si son acciones de guerra cibernética, así como de igual manera existen actos de ciberespionaje francés y acciones de ciberdefensa y ciberseguridad para combatir las ciberamenzas y ciberataques que se presentan. No obstante, no se descarta una ciberguerra declarada en un futuro no solo entre estos dos Estados, sino también entre distintos actores estatales pertenecientes al sistema internacional.

Por su parte, Reino Unido también contempla una ciberguerra con Rusia, debido a que el hackeo por parte de ésta se ha extendido hacia Europa, como se puedo observar con los casos de Francia, Alemania y Reino Unido.

Las constantes ciberamenzas por parte del gobierno ruso, llevaron a que el Centro Nacional de Ciberseguridad de Reino Unido y la Agencia de Seguridad Nacional de Estados Unidos elaboraran un investigación y, posteriormente, un informe en el que se acusa a un grupo de hackers llamados Turla y que, de acuerdo a éste, radican y operan desde Rusia, y han realizado distintos ciberataques a la infraestructura británica, poniendo en peligro su seguridad nacional. Informe que no fue ratificado por falta de pruebas contundentes.

[169] González, Enric, "Francia afirma que "no está a salvo" de ciberataques rusos contra sus elecciones", [en línea], Francia, El Mundo, 09 de enero de 2017, Dirección URL: https://www.elmundo.es/internacional/2017/01/09/58729cd046163fc8028b461a.html [consulta: 20 de diciembre de 2019].
[170] Martínez, Salvador, *Ibíd.*

En 2018, se filtraron una serie de documentos en los que se daban a conocer operaciones en contra de Rusia del organismo Integrity Initiative, el cual está financiado por el gobierno británico, así como el Departamento de Estado estadounidense, la OTAN y Facebook[171] razón por la cual se tiene un vínculo estrecho y por lo que se comprometería no solo a Reino Unido, sino también a Alemania, España, Francia, Grecia, Italia, Lituania, Montenegro, Noruega, Países Bajos y Serbia[172], países que fungen como colaboradores de dicho organismo.

Las tensiones entre Reino Unido y Rusia han ido aumentando, no solo por las constantes ciberamenazas que se dirigen entre un gobierno y otro, sino también debido a los distintos ataques cibernéticos que ha recibido el primero y que ha puesto en riesgo continuo la información más delicada y confidencial del gobierno británico, por lo que existe una gran posibilidad de una ciberguerra entre ambos Estados.

Rusia ha concretado una guerra cibernética latente, que si bien no ha sido expresada por los distintos Estados más que la expuesta por Estados Unidos, la nación rusa está en la mira de las potencias occidentales Francia y Reino Unido, quienes se unen a la nación estadounidense, tras el hackeo masivo llevado a cabo en 2018 por parte del gobierno ruso, y en el que se atacaron equipos con conectividad a internet, redes informáticas pertenecientes a organismos gubernamentales, así como de empresas de esas tres naciones. Asimismo, interfirieron en su infraestructura crítica, pues obstaculizaron los procesos de las redes de telecomunicaciones, de electricidad, agua, transportes y de las centrales energéticas[173], lo que ha generado una mayor tensión con Rusia, creando un escenario mayormente hostil en el ciberespacio.

Rusia se posiciona como un punto de inflexión en esta ciberguerra declarada con Estados Unidos y latente con otros Estados, puesto que se ha convertido en el protagonista tecnológico gracias a sus constantes ciberamenazas y ciberataques que ha llevado a cabo para desestabilizar la infraestructura de sus contendientes. De esta manera, los

[171] s/a, “Rusia tilda de “peligrosa” declaración de Reino Unido sobre supuesta ciberguerra”, [en línea], Moscú, Sputnik Mundo, 22 de noviembre de 2019, Dirección URL: https://mundo.sputniknews.com/politica/201911221089404403-rusia-tilda-de-peligrosa-declaracion-de-reino-unido-sobre-supuesta-ciberguerra/ [consulta: 22 de diciembre de 2019].
[172] *Ibíd.*
[173] Siula, Carlos, “Se desata ciberguerra contra Rusia por presunto hackeo masivo”, [en línea], Francia, El Sol de México, 18 de abril de 2018, Dirección URL: https://www.elsoldemexico.com.mx/mundo/se-desata-ciberguerra-contra-rusia-por-presunto-hackeo-masivo-1622398.html [consulta: 22 de diciembre de 2019].

Estados atacados y sus aliados desde hace tiempo y siempre con continuas actualizaciones han buscado crear y ejecutar estrategias de ciberseguridad para afrontar la guerra cibernética.

4.3. Estrategias de ciberseguridad para afrontar la ciberguerra: México, Estados Unidos, Francia y Reino Unido

La ciberguerra funge como una manifestación que se da entre los Estados que proviene del desarrollo tecnológico que nos ofrece el contexto internacional contemporáneo.

El constante incremento de las vulnerabilidades y amenazas respecto a las estructuras y sistemas de información, tecnologías y comunicaciones han dado pie a que los ciberataques sean factibles y fomenten un entorno hostil, llevándolo a convertirse en guerra dentro del ciberespacio.

Es por ello que los Estados han ido fomentando de manera conjunta y por separado estrategias de ciberseguridad para confrontar la guerra cibernética, que podrían ser un punto de partida para crear una estrategia de ciberseguridad que conlleve a la generación de una regulación jurídica vinculante, homogénea y armonizada, pues ello no se ha logrado debido a las limitaciones que las estrategias pueden llegar a presentar.

La idea de los países de crear estrategias de ciberseguridad es para prevenir, responder o, en su caso, disminuir el impacto de los ataques cibernéticos a los que se enfrentan y de esta manera, hacer más digerible el enfrentar una ciberguerra.

En el ámbito internacional, la comunidad de Estados pertenecientes al sistema internacional ha planteado una serie de estrategias y acciones que permiten llevar a cabo una cultura en materia de seguridad cibernética. Cabe señalar, que la mayoría de éstos se basan en el ya expuesto Convenio de Budapest sobre ciberdelincuencia de 2001. De igual forma, es importante destacar que el Manual de Tallin pronunciado en Estonia y emitido por orden de la OTAN, es considerado como preliminar que va a dar paso a la creación de una norma jurídica internacional que se encargue de las cuestiones respecto a la ciberguerra. Por lo que es el desenlace de las estrategias por parte de los países que han adoptado dicho manual.

Las distintas estrategias son ejecutadas y expresadas de distinta manera por parte de los países, desde planes de desarrollo, manuales, o algún documento escrito, hasta la creación de organismos que son utilizados para su realización.

Es así como es creado el NATO Computer Incident Response Capability o NCIRC, que tiene la capacidad de respuesta ante incidentes que se presenten en los países pertenecientes al Tratado. Lo que hace dicho organismos es "prevent, detect, respond to and recover from cyber security incidents"[174].

Por su parte, desde 2005 en Reino Unido se configuró el Proceso Meridian el cual tiene como objetivo "to exchange ideas and initiate actions for the cooperation of governmental bodies on Critical Information Infrastructure Protection (CIIP) issues globally"[175]. De dicho proceso deriva el Directorio Meridian, el cual es un directorio internacional que contiene organismos y agencias gubernamentales que tienen responsabilidad en la protección de infraestructuras criticas. Por lo que se podría considerar como una estrategia fundamental, pues la ejecución de dicho proceso en la Conferencia Meridian que se lleva a cabo cada año, no solo fomenta la cooperación, sino además busca la protección de una parte sustancial de las estructuras informáticas que es la infraestructura crítica, que como se mencionó anteriormente, si ésta es dañada el Estado puede sufrir graves consecuencias sociales, políticas y económicas.

Regionalmente, los Estados han creado estrategias expresadas de distintas maneras, entre ellas están los foros de colaboración entre los organismos que son responsables de la ciberseguridad.

Tal es el caso de FIRST (por sus siglas en inglés), que es el Foro Global de Respuesta a Incidentes y Equipos de Seguridad, y se considera "la principal organización y líder mundial reconocido en respuesta a incidentes"[176]. FIRST fue establecido para trabajar con los CERT´s, que son los Centros de Coordinación de ciberseguridad localizados en distintos países, por lo que la organización busca la cooperación y trabajar en conjunto en

[174] West, Ian, *Cyber Security*, [en línea], Estados Unidos, NCI NATO, Dirección URL: https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx [consulta: 26 de diciembre de 2019].
[175] s/a, *Meridian Process*, [en línea], Meridian Process, Dirección URL: https://www.meridianprocess.org/ [consulta: 26 de diciembre de 2019].
[176] s/a, *FIRST is the global Forum of Incident Response and Security Teams,* [en línea], FIRST, Dirección URL: https://www.first.org/ [consulta: 26 de diciembre de 2019].

la prevención de incidentes en relación a los sistemas informáticos que esten en organizaciones gubernamentales, educativas y comerciales[177].

El Sistema de Alerta Temprana de la Unión Europea opera desde 2012 y como su nombre lo indica alerta de manera prematura la detección de los ataques cibernéticos, lo hace con la identificación de los CERT´s gubernamentales y así "realizar un intercambio de información y solicitar colaboración en caso de la detección de un ataque que afecte a más de una nación"[178].

Del lado del continente americano, la Organización de Estados Americanos (OEA) con base en la Carta de las Naciones Unidas, y con el riesgo de una ciberguerra entre sus Estados miembro, planeó una estrategia que tiene sustento en programas de seguridad cibernética que consiste en "la presentación de una solicitud de procedimientos para la intervención y estrategia de la OEA"[179]. Tal procedimiento se realiza conforme a 10 medidas que se plantean y se sustentan en capacitaciones, talleres, asistencia técnica e intercambio de información para una mayor preparación para atender las incidencias en cuanto a ciberseguridad, mediante la colaboración mutua.

Pese a la iniciativa internacional y regional de los Estados por implementar medidas estables que confronten las acciones y consecuencias equiparables a la guerra en el ciberespacio, los actores internacionales han puesto en marcha sus propias estrategias de ciberseguridad para proteger sus propias estructuras informáticas.

México carece de capacidades militares para ejecutar actividades y operaciones en el ciberespacio, esto debido a las necesidades tecnológicas con las que cuenta. No obstante, ello no le ha impedido crear sus estrategias en ciberseguridad.

En 2016 y de acuerdo al Plan Nacional de Desarrollo 2013-2018 presentado durante el gobierno del ex presidente Enrique Peña Nieto, se fomentó la iniciativa de crear un Centro de Operaciones del Ciberespacio comandado por la Secretaría de Defensa Nacional (SEDENA), mismo que entraría en funcionamiento en 2018, sin embargo, el proyecto fue

---

[177] *Ibíd.*

[178] Segura, Antonio, *Ibíd.* p. 229.

[179] Carrillo, Leonardo; Vargas, Paola, *Ciberguerra: descripción de estrategias políticas internacionales y algunos planteamientos jurídicos para afrontarla*, [en línea], Bogotá, Universidad Militar Nueva Granada, 2016, Dirección URL: https://repository.unimilitar.edu.co/bitstream/handle/10654/16043/carrillofarfancesarleonardo2017%20%281%29.pdf?sequence=3&isAllowed=y [consulta: 17 de diciembre de 2018], p. 31.

cancelado por la falta de presupuesto que se usaría para la adquisición de nuevas tecnologías que ayudarían a llevar a cabo las operaciones en el ciberespacio.

No obstante, actualmente el Centro Nacional de Respuesta a Incidentes Cibernéticos de México (CERT-MX), creado tiempo atrás, en conjunto con la Universidad Nacional Autonoma de México (UNAM) y en colaboración con la Comisión Nacional de Seguridad (CNS) y la división científica de la Policía Federal, quienes han implementado la estrategia de ciberseguridad que previene y combate la ciberdelincuencia[180], monitorean y brindan respuesta a los ciberataques que recibe la infraestructura critica.

Las estrategias que se han implementado por parte del gobierno mexicano se cimentan en prevención y contención, como el Programa para la Seguridad Nacional (PSN) el cual tiene como fin desarrollar "acciones conjuntas de inteligencia de carácter estratégico y de atención, prevención, coordinación y seguimiento de los riesgos y amenazas"[181].

Así como también, la Estrategia Nacional de Seguridad de la Información (ENSI) con un enfoque mayormente técnico-administrativo pues tiene como objetivo sustancial el de "identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano"[182].

Por lo que dicha estrategia abarca mayormente el entorno público y político, brindando un mayor punto de enfoque para la seguridad. Empero, ello ha sido complejo, pues su implementación ha llevado mayores desafíos debido a su poca difusión y consistencia, lo que ha llevado una falta en la cultura de ciberseguridad entre los organismos y la población de México.

---

[180] Espinosa, Iván, "Hacia una estrategia nacional de ciberseguridad en México", *Revista de Administración Pública,* núm. 1, vol. L, México, Instituto Nacional de Administración Pública, 2015, p. 117.

[181] Secretaría de Gobernación, *DECRETO por el que se aprueba la Estrategia Nacional de Seguridad Pública del Gobierno de la República,* [en línea], México, Secretaría de Gobernación, 16 de mayo de 2019, Dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5560463&fecha=16/05/2019 [consulta: 27 de diciembre de 2019].

[182] s/a, *Estrategia Nacional de Ciberseguridad*, [en línea], México, Gobierno de México, 2017, Dirección URL: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf [consulta: 27 de diciembre de 2019].

México si ha implementado estrategias en temas de ciberseguridad, pero su carencia tecnológica así como la falta de brindarle importancia al tema han hecho que éstas no se lleven a cabo con los resultados esperados, por lo que se requiere reformular las estrategias para crear una como las desarrolladas por otros países.

Estados Unidos es uno de los países que más trabajan en sus estrategias de ciberseguridad, gracias a sus capacidades económicas y militares, esto no solo para evitar ciberamenazas y ciberataques, sino igualmente para que durante la ciberguerra tenga ventaja por sobre sus contendientes, ya que contempla una prospectiva de los conflictos en el ciberespacio.

En primera instancia, y desde 1992 la nación estadounidense ya pensaba en ciberdefensa mediante la estrategia, por lo que creó su Comando Estratégico (USSTRATCOM), creado por distintos comandos que en conjunto, como su nombre lo expresa fomenta la disuasión estratégica y, además, "tiene la responsabilidad de las "Operaciones de Redes de Ordenadores", es decir coordina las operaciones defensivas y ofensivas de las TIC del Departamento de Defensa"[183].

Una de las estrategias más relevantes de Estados Unidos para el combate de la ciberguerra fue la creación del Cibercomando en 2009 en donde se unificaron las Fuerzas Armadas de la nación estadounidense, el cual da lugar a las ciberoperaciones en el espacio cibernético.

En 2003 se promulgó la Estrategia Nacional para Asegurar el Ciberespacio, el cual podría ser la estrategia más completa en la materia, debido a que dentro de sus 3 objetivos cubre las necesidades que se requieren cubrir, pues estos plantean "el primero, prevenir los ataques contra la infraestructura crítica; el segundo, reducir la vulnerabilidad 38 de la nación frente a los ataques; y el tercero, minimizar los daños y agilizar la recuperación cuando estos ocurran"[184], lo que conllevó a la creación del Sistema Nacional de Respuesta que pretende mitigar los daños causados por los ciberataques, asimismo,

[183] Pastor, Óscar, *et al*., *Seguridad Nacional y Ciberdefensa*, Madrid, Isdefe, 2009, primera edición, p. 57.

[184] Rodríguez, Paola; Cordero, Yaneth*, Ciberseguridad: los acuerdos de cooperación para el tratamiento de las amenazas en el ciberespacio. El caso de Estados Unidos y China*, [en línea], Bogotá, Universidad de La Salle, 2018, Dirección URL: http://repository.lasalle.edu.co/bitstream/handle/10185/25117/64122001_2018.pdf?sequence=1&isAllowed=y [consulta: 28 de diciembre de 2019], p. 37.

busca identificar de manera rápida y eficaz las amenazas cibernéticas para poder actuar con respuestas favorables.

Aunado a la estrategia expuesta con anterioridad, se da lugar el Plan de Protección de Infraestructuras Nacionales (NIPP), el cual busca la protección de las infraestructuras nacionales, por lo que en éste entran la infraestructura critica, debido a que las estructuras informáticas están interconectadas de manera directa con las infraestructuras nacionales que brindan servicios esenciales o críticos.

La Estrategia para la Seguridad del Territorio Nacional se posiciona como una de las estrategias sustanciales, empero, es de importancia destacar que esta no es específica para temas de ciberespacio, pues en él:

"se reconoce la necesidad de gestionar cualquier evento de tipo catastrófico, desastres naturales o causados por el hombre, por las implicaciones que tiene para la seguridad del territorio nacional. El documento proporciona orientación a los departamentos federales y agencias que tienen algún rol dentro de la seguridad nacional, y ofrece sugerencias para los departamentos locales y organizaciones privadas de cara a mejorar la seguridad"[185].

Pero es adaptable al ciberespacio y la defensa contra la ciberguerra, pues conforme a los avances tecnológicos y las amenazas que se presentan en el entorno cibernético, mismo que ya es parte del territorio nacional de cada uno de los Estados, por lo que todo aquello que implique poner en riesgo la seguridad del territorio nacional, incluyendo lo que se desarrolle en dicho dominio, cabe en lo que describe la estrategia.

El Programa Einstein, por su parte, es un programa que desarrolla un proceso automatizado[186] para recolectar, analizar, relacionar y compartir información entre distintos organismos gubernamentales federales y, de esta forma, ampliar y reafirmar el conocimiento de la ciberseguridad en Estados Unidos, para que de ello se generen la estrategias adecuadas para actuar.

Otra que es esencial destacar es la Estrategia Nacional Militar de Estados Unidos de América de 2011, pues se enfoca en las capacidades militares en cuanto a redes, preparación y resistencia para disuadir y actuar en el ciberespacio.

[185] Pastor, Óscar*, Ibíd.* p. 58.
[186] *Ibíd.* p.66.

En cuanto a la Estrategia Nacional de Seguridad, como en todos los Estados, figura como la más importante para el país, pues pese a sus constantes cambios de 2008, 2010, 2015 y, la más reciente, 2018, así como también por el énfasis y relevancia que le otorga al ciberespacio y el constante peligro que existe de ciberguerra.

Respecto al tema, se enfoca en "asociación del sector público y el sector privado, intercambio de información y el avance en las capacidades tecnológicas"[187], pues la idea de unificar los sectores brindaría una mayor extensión para el desarrollo de la ciberseguridad y tener una cobertura aún mayor para frenar los ciberataques. Igualmente, la actualización constante en las capacidades tecnológicas ofrece mayores ventajas por la contemporaneidad en su arsenal cibernético.

La actualización de la Estrategia Nacional de 2018 tiene un cambio que representa la constante y rápida transformación que existe en el contexto tecnológico, pues ésta se orienta en las nuevas amenazas cibernéticas que se dan gracias a las tecnologías emergentes, como la Inteligencia Artificial (IA), pues ello daría mayores capacidades tecnológicas y militares a sus adversarios, como China, lo que pone en alerta a la nación estadounidense, e incita a que se invierta mayor conocimiento y esfuerzos a frenar y erradicar estas amenazas contemporáneas.

Estados Unidos es un país que dedica sus esfuerzos políticos, económicos y militares para la obtención de una Seguridad Nacional eficaz y eficiente, también lo hace para tomar ventaja por sobre sus contendientes para de esta forma conservar su liderazgo dentro del sistema internacional.

Francia es uno de los países que ha sufrido intervenciones a su infraestructura informática, por lo que dar pie a una cultura de ciberseguridad se ha ido convirtiendo en una prioridad.

Desde 1972 el gobierno francés dio a conocer el Libro Blanco, mismo que tuvo su última actualización en 2013, pues esto se realiza antes de cada nueva ley de programación militar y de seguridad interior[188]. que si bien no es una estrategia de ciberseguridad, es un estudio que centra su análisis en el área de ciberdefensa del país, así como un enfoque a

[187] Rodríguez, Paola; Cordero, Yaneth, p. 40.
[188] Presidencia de la República Francesa, *Libro Blanco sobre defensa y seguridad nacional,* [en línea], Francia, Presidencia de la República Francesa, 2013, Dirección URL: https://es.ambafrance.org › IMG › pdf › LIBRO_BLANCO [consulta: 28 de diciembre de 2019], p. 2.

los intereses de seguridad de manera global, y que con base en ello se cree una estrategia de seguridad nacional en relación a lo que plantea dicho libro, el cual menciona que “la estrategia de seguridad nacional se articula en torno a cinco funciones estratégicas que las fuerzas de defensa y de seguridad deben dominar: conocimiento y anticipación, prevención, disuasión, protección e intervención”[189].

En otras palabras, el Libro Blanco es un análisis precedente que se enfoca en tomar en cuenta el contexto nacional e internacional más recientes para con ello exponer las estrategias adecuadas que serán planteadas y ejecutadas en la estrategia nacional, para que de ésta manera, existan menores errores y mayor seguridad a la estructura gubernamental.

Cabe resaltar, que el Libro Blanco es aplicable a la ciberseguridad dentro del espacio cibernético, pues, como se mencionó, éste se actualiza conforme a las nuevas leyes militares y de seguridad, mismas que se adaptan también al entorno internacional.

Es así como desde 2010 la Estrategia de Seguridad Nacional de Francia se comenzó a enfocar en el ámbito digital, pues se pretendía crear una ciberdefensa capaz de prevenir los ciberataques. No obstante, tras el ataque cibernético a la cadena de televisión TV monde en 2015, se decidió crear la Estrategia Nacional Francesa para la Seguridad del Ámbito Digital, misma que cuenta con 5 objetivos fundamentales, resumidos en defensa y seguridad de los sistemas de información, enfocándose en la infraestructura crítica; protección digital de los datos personales, así como el de las empresas y la industria; siempre y aunado a lo anterior, con una total soberanía en el ciberespacio; asimismo, como la sensibilización de la sociedad respecto al tema digital[190].

Con ello Francia se posiciona como un Estado que tiene superioridad en cuanto a estrategia, debido a que es de los pocos países, junto a Reino Unido, que además de su estrategia nacional de seguridad, que tiene una parte enfocada a la ciberseguridad, hay una estrategia nacional que está orientada completamente a lo que ocurre en el entorno cibernético.

Por otro lado, para Reino Unido la seguridad nacional es un pilar sustancial, como lo es para Estados Unidos, pues han trabajado en ello desde mucho tiempo atrás, no obstante,

[189] *Ibíd.* p. 2.
[190] República de Francia, *Estrategia Nacional Francesa para la Seguridad en el Ámbito Digital,* Francia, República de Francia, 2015, p. 3.

con las actualizaciones se han impulsado estrategias acordes al contexto cibernético entre las que destacan la creación del Centro para la Protección de la Infraestructura Nacional (CPNI) en 2007.

La Estrategia de Seguridad Nacional de Reino Unido contempla una perspectiva concreta hacia el ciberespacio, mismo que se pretende por parte del gobierno que sea más "fuerte y seguro"[191], y lo hace promoviendo el Programa Nacional de Seguridad Cibernética, que pronto se reflejaría y establecería en la Estrategia de Ciberseguridad Nacional.

De igual manera, en 2007 se fomentó la Estrategia Nacional de Seguridad de la Información, que pretendía fortalecer la seguridad nacional para poder ejecutar una mejora en la protección de los sistemas informáticos y así evitar las amenazas. Empero, esta estrategia fue sustituida, debido a los avances tecnológicos, por la Estrategia de Ciberseguridad Nacional que abarca desde 2016 hasta el 2021, misma que trata 3 objetivos, defensa, disuasión y desarrollo en ciberdefensa[192]. Igualmente, se busca la cooperación internacional y alianzas que impulse progreso en cuestiones de ciberespacio para intereses económicos nacionales de Reino Unido.

Reino Unido con dicha estrategia que proporciona una prospectiva hacia el 2021 no solo pretende continuar obteniendo medios tecnológicos que les permitan ejecutarla, sino que igualmente están conscientes de la complejidad con la que cuenta el ciberespacio, puesto que consideran la rapidez con que el medio se transforma y las nuevas amenazas y fenómenos como la ciberguerra que eso puede traer.

Las estrategias figuran como elementos esenciales para crear planes y programas de seguridad nacional que puedan ser ejecutados de manera efectiva e, igualmente, con la obtención de grandes resultados que brinden una atmosfera segura para los Estados que llevan a cabo dichas estrategias para afrontar lo que la ciberguerra trae consigo.

Sin embargo, al ser pensadas de manera interna, no se genera un entorno de cooperación internacional que permita dar lugar a la creación de una legislación que no

[191] Carrillo, Leonardo; Vargas, Paola, *Ibíd.* p. 28.
[192]HM Goverment, *Estrategia de ciberseguridad nacional 2016-2021,*[en línea], Reino Unido, HM Goverment, 2016, Dirección URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643420/Spanish_translation_-_National_Cyber_Security_Strategy_2016.pdf [consulta: 05 de enero de 2020], p.6.

solo se enfoque en la ciberdefensa, sino también en la ciberseguridad y la sanción ante las consecuencias que la ciberguerra brinda.

Concluyendo la estrategia de adquisición de poder

Los Estados siempre buscan planificar los mejores métodos y estrategias que les permitan obtener ventajas competitivas dentro del sistema internacional, pues el liderazgo es una meta que se pretende conservar.

La ciberguerra no solo ha transformado al quinto dominio, es decir, el ciberespacio, mismo que es alterado de manera continua por los avances tecnológicos, sino también la manera en la que se desenvuelven las relaciones entre los Estados, pues la guerra contemporánea en un escenario moderno crea un ambiente hostil similar al que se genera durante la guerra tradicional, pero con una mayor incertidumbre por las nuevas herramientas que modifican constantemente. Es así como los actores de dicha ciberguerra tienen nuevas formas de hacer guerra.

De esta manera, los Estados usan la tecnología para obtener ventaja por sobre sus contendientes mediante los avances tecnológicos que son utilizados para llevar a cabo modificaciones avanzadas en comunicaciones, armamento, transporte y herramientas que son un pilar fundamental para poder generar las estrategias y técnicas adecuadas durante la guerra para dirigir y liderar las hostilidades a su conveniencia en relación a sus intereses.

Por lo que la tecnología y todo aquello que ha sido transformado por ésta, es aprovechado por los actores estatales del sistema internacional para realizar acciones equiparables a la guerra en el espacio cibernético, pues la guerra ha migrado al quinto dominio.

Estados Unidos, Francia y Reino Unido han sido protagonistas de ciberataques que los han llevado a generar un ambiente bélico sumamente hostil por su capacidad de respuesta.

Estados Unidos, es uno de los países que cuenta con grandes e importantes estructuras informáticas que controlan los servicios sustanciales del país, además de su capacidad como potencia económica, por lo que es un blanco sustancial para sus enemigos. Al ser una de las naciones con robustez en cuanto a red eléctrica y siendo uno de los servicios

principales para la infraestructura critica del país, ésta se ha convertido en un objetivo de ataque para Rusia, misma que, como se expuso en el texto presente, ha realizado distintos ataques cibernéticos que detonaron una guerra en el ciberespacio con la nación estadounidense, lo que ha llevado que ésta última plantee una ciberdefensa con base en la respuesta hacia las redes eléctricas rusas y otras estructuras importantes, declarando la ciberguerra más contundente en el contexto internacional actual.

China, por su parte, es otro actor en el contexto de ciberguerra estadounidense, pues si bien la guerra que existe entre ambas naciones es tácita e, incluso, es una ciberguerra fría, fundamentada en una carrera armamentística virtual[193], con un incremento progresivo de sus capacidades cibernéticas, y en la que solo hay ciberamenazas por ambas partes, puesto que los ciberataques orquestados por ambas naciones no han sido demostrados con pruebas convincentes.

Además, el convertir la ciberguerra fría en una guerra explicita daría lugar a grandes afectaciones económicas y políticas que derivan de la competencia y su asociación comercial.

En el caso de Francia y Reino Unido se está en un riesgo palpable de ciberguerra con Rusia, que es el protagonista de los ciberataques y ciberamenazas constantes a las potencias europeas, por lo que el verdadero adversario que se convirtió en una amenaza es la nación rusa.

La situación de México difiere de los casos anteriores, sin embargo, no es tan distinto de ellos, debido a que en realidad no existe una ciberguerra del Estado mexicano con algún país, pero su relación estrecha e independiente con Estados Unidos da paso a que los daños que se deriven de una ciberguerra con afectaciones a las estructuras informáticas del país estadounidense perjudiquen directamente a nuestro país por la inversión extranjera privada que tiene Estados Unidos.

Por lo que la independencia mexicana hacia el país norteamericano ha fomentado que una parte importante de la economía y la política se basen en las acciones de Estados Unidos, por lo que podría ser acertado decir que la ciberguerra de Estados Unidos con otros Estados podría convertirse en la de México directa o indirectamente.

[193] Lejarza, Eguskiñe, *Ibíd.* p.18.

Con base en sus experiencias, tanto los Estados como algunas Organizaciones Internacionales han realizado estrategias enfocadas en la seguridad y protección de los países respecto al tema del ciberespacio y la ciberguerra.

Como en los casos ya presentados, los planes y estrategias de ciberseguridad se han priorizado en los Estados, más aún en los que han sufrido ciberataques y estén en guerra como es el caso de Estados Unidos, o proceso de comenzar una, como el resto de los casos expuestos, debido a que éstos hacen que la situación bélica pueda ser prevenida, priorizada, disuadida e, incluso, erradicada, por lo que es de suma importancia que la estrategia de seguridad nacional de los países esté íntimamente relacionada con las estrategias que se generan en torno a la ciberseguridad.

Asimismo, es relevante que estas estrategias estén orientadas más hacia la prevención, pues al evitar una ciberguerra hay la posibilidad de que no existan tensiones entre los Estados, así como tampoco cree un ambiente hostil dentro y fuera del ciberespacio.

No obstante, esto es una propuesta idealizada, ya que para los Estados realizar ataques no tiene gran impacto, jurídicamente hablando, puesto que al no existir la regulación jurídica internacional adecuada y correspondiente no hay sanciones que realmente puedan prevenir dicho escenario bélico, por lo que se da lugar a mayores desafíos para el Derecho Internacional en materia de espacio cibernético, además, de los grandes avances tecnológicos que crean mayores posibilidades para realizar las actividades referentes a la guerra en el ciberespacio.

Conclusiones

La organización estructural política y social ha sido cambiada gracias al contexto tecnológico que se ha desarrollado conforme a las alteraciones que han surgido de éste, lo que ha llevado a configuraciones diversas dentro del sistema internacional y de los actores pertenecientes a éste mismo, pues la tecnología que ha intervenido en dichas modificaciones se plasma en herramientas tecnológicas y medios digitales que han dado lugar a que los pertenecientes a dicho sistema realicen la adaptación para la obtención de ventajas competitivas entre ellos y, de esta manera, la adquisición de poder como una meta particular para éstos.

El ciberespacio, lugar donde se albergan las transformaciones tecnológicas, se ha convertido en un escenario vital para los actores del sistema internacional, puesto que no solo se utiliza para el proceso tecnológico, sino también para realizar actividades que han interferido de manera directa en la interrelación entre dichos actores.

De esta forma, el espacio cibernético es un escenario que ha adquirido relevancia por el papel que juega en las distintas manifestaciones políticas, jurídicas y sociales que se cimientan en las relaciones entre los Estados.

Asimismo, también las complicaciones que existen dentro de éste se basan en su territorialidad, pues de ello deriva la controversia porque ésta es amorfa, sin una forma definida, y emitir un criterio respecto a la soberanía y la jurisdicción es complejo, puesto que la primera requiere de una delimitación territorial, por lo que surge la adaptabilidad antes mencionada, en donde el concepto se ajusta al contexto cibernético, llamándolo cibersoberanía, que tiene como deficiencia solo el control de internet[194], mientras que el ciberespacio abarca mayor contenido; en tanto, la segunda es referida a la ejecución de autoridad por parte de un actor especifico en un territorio que está delimitado, por lo que la utilización de ambos conceptos en un escenario como el espacio cibernético conlleva a una serie de retos para su aplicación por la necesidad de entablar la delimitación territorial que es inexistente de manera general, pero ello depende de cada Estado que de manera interna tenga dicha demarcación.

La aplicabilidad de lo anterior es necesaria para manifestaciones que emergen de las relaciones entre los Estados, como la ciberguerra.

[194] Mallol, Eugenio, *Idem.*

La ciberguerra es un fenómeno que se presenta entre los Estados y es la forma contemporánea de hacer guerra con un escenario diferente, entendido como el quinto dominio, apoyado de herramientas tecnológicas, como los ciberataques, que son utilizados para realizar las actividades bélicas.

Los Estados utilizan la tecnología no solo por los avances que ésta les da en cuanto a sus herramientas físicas y cibernéticas, sino porque ésta les brinda esa ventaja competitiva que se ha planteado para poder obtener éxito en su objetivo principal, la adquisición de poder que les brindaría liderazgo, dominio, potestad y jurisdicción dentro del sistema internacional, que les permita controlar las decisiones de éste para llevar a cabo la construcción de una estructura estatal propia que los lleve a la satisfacciones de intereses nacionales y propios.

Dicha manifestación bélica conlleva a que el entorno cibernético se encuentre en constante amenaza, en especial cuando se trata de la infraestructura critica, como base sustancial para la sociedad, por lo que los Estados están en una búsqueda continua de dar pie a la habilitación y desarrollo de su ciberseguridad y ciberdefensa para que no solo exista la prevención, sino que también, en caso de ser atacados, se dé lugar a la respuesta y la resolución de las controversias.

Lo anterior, se ha realizado con base en el Derecho de guerra o, como actualmente se conoce como Derecho Internacional Humanitario, mismo que ha sido acondicionado a la guerra cibernética, que si bien si puede utilizarse para algunas cuestiones de tal guerra, se contemplan huecos jurídicos debido a, como se planteó con anterioridad, la soberanía y jurisdicción que tienen complicaciones para ser utilizado en el conflicto cibernético, así como también por las herramientas, como los ciberataques, que requieren de una regulación concreta.

Es así como la guerra cibernética supone un desequilibrio basado en una carencia de control dentro del sistema internacional, puesto que no hay una estructura estatal sustentable y eso frena el desarrollo deseable, lo que deja que las consecuencias que se dan como en la guerra convencional, tengan mayor impacto negativo en la estructura económica y social.

También jurídicamente se presentan dichos desafíos, pues esta parte se ha vuelto un reto relevante para la aplicabilidad del Derecho Internacional en la guerra cibernética, ya que

ésta carece de un marco regulatorio oficial, internacional y vinculante, que si bien si hay la existencia de regulaciones que se derivan de otro tipo de normativas referentes a la guerra convencional o a temas envueltos en el ciberespacio, no son vinculantes y tampoco tienen consistencia con la ciberguerra.

El *Manual de Tallin* es una propuesta de regulación que tiene cimentación en conocimientos de expertos jurídicos que buscan crear una normativa en la materia, basados en un panorama respecto a las actividades equiparables a la guerra en el ciberespacio.

No obstante, como se mencionó, es una propuesta que no ha sido efectuada como una legislación legitima por parte de los Estados, que pese a estar muy bien sustentada, a ser consistente y abarcar lo referente al tema en cuestión, no se armoniza con la legislación interna de cada Estado o ¿con sus intereses nacionales?, así como con la de algunos tratados y resoluciones que se contraponen a lo planteado.

Además de que se destaca la vulnerabilidad del *Manual,* pues éste recae en redundancias y malas interpretaciones en cuanto a conceptos, ideas y aplicaciones, por lo que se requiere analizar y perfeccionar para que no se preste a inconsistencias y se ejecute una aplicabilidad adecuada y eficiente.

Ahí radica el mayor desafío para el Derecho Internacional en cuanto a la ciberguerra, pues para su regulación la concepción de homologación, unificación, homogeneidad, entre otros sinónimos, no ha sido posible, así como también aquella que se relaciona con la armonización de leyes entre el Derecho Internacional y el derecho interno de los Estados.

Los Estados han trabajado en lograr su ciberseguridad y lo han hecho mediante la creación de tratados y resoluciones internas, así como mediante la asociación con otros Estados, que en ocasiones, como la Unión Europea, se han transformado en cuestiones regionales.

Igualmente, han creado estrategias y acciones de seguridad cibernética que buscan la prevención, disuasión y, en algunos casos, la erradicación, la réplica y/o resolución de la guerra cibernética que les permitan sobrellevar y poder contrarrestar los efectos de ésta, lo que ha dado lugar a que los Estados tengan desarrollo en seguridad nacional y puedan

confrontar las ciberamenazas y las consecuencias de las actividades bélicas que se derivan.

Sin embargo, ello solo determina la parte de un entorno seguro para los Estados, algo que es natural y obvio para resguardar la seguridad y los intereses nacionales, y no una relación jurídica estrecha y armónica con los demás pertenecientes al sistema internacional.

Los casos de ciberguerra que se mostraron en el presente trabajo, son los ejemplos más incuestionables y evidentes de una guerra concurrente o, en casos como Francia y Reino Unido, una guerra latente, o el caso chino-estadounidense el de una guerra fría manifiesta.

Empero, el acontecimiento es la coyuntura Rusia contra el resto de los Estados occidentalizados que pretenden liderar el contexto mundial, pues se puede ver que las guerras cibernéticas que se presencian o están palpables son con la nación rusa, omitiendo la que viven China y Estados Unidos, por lo que el liderazgo y la guerra de poder procura ser ganada por la potencia y ahora superpotencia emergente.

¿Rusia es el punto de enfoque en esta ciberguerra? La respuesta es sí. Pues en un mundo multipolar en el que en realidad destacan, de nueva cuenta y como hace años, dos potencias Estados Unidos y Rusia, que si bien no debemos dejar a China de lado como potencia emergente y que también figura con un papel destacable en la guerra cibernética, los dos primeros son los protagonistas por una lucha de poder ya no solo en los 4 dominios existentes, sino también en el quinto dominio que se ha convertido en un punto de enfoque para los Estados y en un escenario relativamente nuevo y aprovechable para hacer la guerra, que tiene como objetivo principal una lucha de poder o, mejor dicho, ciberpoder, pues desde el fin del orden bipolar Estados Unidos ha creado una arquitectura política, social y económica que le permita mantener su papel de liderazgo en el sistema internacional.

Es de ello que se destaca el vacío jurídico internacional que se puede presenciar, pues los países más influyentes dentro del sistema internacional están en guerra y para que comience una iniciativa para contrarrestarla debe ser por parte de alguno de ellos para que ésta contenga mayor relevancia y legitimidad a nivel internacional.

No obstante, las intenciones son nulas e inexistentes, pues en esta carrera por el ciberpoder que llevaría a la adquisición de poder mundial a través de la guerra, no se pretende que sea apacible para evitar brindar facilidad a cualquiera que quisiese ganarla.

Por lo que el derecho debe entrar en ese entorno de adaptación y contemporaneidad basado en un clima multipolar de tensión para que dejen de existir esas lagunas jurídicas internacionales que no permiten desarrollar una legislación jurídica internacional en relación a la ciberguerra, y eso pasará cuando los Estados estén en completa disponibilidad de armonizar sus normativas y el poder deje de ser el motor de la guerra.

Tal propuesta solo ocurriría en un mundo utópico, multipolar y comprometido a las sociedades y no a los intereses de cada Estado.

Asimismo, la obtención de control dentro de un dominio que tiene poca dirección por su amorfosidad, abriría las posibilidades de crear la regulación jurídica internacional sobre la ciberguerra que pueda figurar como la ideal que abarque los requerimientos para poder confrontar un fenómeno tan complejo e importante para el sistema internacional y sus actores.

De igual manera, se destaca que se tiene que tomar en cuenta que los avances tecnológicos están en una transformación continua, por lo que además de que las legislaciones del Derecho Internacional sean adaptables deben ser dinámicas para no tener que hacer reestructuraciones, o realizar normativas nuevas, y que no existan los vacíos jurídicos que no permitan llevar a cabo un orden internacional que de pie a un sistema equilibrado.

Referencias

Bibliografía

- Bodin, Jean, *De la soberanía* en *Los seis libros de la Republica,* Madrid, Tecnos, 1997, tercera edición, pp. 389.

-Buick, Joanna; Jevtic, Zoran, *Ciberespacio para principiantes,* Argentina, Era Naciente, 2002, pp.175.

--Cabanellas de Torres, Guillermo, *Diccionario Jurídico Elemental,* Perú, Libros Derecho, 2006, pp.506.

- Casar, Corredera, *El ciberespacio. Nuevo escenario de confrontación*, España, Centro Superior de Estudios de la Defensa Nacional, 2012, pp.34.

-Clausewitz, Karl, *De la guerra,* Greenbooks editores, 2016, pp. 353.

- Consejo de Europa, *Convenio sobre la ciberdelincuencia,* Budapest, Consejo de Europa, 23 de noviembre de 2001, pp.26.

-De Izcue, Carlos, *Principios de la guerra* en *Apuntes de estrategia operacional,* Perú, División de publicaciones de la Escuela Superior de Guerra Naval, octubre de 2013, segunda edición, pp. 160.

-Gajate, María; González, Laura, *Guerra y tecnología. Interacción desde la antigüedad al presente,* Madrid, Centro de Estudios Ramón Areces, 2017, pp. 552.

-Galvani, Iván, *La vida cotidiana en el ciberespacio,* Argentina, Universidad Nacional de La Plata, pp. 98.

-Levy, Pierre, *¿Qué es lo virtual?,* Barcelona, Paidos Iberica, 1999, p.142.

- López de Turiso, Javier, *La evolución del conflicto hacia un nuevo escenario bélico* en *El ciberespacio. Nuevo escenario de confrontación*, España, Centro Superior de Estudios de la Defensa Nacional, 2012, pp.117-166.

-Marowski, Carl, *Efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica* en *La ciberguerra: sus impactos y desafíos,* Chile, Centro de Estudios Estratégicos de la Academia de Guerra Ejército de Chile, 2018, primera edición, pp. 168.

- Ministerio de Defensa, Ciberseguridad*. Retos y amenazas a la seguridad nacional en el ciberespacio*, España, Instituto español de estudios estratégicos, 2010, pp.368.

- Naciones Unidas, *Declaración Universal de Derechos Humanos,* Naciones Unidas, pp. 72.

- NATO, *Anual Report 2016,* Bélgica, NATO, 2016, pp.121.

-Nye, Joseph, *Cyber Power, United States, Belfer Center for Science and International* Affairs, 2010, pp. 24.

- Pastor, Óscar, *et al*., *Seguridad Nacional y Ciberdefensa*, Madrid, Isdefe, 2009, primera edición, pp. 177.

- Real Academia Española*, Diccionario de la Lengua Española*, Madrid, Espasa Calpe, 1984, segunda edición, pp. 1432.

- República de Francia, *Estrategia Nacional Francesa para la Seguridad en el Ámbito Digital,* Francia, República de Francia, 2015, pp. 44.

- Schjolberg, Stein; Ghernaouti-Helie, Solange, *A Global Treaty on Cybersecurity and Cybercrime,* AiTOslo, 2011, segunda edición, pp. 97.

- Touré, Hamadoun, *La búsqueda de la confianza en el ciberespacio,* Suiza, Unión Internacional de Telecomunicaciones, 2014, pp. 182.

-Valdés, Luis A, *Planeación estratégica integral con enfoque de sistemas: caso de éxito con observaciones* en Planeación Prospectiva Estratégica, México, UNAM, 2015, pp. 559-588.

Hemerografía

- Amigo, Alejandro, “Consideraciones sobre la ciberamenaza a la seguridad nacional”, *Revista Política y Estrategia*, núm. 125, Chile, Academia Nacional de Estudios Políticos y Estratégicos, 2015, pp.83-96.

-Cabrera Mendoza, Elizabeth; y Valdés Godines, Juan Carlos, “Ciberespacio y cibersociedad, su relación con las formas alternativas de socialización para la apropiación social de las TIC´s”, Revista Iberoamericana para la Investigación y el Desarrollo Educativo, núm. 10, enero-junio, 2013, [en línea], México, Ride, 2013, Dirección URL:

http://ride.org.mx/1-11/index.php/RIDESECUNDARIO/article/viewFile/564/553, [consulta: 16 de diciembre de 2018], pp.18.

- Contreras, Emigdio, “El concepto de estrategia como fundamento de la planeación estratégica”, Pensamiento y Gestión, núm. 35, Colombia, Universidad del Norte, julio-diciembre, 2013, pp. 152-181.

- Espinosa, Iván, “Hacia una estrategia nacional de ciberseguridad en México”, *Revista de Administración Pública,* núm. 1, vol. L, México, Instituto Nacional de Administración Pública, 2015, pp. 115-146.

- Guevara, Anaid, “Hacking ético: mitos y realidades”, *Revista Seguridad,* núm. 12, México, Coordinación de Seguridad de la Información-UNAM, 2018, pp.8.

-Llorens, María del Pilar, “Los desafíos del uso de la fuerza en el ciberespacio”, [en línea], pp. 32, México, Instituto de Investigaciones Jurídicas-UNAM, 2017, Dirección URL: https://revistas.juridicas.unam.mx/index.php/derechointernacional/article/viewFile/11052/13078, [consulta: 26 de noviembre de 2018].

- Martínez, Fernando, “La guerra silenciosa”, [en línea], pp. 44-49, España, Revista Española de Defensa, núm. 294, abril 2013, Dirección URL: https://www.defensa.gob.es/Galerias/documentacion/revistas/2013/red-294-ciberguerra.pdf [consulta: 20 de diciembre de 2019].

- Raboin, Bradley, “Corresponding Evolution: International Law and the Emergence of Cyber Warfare”, [en línea], pp. 604-668, Estados Unidos, Journal of the National Association of Administrative Law Judiciary, vol. 31, núm. 2, octubre 2011, Dirección URL:
https://digitalcommons.pepperdine.edu/cgi/viewcontent.cgi?article=1013&context=naalj [consulta: 30 de julio de 2019].

Cibergrafía

- Asamblea General de las Naciones Unidas, *Definición de la agresión Resolución 3314 (XXI),* [en línea], pp.2, ACNUR, 14 de diciembre de 1974, Dirección URL: https://www.acnur.org/fileadmin/Documentos/BDL/2007/5517.pdf [consulta: 28 de julio de 2019].

-Asamblea General de las Naciones Unidas, *Resolución 63/202. Las tecnologías de la información y las comunicaciones para el desarrollo,* [en línea], pp. 4, Naciones Unidas, 19 de diciembre de 2008, Dirección URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/63/202&Lang=S [consulta: 14 de octubre de 2019].

- BBC, "El virus que tomó control de mil máquinas y les ordenó autodestruirse", [en línea], BBC News Mundo, 11 de octubre de 2015, Dirección URL: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet [consulta: 13 de junio de 2019].

- BBC, "Royal Navy website attacked by Romanian hacker", [en línea], BBC News Technology, 08 de noviembre de 2010, Dirección URL: https://www.bbc.com/news/technology-11711478 [consulta: 13 de junio de 2019].

- Carracosa, Celia, *Ciberespacio, el quinto dominio de la guerra,* [en línea], GIASP Intelligence & Strategy, 08 de marzo de 2017, Dirección URL: https://intelgiasp.com/2017/03/08/ciberespacio-el-quinto-dominio-de-la-guerra-cyberspace-the-fifth-domain-of-the-war/ [consulta: 11 de junio de 2019].

- Carrillo, Leonardo, Vargas, Paola, *Ciberguerra: descripción de estrategias políticas internacionales y algunos planteamientos jurídicos para afrontarla*, [en línea], pp.114, Bogotá, Universidad Militar Nueva Granada, 2016, Dirección URL: https://repository.unimilitar.edu.co/bitstream/handle/10654/16043/carrillofarfancesarleonardo2017%20%281%29.pdf?sequence=3&isAllowed=y, [consulta: 17 de diciembre de 2018].

- Conferencia General, *Carta sobre la Preservación del Patrimonio Digital,* [en línea], UNESCO, 15 de octubre de 2003, Dirección URL: http://portal.unesco.org/es/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html [consulta: 15 de octubre de 2019].

-Comité Internacional de la Cruz Roja, *¿Qué tratados forman el Derecho Internacional Humanitario?*, [en línea], Comité Internacional de la Cruz Roja, Dirección URL: https://www.icrc.org/es/doc/resources/documents/misc/5tdlja.htm [consulta:14 de septiembre de 2020].

- Comité Internacional de la Cruz Roja*, Principios generales básicos del Derecho Internacional Humanitario,* [en línea], Comité Internacional de la Cruz Roja, Dirección URL: http://www.cruzroja.es/portal/page?_pageid=878,12647079&_dad=portal30&_schema=PORTAL30 [consulta: 02 de noviembre de 2019].

- Cumbre Mundial sobre la Sociedad de la Información, *Declaración de Principios y un Plan de Acción,* [en línea], Ginebra, Consejo de la Unión Internacional de Telecomunicaciones, 12 de mayo de 2004, Dirección URL: https://www.itu.int/net/wsis/docs/geneva/official/poa-es.html [consulta: 13 de octubre de 2019].

- De los Reyes, Ignacio, “Lo que se sabe de una posible ciberguerra contra el narco en México”, [en línea], México, BBC News Mundo, 02 de noviembre de 2011, Dirección URL: https://www.bbc.com/mundo/noticias/2011/11/111101_mexico_anonymous_zetas_opcarte l_irm [consulta: 10 de diciembre de 2019].

- Fernández, Jesús; Molina, David, *Cibersociedad y ciencias humanas: el caso de la Historia Actual,* [en línea], Argentina, Instituto Argentino para el desarrollo económico, Dirección URL: http://www.iade.org.ar/noticias/cibersociedad-y-ciencias-humanas-el-caso-de-la-historia-actual-0, [consulta: 25 de abril de 2018].

- Gasperin, Rafael, *Adolescencia y ciberespacio,* [en línea], Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura, 2005, Dirección URL: https://www.oei.es/historico/valores2/monografias/monografia05/reflexion04.htm, [consulta: 18 de marzo de 2019].

- Gisel, Laurent, *El derecho de la guerra también impone límites a la guerra cibernética,* [en línea], Comité Internacional de la Cruz Roja, 01 de julio de 2013, Dirección URL: https://www.icrc.org/es/doc/resources/documents/interview/2013/06-27-cyber-warfare-ihl.htm [consulta: 02 de noviembre de 2019].

- González, Enric, “Francia afirma que "no está a salvo" de ciberataques rusos contra sus elecciones”, [en línea], Francia, El Mundo, 09 de enero de 2017, Dirección URL: https://www.elmundo.es/internacional/2017/01/09/58729cd046163fc8028b461a.html [consulta: 20 de diciembre de 2019].

- Guimón, Pablo, “Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero”, [en línea], El País, 12 de mayo de 2017, Dirección URL: https://elpais.com/tecnologia/2017/05/12/actualidad/1494602389_458942.html [consulta: 31 de julio de 2019].

- Herraiz, Pablo, “Presupuestos 2019: Defensa recibe 900 millones para mejorar la profesionalización del ejército”, [en línea], *El mundo,* 14 de enero de 2019, Dirección URL: https://www.elmundo.es/espana/2019/01/14/5c3c79e5fdddff5d078b45a2.html [consulta 16 de septiembre de 2019].

- HM Goverment, *Estrategia de ciberseguridad nacional 2016-2021,*[en línea], pp. 59, Reino Unido, HM Goverment, 2016, Dirección URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643420/Spanish_translation_-_National_Cyber_Security_Strategy_2016.pdf [consulta: 05 de enero de 2020].

- IT User, “La UE declarará los ciberataques como acto de guerra, [en línea], IT User, 09 de noviembre de 2017, Dirección URL: https://discoverthenew.ituser.es/security-and-risk-management/2017/11/la-ue-declarara-los-ciberataques-como-acto-de-guerra [consulta: 10 de julio de 2019]

-Lejarza, Eguskiñe, *Estados Unidos- China: equilibrio de poder en la nueva ciberguerra fría,* [en línea], pp. 21, España, Instituto Español de Estudios Estratégicos, 01 de julio de 2013, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO60-2013_Ciberguerra_Fria_EEUU-China_E.Lejarza.pdf [consulta: 20 de diciembre de 2019].

- Lima, Lioman, “Estados Unidos vs Rusia: cómo el hackeo de las redes eléctricas se convirtió en un nuevo campo de batalla entre Washington y Moscú”, [en línea], BBC News Mundo, 19 de junio de 2019, Dirección URL: https://www.bbc.com/mundo/noticias-internacional-48668879 [consulta: 15 de diciembre de 2019].

- Mallol, Eugenio, *La era de la cibersoberanía*, [en línea], El Mundo, 18 de diciembre de 2017, Dirección URL: https://www.elmundo.es/economia/2017/12/11/5a2e6c3546163f552d8b4642.html, [consulta: 19 de abril de 2019].

-Mateos, Iván, “Corea del Norte, la última apuesta nuclear”, [en línea], *CISDE Observatorio,* 13 de septiembre de 2019, Dirección URL: https://observatorio.cisde.es/actualidad/corea-del-norte-la-ultima-apuesta-nuclear/ [consulta: 16 de septiembre de 2019].

- Martínez, Salvador, “Europa y sus elecciones, objetivo de la ciberguerra rusa”, [en línea], El español, 10 de enero de 2017, Dirección URL: https://www.elespanol.com/mundo/europa/20170109/184732377_0.html [consulta: 20 de diciembre de 2019].

- Molina, Mateos, *Aproximación Jurídica al ciberespacio,* [en línea], pp. 20, España, Instituto Español de Estudios Estratégicos, 08 de junio de 2015, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO57-2015_Aproximacion_Juridica_Ciberespacio_MolinaMateos.pdf [consulta: 07 de octubre de 2019].

-Naciones Unidas, *Carta de las Naciones Unidas,* [en línea], San Francisco, Naciones Unidas, 26 de junio de 1945, Dirección URL: https://www.un.org/es/charter-united-nations/index.html [consulta: 15 de noviembre de 2019].

- Pantano, Ariel, *Ci*berguerra, [en línea], pp.7, Argentina, Universidad de Palermo, Dirección URL: https://dspace.palermo.edu:8443/xmlui/bitstream/handle/10226/1448/Ciberguerra-Pantano%2068586.pdf?sequence=1 [consulta: 14 de abril de 2018].

- Perry, John, *A Declaration of the Independence of Cyberspace,* [en línea], pp. 4, Estados Unidos, Nomadas y Rebeldes, 08 de febrero de 1996, Dirección URL: https://nomadasyrebeldes.files.wordpress.com/2012/05/manifiesto_de_john_perry_barlow-1.pdf [consulta: 13 de octubre de 2019].

- Presidencia de la República Francesa, *Libro Blanco sobre defensa y seguridad nacional,* [en línea], Francia, Presidencia de la República Francesa, 2013, Dirección URL: https://es.ambafrance.org › IMG › pdf › LIBRO_BLANCO [consulta: 28 de diciembre de 2019], pp.7.

- Real Academia Española, *Diccionario de la lengua española,* [en línea], Real Academia Española, 2019, Dirección URL: https://dle.rae.es/estrategia [consulta: 06 de diciembre de 2019].

- Ridder, Helmut, *La guerra y el derecho de guerra en el Derecho Internacional y en la doctrina internacionalista,* [en línea], pp. 31-50, Dialnet, Dirección URL: https://dialnet.unirioja.es/descarga/articulo/2129071.pdf, [consulta: 19 de abril de 2019].

- Rodríguez, Paola; Cordero, Yaneth*, Ciberseguridad: los acuerdos de cooperación para el tratamiento de las amenazas en el ciberespacio. El caso de Estados Unidos y China*, [en línea], Bogotá, Universidad de La Salle, 2018, Dirección URL: http://repository.lasalle.edu.co/bitstream/handle/10185/25117/64122001_2018.pdf?sequence=1&isAllowed=y [consulta: 28 de diciembre de 2019], pp.63.

- Ruíz, Joaquín, *Ciberamenazas: ¿el terrorismo del futuro?,* [en línea], pp. 21, España, Instituto Español de Estudios Estratégicos, 19 de agosto de 2016, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf, [consulta: 24 de abril de 2019].

- s/a, *Ciberguerra*, [en línea], Instituto de Ingeniería-UNAM, Dirección URL: http://www.iingen.unam.mx/esmx/Publicaciones/GacetaElectronica/Mayo2016/Paginas/Ciberguerra.aspx, [consulta: 16 de diciembre de 2018].

- s/a, *Ciberseguridad y protección de datos en México*, [en línea], México, Asociación Mexicana de Ciberseguridad, Dirección URL: https://www.ameci.org/, [consulta: 23 de abril de 2019].

-s/a, *Ciberdefensa,* [en línea], España, Estado Mayor de la Defensa, Dirección URL: http://www.emad.mde.es/ciberdefensa/ [consulta: 16 de septiembre

- s/a, *Ciberdefensa-Ciberseguridad Riesgos y Amenazas,* [en línea], pp.31, Consejo Argentino para las Relaciones Internacionales, noviembre 2013, Dirección URL: http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf, [consulta: 24 de abril de 2018].

- s/a, *Ciberoperaciones*, [en línea], España, Astabis Information Risk Management, Dirección URL: https://www.astabis.com/es/servicios-para-los-gobiernos/defensa/ciberoperaciones, [consulta: 25 de abril de 2019].

- s/a*, Cómo aumentar el rendimiento de tu infraestructura informática,* [en línea], España, RCG Comunicaciones, Dirección URL: http://rcg-comunicaciones.com/rendimiento-infraestructura-informatica/, [consulta: 20 de abril de 2019].

- s/a, *Declaración Americana de los derechos y deberes del hombre,* Bogotá, 1948, p. 2.

- s/a, *El DIP de guerra* en Derecho Internacional Público, [en línea], pp. 7, México, Instituto de Investigaciones Jurídicas de la UNAM, Dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/7/3262/21.pdf, [consulta: 19 de abril de 2019], p.

- s/a, *Estado,* [en línea], La Habana, EcuRed, Dirección URL: https://www.ecured.cu/Estado, [consulta: 20 de abril de 2019].

- s/a, *Estrategia Nacional de Ciberseguridad*, [en línea], México, Gobierno de México, 2017, Dirección URL: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf [consulta: 27 de diciembre de 2019].

- s/a, *El poder del Estado*, [en línea], La Guía 2000 de Derecho, 27 de agosto de 2010, Dirección URL: https://derecho.laguia2000.com/derecho-politico/el-poder-del-estado, [consulta: 20 de abril de 2019].

- s/a, *FIRST is the global Forum of Incident Response and Security Teams,* [en línea], FIRST, Dirección URL: https://www.first.org/ [consulta: 26 de diciembre de 2019].

- s/a, *Fortalecimiento del marco de trabajo legal y regulatorio relativo al subcomponente de revisión del marco de trabajo regulatorio a la etapa de monitoreo 2011, Asociación Mexicana de Internet,* 2011, pp. 488.

- s/a, *Hacker*, [en línea], Avast, Dirección URL: https://www.avast.com/es-es/c-hacker, [consulta: 25 de abril de 2019].

- s/a, *Hardware y software*, [en línea], Instituto de Ingeniería-UNAM, Dirección URL: http://www.iingen.unam.mx/es-mx/Publicaciones/GacetaElectronica/GacetaNoviembre2013/Paginas/Hardwareysoftware.aspx, [consulta: 21 de abril de 2019].

- s/a, *Infrastructure Security,* [en línea], Estados Unidos, United States Department of Homeland Security, Dirección URL: https://www.dhs.gov/topic/critical-infrastructure-security [consulta: 12 de junio de 2019].

- s/a, *La ley de decencia en las comunicaciones y GILC,* [en línea], Estados Unidos, Biblioweb Sin Dominio, Dirección URL: https://biblioweb.sindominio.net/telematica/republica/node12.html [consulta: 13 de octubre de 2019].

- s/a, *Malware y antimalware,* [en línea], Avast, Dirección URL: https://www.avast.com/es-es/c-malware, [consulta: 23 de abril de 2019].

- s/a, *Meridian Process*, [en línea], Meridian Process, Dirección URL: https://www.meridianprocess.org/ [consulta: 26 de diciembre de 2019].

-s/a, " México se arma contra ciberataques", [en línea], México, Vanguardia, 20 de enero de 2016, Dirección URL: https://vanguardia.com.mx/articulo/mexico-se-arma-contra-ciberataques [consulta: 10 de diciembre de 2019].

- s/a, *OTAN considera el ciberespacio como un dominio militar legitimo,* [en línea], México, Coordinación de Seguridad de la Información- UNAM, 29 de junio de 2017, Dirección URL: https://www.seguridad.unam.mx/otan-considera-el-ciberespacio-como-un-dominio-militar-legitimo [consulta: 11 de junio de 2019].

- s/a, *¿Qué es big data?,* [en línea], Oracle, Dirección URL: https://www.oracle.com/mx/big-data/guide/what-is-big-data.html, [consulta: 10 de septiembre de 2019].

- s/a, *¿Qué es ciberseguridad y de qué fases consta?*,[en línea], Barcelona, OBS Business School, Dirección URL: https://www.obs-edu.com/int/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta, [consulta: 23 de abril de 2019].

- s/a, *¿Qué es la Ciberdefensa y en qué se diferencia de la Ciberseguridad?,* [en línea], España, Next International Business School, 15 de agosto de 2018, Dirección URL: https://www.nextibs.com/que-es-ciberdefensa-se-diferencia-ciberseguridad/, [consulta: 24 de abril de 2018].

- s/a, *¿Qué es un ciberataque y qué tipos existen*?, [en línea], Valencia, Transformación Digital Cámara de Valencia, Dirección URL: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/#Que_es_un_ciberataque, [consulta: 24 de abril de 2019].

- s/a, *¿Qué es el ramsomware?,* [en línea], Kaspersky, Dirección URL: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware [consulta: 10 de julio de 2019].

- s/a, "Rusia tilda de "peligrosa" declaración de Reino Unido sobre supuesta ciberguerra", [en línea], Moscú, Sputnik Mundo, 22 de noviembre de 2019, Dirección URL: https://mundo.sputniknews.com/politica/201911221089404403-rusia-tilda-de-peligrosa-declaracion-de-reino-unido-sobre-supuesta-ciberguerra/ [consulta: 22 de diciembre de 2019].

- s/a, *Soberanía,* [en línea], Sistema de Información Legislativa, Dirección URL: http://sil.gobernacion.gob.mx/Glosario/definicionpop.php?ID=229, [consulta: 19 de abril de 2018].

- Saavedra, Alberto, *¿Qué es la Infraestructura Tecnológica IT? Beneficios en la Transformación Digital,* [en línea], España, Clavei Expertos en Transformación Digital, 13 de febrero de 2018, Dirección URL: https://www.clavei.es/blog/que-es-la-infraestructura-it/, [consulta: 21 de abril de 2019].

- Salazar, Juan Pablo, *La migración de la guerra al espacio digital*, [en línea], pp. 58, Madrid, Universidad Complutense de Madrid, Dirección URL: https://www.sites.oas.org/cyber/Documents/2016%20%20La%20migracio%CC%81n%20de%20la%20guerra%20al%20espacio%20digitalJuan%20Pablo%20Salazar.pdf, [consulta: 17 de diciembre de 2018].

- Sánchez, Gema, *Los Estados y la ciberguerra*, [en línea], pp.13, España, Universidad de La Rioja, 2010, Dirección URL: https://dialnet.unirioja.es/servlet/articulo?codigo=3745519, [consulta: 16 de diciembre de 2018].

- Schmitt, Michael, *Tallin Manual on the International Law applicable to cyber warfare*, [en línea], pp. 215, Cambridge University, 2013, Dirección URL: http://csef.ru/media/articles/3990/3990.pdf, [consulta: 28 de noviembre de 2018].

- Secretaría de Gobernación, *DECRETO por el que se aprueba la Estrategia Nacional de Seguridad Pública del Gobierno de la República,* [en línea], México, Secretaría de Gobernación, 16 de mayo de 2019, Dirección URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5560463&fecha=16/05/2019 [consulta: 27 de diciembre de 2019].

- Segura, Antonio, *Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio,* Granada, Universidad de Granada, 2013, pp. 238.

- Seminario Judicial de la Federación, *Jurisdicción y competencia,* [en línea], México, Suprema Corte de Justicia de la Nación, 07 de agosto de 1975, Dirección URL: https://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/245/245837.pdf, [consulta: 19 de abril de 2019].

- Siula, Carlos, "Se desata ciberguerra contra Rusia por presunto hackeo masivo", [en línea], Francia, El Sol de México, 18 de abril de 2018, Dirección URL: https://www.elsoldemexico.com.mx/mundo/se-desata-ciberguerra-contra-rusia-por-presunto-hackeo-masivo-1622398.html [consulta: 22 de diciembre de 2019].

- Smith-Spark, Laura, "Hospitales británicos también son blanco de ciberataque", [en línea], CNN, 12 de mayo de 2017, Dirección URL: https://cnnespanol.cnn.com/2017/05/12/hospitales-britanicos-tambien-son-blanco-de-ciberataque/ [consulta: 31 de julio de 2019].

- Soto, Armando, "Derecho de la guerra = Derecho Internacional Humanitario", [en línea], pp.6, México, Instituto de Investigaciones Jurídicas- UNAM, 2015, Dirección URL: http://dx.doi.org/10.22201/fder.24488933e.2015.263.59871, [consulta: 19 de abril de 2019].

- West, Ian, *Cyber Security*, [en línea], Estados Unidos, NCI NATO, Dirección URL: https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx [consulta: 26 de diciembre de 2019].

- White House, *Cybersecurity funding,* [en línea], pp. 273-287, Estados Unidos, The White House, Dirección URL: https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf, [consulta 15 de septiembre de 2019].