UNIVERSIDAD AUTÓNOMA DEL
ESTADO DE QUINTANA ROO

DIVISIÓN DE CIENCIAS POLÍTICAS Y ECONÓMICAS

# La militarización del Ciberespacio por parte de los Estados Unidos, 2008-2015.

**Tesis**

Para obtener el título de

**Licenciado en Relaciones Internacionales.**


PRESENTA

**Edwin Damián Matú Álvarez**


UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO
ÁREA DE TITULACIÓN

DIRECTOR DE LA TESIS

**Dr. Juan Carlos Arriaga Rodríguez**

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO
DIVISIÓN DE CIENCIAS POLÍTICAS Y ECONÓMICAS

UNIVERSIDAD AUTÓNOMA DEL
ESTADO DE QUINTANA ROO

DIVISIÓN DE CIENCIAS POLÍTICAS Y ECONÓMICAS

# La militarización del ciberespacio por parte de Estados Unidos, 2008-2015

Presenta:
Edwin Damián Matú Álvarez

Tesis para obtener el título de Licenciado en Relaciones Internacionales

COMITÉ DE SUPERVISIÓN

Sinodal propietario:

Dr. Juan Carlos Arriaga Rodríguez

Sinodal propietario:

Dra. Tania Libertad Camal Cheluja

Sinodal propietario:

Mtro. Mario Edgardo Vargas Paredes

Suplente:

Dr. Jaime Uribe Cortes

Suplente:

Mtro. José Manuel Calderón Pérez

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE QUINTANA ROO
DIVISIÓN DE CIENCIAS POLÍTICAS Y ECONÓMICAS

UNIVERSIDAD AUTÓNOMA DEL
ESTADO DE QUINTANA ROO

**ÁREA DE TITULACIÓN**

Chetumal, Quintana Roo, México, mayo de 2022

**Agradecimientos:**

**Esta tesis tiene una dedicatoria especial a mis padres, que sin su apoyo en mi proceso formativo y académico este trabajo no hubiera sido concluido.**

**A mi Director de tesis el Dr. Juan Carlos Arriaga, al pasar de los meses siempre fue insistente con que concluyera este trabajo, además de ser el único Docente el cual acepto mi tema de tesis, de aquel ya lejano 2014 donde el ciberespacio y las relaciones internacionales eran un tema que parecía mantener poca relevancia dentro los estudios internacionales, y que a principios de este trabajo era poca la información que se podía obtener.**

**También a cada docente de la Licenciatura en Relaciones Internacionales, aunque cada uno con posturas incluso opuestas sobre la comprensión de la realidad internacional, en cada uno reconocí la pasión y el deseo por el aprendizaje, aprendía escuchándoles en cada clase.**

**Y por último agradezco a cualquier persona que considere este trabajo para la realización del suyo o se tome el tiempo que para la lectura de este.**

## Dedicatoria

Este trabajo me lo dedico, a ese  Edwin de 2014 a quien le debo tanto.

# Resumen

El siguiente trabajo de tesis presenta un análisis de las medidas adoptadas por el gobierno del presidente estadounidense Barack Obama (2008-2016) para la vigilancia y control militar del ciberespacio. El mundo virtual es un campo de interés para el desarrollo de actividades de diversos tipos, especialmente las de corte militar, que son consideradas como amenazas a la seguridad de las potencias. En este marco, los Estados nacionales ha decidido normar y aplicar medidas de seguridad diseñadas por los militares. El objetivo central de la investigación es identificar caracterizar las medidas de control del ciberespacio emprendidas por la administración de Barack Obama, las cuales consideramos fundamentan el proceso de militarización del ciberespacio. Con base en la teoría neorrealista de las Relaciones Internacionales, analizamos la doctrina denominada "teoría del colapso", la cual identifica las amenazas a la seguridad estadounidense que están presentes en el ciberespacio.

**Palabras clave**

Teoría del colapso, ciberseguridad, ciberamenaza, ciberterrorismo, militarización del ciberespacio.

# ÍNDICE



**Índice de Tablas y figuras.**

# INTRODUCCIÓN

El ciberespacio es un campo apenas normado, pragmático y complejo, en donde ocurren fenómenos que llaman la atención de las Relaciones Internacionales. El ciberespacio no posee frontera alguna, pues ahí no existen espacios geográficos físicos. Es un ámbito tecnológico en donde converge e interactúa la mayor parte de la población mundial que posee cualquier dispositivo con acceso a internet.

Esta investigación de tesis aborda la política de protección militar del ciberespacio realizada por la administración del expresidente estadounidense Barack Obama (2008-2016). Las variables de investigación son las político-militares y las concepciones estratégicas para enfrentar distintas amenazas provenientes del ciberespacio ciberataques, estas diseñadas por el gobierno estadounidense, en atención a los posibles riesgos que representan para la hegemonía global de esta potencia. Esta investigación es de tipo cualitativo documental.

El planteamiento del problema alude a la preocupación de las distintas potencias mundiales, las cuales han señalado que en el espacio virtual existen amenazas que atentan contra la seguridad nacional de cada una de ellas, de manera que han recurrido a medidas de corte militar para contrarrestarlas. La militarización es una respuesta a las amenazas pues impactan directamente al mundo material. Según las doctrinas que promueven la militarización del ciberespacio, las políticas de corte militar son la única manera de garantizar la seguridad nacional y proteger los intereses de los Estados.

La militarización del mundo virtual es una política de las grandes potencias tecnológicas (China, Japón, Rusia, Corea del Sur, Estados Unidos, Brasil, Gran Bretaña y la UE). Esos Estados buscan proteger sus sistemas electrónicos de posibles ataques, pues señalan, los sistemas informáticos permiten la administración eficiente de servicios públicos (suministro de agua potable, de electricidad, trámites administrativos, vialidad, el transporte masivo como el subterráneo, tránsito aeroportuario, etcétera), y si fueran atacados, los daños generarían un caos urbano.

Por su parte, las grandes corporaciones del sector privado han reportado ataques a sus sistemas computacionales; esos ataques tienen como principal objetivo el robo de información. La información confidencial de personas y empresas es subastada o vendida por los piratas informáticos en la red. No obstante, lo anterior, lo que genera mayor preocupación para los gobiernos, en especial a Estados Unidos, es un eventual ataque el

sistema informático militar; el uso de la red global de información es fundamental para las operaciones de los ejércitos.

De esta forma, durante el gobierno de Barack Obama se estableció políticas de corte político y militar para enfrentar las supuestas amenazas contra la seguridad nacional que están presentes en el ciberespacio. Tales políticas son identificadas en la llamada "teoría del colapso". Los objetivos estratégicos identificados en la teoría del colapso son dos: primero, el control del ciberespacio como una condición para conservar el poder militar estadounidense a escala global; y segundo, la militarización para enfrentar las amenazas potenciales y latentes generadas por otras potencias o Estados enemigos. (Clarke y Kanake, 2010, p. 3).

Por lo anterior, en la investigación pretendo responder las siguientes preguntas de investigación: ¿Cuáles son los intereses estratégicos de Estados Unidos en el ciberespacio? Y ¿Cuáles son las políticas militares diseñadas e implementadas por la administración de Barack Obama para enfrentar las amenazas presentes en el ciberespacio?

La hipótesis de investigación es que el gobierno de Barack Obama ha establecido políticas de corte político y militar para enfrentar las amenazas a la seguridad nacional de Estados Unidos existentes en el ciberespacio. Esas políticas buscan contraatacar a las nuevas amenazas que identifica la teoría del colapso diseñada por los estrategas militares. Es posible pensar que los objetivos estratégicos que emanan de la implementación de estas acciones corresponden a la necesidad de controlar este nuevo espacio a reserva de conservar parte de las esferas de influencia a nivel internacional y responder de forma eficaz ante las amenazas potenciales de posibles Estados antagonistas o nuevos actores dentro del escenario internacional.

Para demostrar la hipótesis anterior, este trabajo desarrollará tres objetivos de investigación. Primero, buscaremos explicar en qué consiste la teoría del colapso y emplearla como herramienta de análisis de las estrategias y políticas de militarización del ciberespacio por parte de Estados Unidos. En segundo lugar, procederemos a describir el origen del ciberespacio, a identificar el marco jurídico e institucional que lo regula y a caracterizar el tipo de conflictos que ahí ocurren, con el fin de establecer el contexto en el que Estados Unidos procede en militarización del ciberespacio. Finalmente, buscaremos identificar la política estratégica (objetivos, retos y acciones) del proceso de militarización del

ciberespacio por parte de Estados Unidos, y a explicar las acciones concretas realizadas por el gobierno de Barak Obama en este tema.

De esta forma, la tesis está dividida en tres capítulos. En el primero se expone la perspectiva de análisis que soporta la investigación, en este caso la teoría realista en las Relaciones Internacionales, y a partir de lo anterior, se explica que la "teoría del colapso" consiste en un programa de acción militar en la internet.

En el segundo capítulo se describen los orígenes de la Internet. Al respecto, reflexionamos sobre los usos sociales, políticos y militares de esta herramienta de comunicación e información. Además, identificamos algunos de los conflictos más relevantes que han impactado en la estabilidad en las instituciones económicas y políticas de algunos Estados.

En el último capítulo se analizarán los acontecimientos que han justificado la militarización del ciberespacio, así como las medidas que se implementaron durante la administración de Barack Obama, analizando cada una de estas acciones desde la perspectiva de la teoría neorrealista, empleando términos a fines a dicha perspectiva teórica, contextualizando la postura estadounidense respecto al proceso de militarización del ciberespacio.

# CAPÍTULO I.- MARCO TEÓRICO. EL NEORREALISMO POLÍTICO Y LA TEORÍA DEL COLAPSO

El objetivo de este capítulo es explicar la teoría del colapso mediante la perspectiva neorrealista de las Relaciones Internacionales. Esto se realiza en tres apartados: en el primero se identifica los postulados básicos del neorrealismo; en el segundo, se sistematizan los planteamientos centrales de la "teoría del colapso" y sus principales propuestas para la militarización del ciberespacio; por último, en el tercer apartado se explican los fundamentos neorrealistas de la teoría del colapso.

## 1.1- La propuesta del realismo político para el estudio de la política internacional

El realismo político es una de las teorías más importantes e influyentes para el estudio de las Relaciones Internacionales. En esta disciplina existen diferentes enfoques para explicar la realidad mundial, entre los que podemos mencionar el idealismo, el neo institucionalismo, la teoría de sistemas, el conductismo, la sociología histórica etcétera. En este trabajo nos enfocaremos únicamente en la teoría realista para explicar el proceso de militarización.

El realismo apareció como teoría académica a finales de la década de 1920. Su objetivo fue explicar la nueva realidad mundial generada por la Primera Guerra Mundial. Tiene su primera expresión en tiempos de la Grecia antigua, especialmente en el texto, "Historias de las Guerras del Peloponeso, escrito por Tucídides. Posteriormente, autores como Maquiavelo y Thomas Hobbes le hicieron reformulaciones para convertirla en parte de la filosofía política (Arenal, 1990, p.104).

Como podemos notar, el realismo tiene una larga tradición intelectual e histórica, y a lo largo del tiempo se ha ajustado a las nuevas circunstancias y condiciones de la realidad

internacional. Existen diferentes formas de pensar el realismo, de las cuales expongo brevemente algunas de sus propuestas.

De acuerdo con Timothy Dunne (2001) existen tres tipos de realismo entre ellos el realismo histórico, el realismo estructural y el liberal o neo-realismo. El realismo histórico o clásico fue desarrollado con base en las ideas de Maquiavelo en los albores de la concepción de la formación del Estado Nación, dicho realismo consiste en mantener una política con principios, y tener la capacidad política de adaptarse a los cambios reproducidos por y en el sistema internacional, siendo una de las corrientes del realismo que se frecuenta en los estudios de la ciencia política y la filosofía política, aunque esta corriente se limita entender el actuar político de los actores en la escena internacional (Dougherty y Pfaltzgraff, 1971, p.148).

Por su parte, el realismo estructural tiene como eje principal, vincular la naturaleza del hombre con la naturaleza del Estado, concibiendo como idea primaria la búsqueda interminable de poder, así como la supremacía del estado ante cualquier entidad supranacional o internacional, dejando atrás ideas como la justicia, la ética y lo moral (Waltz, 2000, p. 11).

En la década de 1970, el realismo estructural propone que la naturaleza del Estado recae y es el reflejo de la condición de maldad y egoísmo que posee el ser humano, siendo la composición de este un paralelismo que justifica y afirma el actuar del Estado mimetizado a la condición intrínseca de los individuos y a los intereses de los mismos (Dunne, 2001, p.113).

Por último, existe el realismo liberal, mejor conocido como Neorrealismo nacido a finales de la década de los 1970s y como vertiente de la lógica propuesta por el realismo estructural, argumentando que, pese a la condición del Estado, es posible la coexistencia de estos, sólo si se someten a las condiciones establecidas y leyes impuestas por los Estados hegemónicos (Dougherty y Pfaltzgraff 1971, p.150).

No obstante, las tres percepciones dentro del marco teórico realista, es notorio que cada una de estas visiones teóricas coinciden con el argumento central, el cual gira en torno al concepto de “poder”, el cual enmarca que las relaciones de los Estados dentro del escenario internacional se traducen en relaciones de poder (Salomón, 2002, p.12).

Cabe Señalar que el concepto poder, es meramente abstracto y ha motivado a diferentes autores a estudiarlo y definirlo, por ejemplo, Thomas Hobbes hace una analogía donde el Estado representa al monstruo mítico el "Leviatán" sugiriendo la capacidad de poder vertido sobre un ser de magnitudes sorprendentes y la fuerza que este representa (Foguel, 2007, p.12).

Max Weber quien se acerca a la política por medio de la sociología y la filosofía, propone lo siguiente: "Probabilidad de que un actor dentro de una relación social esté en posición de realizar su propia voluntad, a pesar de las resistencias". La definición weberiana del concepto poder es la más aceptada en el campo de estudio de lo político, pues la resumen en que es la capacidad de un actor en imponer su voluntad ante un grupo de sujetos. Esta definición es clara y aunque sencilla nos remite a la esencia del concepto (Weber, 2005, p.36).

Una definición más precisa, considero que es la de Laswell y Kaplan el cual acentúa la cuestión de los intereses de los actores, sobreponiendo estos, ante cualquier otro grupo, Kaplan define poder de la siguiente manera: "El poder es una relación en la cual una persona o un grupo puede determinar las acciones del otro en la dirección de los propios fines del primero" (Lasswell, y Kaplan, 1950, p. 86).

Autores como el francés Michel Foucault (2006) desarrollan teorías del poder desde la óptica social y filosófica. La importancia de definir este concepto incurre en que es un término base para entender la ciencia política, en este caso, el ejemplo que describo y considero necesario para comprender y en donde se evidencian de forma práctica las relaciones de poder entre los Estados, sin duda es el periodo de Guerra Fría.

## La Guerra Fría y el Realismo aplicado

Durante la Guerra Fría la corriente realista tuvo influencia decisiva en el diseño de la política internacional de las grandes potencias. Terminada la Segunda Guerra Mundial, la escena internacional se divide en dos grandes bloques de poder: por un lado, el bloque de occidente liderado por la nueva gran potencia, Estados Unidos, emergida como super potencia después de la "autodestrucción" europea; en contraparte, y como contrapeso político, ideológico, económico, militar y cultural surgió el bloque socialista, encabezado por Unión de

Repúblicas Socialistas Soviéticas (URSS) (Delicia, 2002, p. 8). En el sistema internacional surgido de la Segunda Guerra Mundial, las nuevas dinámicas interestatales exigían nuevos estudios que permitieran comprender la nueva realidad política internacional. Esos nuevos estudios estuvieron influenciados por la teoría realista.

La tensión generada por los dos bloques fue la antesala para un conflicto a gran escala que no llegó a ocurrir de forma directa, pero que estuvo latente debido la necesidad de las superpotencias por prevalecer sobre el contrario. A pesar de las diferentes ideologías entre occidente y los socialistas, el objetivo primario fue destruir a la potencial rival. De esta manera, términos como destrucción mutua asegurada (MAD), eran muy frecuentes en aquella época. La necesidad de explicar esta nueva realidad internacional, dio pie a que autores como Hans Morgenthau se enfocaran en consolidar la teoría realista y convertirla en la perspectiva dominante en gran parte de los estudios internacionales (Dunne, 2001, p.109).

Robert Keohane (1983) describe al realismo como el motor de los estudios de las Relaciones Internacionales ya que, según él, todo aquel análisis coherente de la política mundial requiere haber pasado bajo la óptica realista. Esta presta especial atención a temas como el poder, los intereses y la racionalidad (p. 19). Entre las características del pensamiento realista destaca la idea de que la naturaleza y condición del sistema internacional, se mantiene permanentemente en completa anarquía, sin actor dominante, que regule y mantenga el orden internacional. Dada la condición del sistema es comprensible la importancia de priorizar la seguridad nacional y la supervivencia del Estado y la autoayuda.

A diferencia del idealismo, el sistema internacional para el realismo es jerárquico y no horizontal, en pocas palabras el orden internacional se encuentra subordinado a los intereses y las relaciones de poder entre las potencias hegemónicas. Por ende, la corriente estructural realista no mantiene una relación de confianza con el Derecho Internacional, y pone en duda la efectividad de las Organizaciones internacionales. La idea de paz perpetua es utópica e inalcanzable, ya que la condición anárquica y conflictiva del sistema lo impide, la ausencia de un ente capaz de regular y sistematizar las relaciones entre Estados, siendo estos últimos quienes por voluntad cedan y estén de acuerdo con la creación de este. Aunque en la actualidad podemos identificar intentos que faciliten alcanzar la paz, es notoria la incapacidad de estos organismos para hacerla efectiva (Oro, 2009, p. 16).

Una característica fundamental de la teoría realista es la figura del Estado como el actor central dentro del Sistema Internacional, ya que en este reside y se concentra la mayor parte de los elementos de poder. Para Hans Morgenthau (1986) la naturaleza del Estado-Nacional se asemeja a la naturaleza del ser humano, en donde se actúa guiado por la "razón" además, el egoísmo y la búsqueda de poder, estas ideas se ven plasmadas en el pensamiento de Hobbes el cual explica que las relaciones interpersonales se reflejan en la realidad interestatal, es por esto que existe la imperante necesidad de supremacía por parte de los Estados (p. 38).

La supremacía, el equilibrio de poder, la supervivencia de los Estados, la hegemonía, *Status Quo*, son conceptos realistas que tienten significado en función del "concepto poder". El poder para el realismo es el eje sobre el cual gira toda la dinámica de la escena Internacional. La obtención y acumulación de poder va de la mano con el deseo de mantener el *status quo* del sistema internacional, permitiéndole a las potencias dominar a los Estados más débiles, o bien, destruir las áreas de influencia de otras potencias (Dunne, 2001, p.122).

El poder se concentra en tres vertientes, mejor conocidas como factores reales de poder. El principal es el factor militar, el cual representa la fuerza bruta del Estado. El segundo factor es el económico regularmente la potencias con mayor capacidad económica figuran como potencias y establecen las condiciones para los acuerdos comerciales y determinan el sistema financiero internacional. El tercer factor es la ventaja tecnológica que las potencias puedan alcanzar (Palacio, 2004, p. 4).

El poder militar es el más importante de los factores reales de poder al respecto, E. H. Carr mencionan lo siguiente: "La suprema importancia del instrumento militar descansa en el hecho de que la última ratio del poder en las Relaciones Internacionales es la guerra" (Arenal, 1990, p.129). La guerra es un instrumento más de los Estados, ya que permite reconfigurar el balance de poder dentro del sistema internacional, el conflicto es el elemento preponderante dentro de la escena internacional, al igual, es una constante que mantiene en boga de paz a las organizaciones internacionales y a los Estados mismos (Donelly, 2000, p.10).

En un sistema internacional anárquico, la supervivencia de los Estados es la prioridad máxima de estos, a lo largo de la historia los Estado han empleado diferentes medios para sobrevivir dentro del sistema; siendo la política exterior el vehículo por excelencia de los

Estados para satisfacer sus intereses. De esta forma, uno de los intereses más importantes para todos los Estados dada la condición enunciada del sistema, es la seguridad, este interés justifica la importancia del poder militar siendo este uno de los factores reales de poder que garantiza la soberanía y salva guarda la integridad de los Estados.

La seguridad nacional es el elemento clave el cual se encuentra intrínseco dentro de los intereses expresados en la política exterior de cada Estado, ya que esta se traduce en la supervivencia del Estado mismo; Es por eso que para garantizar dicha supervivencia y hacer efectivos sus intereses es importante mantener el poder y obtener más de este. La política exterior es una de las mejores herramientas para alcanzar y satisfacer los intereses de un Estado, aunque no es la mejor, ya que esta se encuentra supeditada a los cambios que se generen en el sistema internacional, modificándose en razón de las nuevas amenazas a la estabilidad política, económica, tecnológica y militar de los Estados (Oro, 2009, p.19).

El realismo en esencia no considera valores, ni principios, así como cuestiones de orden ético y aspectos morales, ya que, de acuerdo a esta visión, y bajo la perspectiva antropológica del Estado, la toma de decisiones y el actuar político se guía por intereses más que sentimientos y buenos valores. El conflicto es otro de los medios con los que cuenta el Estado para satisfacer sus intereses, para modificar el balance de poder dentro del sistema internacional; siendo estos de diferente índole y como antesala a una posible guerra, ya que el caos es parte de la condición del propio sistema internacional invadido por la anarquía.

A partir de 1945 el realismo se ha convertido en la esencia de la política exterior estaounidense, siendo esta visión la que pretende justificar el actuar de los Estados Unidos asumiendo un *status quo* como superpotencia en aquella época y que, desde entonces, motiva el actuar estadounidense en la preservación de su hegemonía a nivel internacional.

La teoría realista se transforma y adapta a las nuevas condiciones de la realidad internacional, en la década de 1990, Estados Unidos se consolida como súper potencia hegemónica, contando con los tres factores reales de poder: es una potencia militar, económica y tecnológica. terminada la Guerra Fría, no existía un Estado que funja como contrapeso a la hegemonía estadounidense (Oro, 2009, p. 21).

Kenneth Waltz, uno de los neorrealistas norteamericanos contemporáneos de mayor importancia, se ha dedicado a generar nuevas perspectivas dentro del marco neorrealista, y ha dado continuidad a la tradición teórica argumentando que las alianzas son posibles pero

que dentro de esas alianzas no se pretende la seguridad colectiva o el bien común sino el interés particular de los Estados, será este el que preponderé en los objetivos o metas a alcanzar por dicha alianza (Strinde, 2011, p. 11).

Además de las alianzas y la división del realismo político Waltz añade los conceptos de realismo ofensivo y defensivo, en donde el primer tiene como máxima la búsqueda de poder, con base en las mismas ideas establecidas por Morgenthau, mientras que la novedad recae en el concepto de realismo defensivo, el cual tiene como objetivo la seguridad del Estado dentro de su búsqueda de poder generándose así un debate intrarealista (Petrollini, 2012, p.1).

Es común encontrar en el discurso político estadounidense una postura muy liberal, en favor de la democracia, la cooperación internacional, la paz internacional, la seguridad colectiva y elementos claves propios de la teoría idealista –Neoinstucionalismo-. Pero en la práctica, los Estados Unidos es totalmente distinto, partiendo del hecho de la ausencia de respeto hacia a las instituciones y diferentes organismos internacionales, así como las faltas al Derecho Internacional, - dentro de este capítulo se ejemplificará esta afirmación- además del uso del conflicto como medio de obtención de poder, y el debilitamiento enemigo. Estas sin duda son las claves constitutivas de la teoría realista y coinciden con el actuar político estadounidense y son las bases de la política exterior estadounidense.

A finales del siglo XX Estados Unidos adquirió el estatus de potencia mundial y Estado hegemónico, el legitimar la guerra no ha sido sencillo, pero sus intereses son claros, el más importante de estos ha sido alcanzar y mantener la hegemonía global, las acciones hacia el exterior han demostrado la capacidad de esta potencia. (Arenal, 1990, p. 114).

En 2001 el concepto de seguridad nacional dominó y prevaleció en la política interna y externa estadounidense, para este año los Estados Unidos indiscutiblemente se mantenían como la potencia hegemónica y sin duda la más influyente a nivel mundial, apenas una década antes transitaríamos de un mundo bipolar a un modo más global y poco se vislumbraba la idea de una guerra o conflicto contra dicha potencia, hasta el 11 de septiembre de ese año. El terrorismo se convirtió en el archienemigo estadounidense, siendo este el componente que dio pie al desarrollo y legitimación de doctrinas como la de “ataque preventivo” patentada por el ex presidente George W. Bush, quien en 2003 justifica la intervención estadounidense en Afganistán e Irak con acusación de que dichos Estados

poseían armas de destrucción masiva. El objetivo de fondo era destruir y minimizar la capacidad de ataque del enemigo, legitimando la hegemonía estadounidense además daba muestra del poderío militar estadounidense (Pascual, 2005, p. 78).

El Derecho Internacional, y organizaciones internacionales en defensa de la paz se encontraron limitadas a sancionar la intervención estadounidense en 2003, la violación a los derechos humanos y tratados internacionales dan muestra que el enfoque teórico neo institucional se queda obsoleto para explicar la realidad internacional, El Estado, la seguridad nacional, los factores reales de poder, la obtención y preservación del poder así como los intereses del Estado son elementos que explican y nos permiten comprender las Relaciones Internacionales y la realidad internacional. Estos son parte de las razones por las cuales la teoría realista y recientemente la corriente neorrealista predominan en los estudios internacionales, en resumen, nos ayuda a entender el actuar de los Estados Poderosos. Una teoría estatista por excelencia en donde la realidad internacional es escenificada como un juego de poder de suma cero entre los Estados.

El poder será la moneda de cambio para la política realista. La divisa que todo Estados poderros busca obtener y acumular con el fin de proteger su soberanía y su seguridad. El poder militar y económico son las armas que tienen los Estados para enfrentar la adversidad que pueda presentarse en el sistema internacional anárquico (Pascual, 2005, p. 84).

## 1.2- Militarización del ciberespacio y el neorrealismo

En el siguiente apartado se explica la relación entre el proceso de militarización del ciberespacio y el Neorrealismo. La militarización del ciberespacio es una forma de política internacional poco estudiada, y por tanto novedosa, dentro de los estudios internacionales. Con esta política, las potencias buscan disuadir a sus enemigos de cualquier posible conflicto internacional, lo que ha desatado tensión entre las grandes potencias tecnológicas. En este apartado se describe la evolución de la internet y la creación de algo tan abstracto y complejo como lo es el ciberespacio. En el contexto de la era digital, el ciberespacio forma parte literalmente de la realidad internacional. El ciberespacio es el nuevo terreno del conflicto político, económico, cultural y militar entre los Estados.

El ciberespacio es un entorno completamente virtual dotado de una ingeniera que escapa a la comprensión de lo tangible representado por elementos compuestos de unos y ceros; El cual se ha convertido en una zona estratégica y competitiva, en donde se ha generado una serie de acontecimientos que han impactado de forma significativa en el mundo real y tangible, tal es así el alcance, que existe una exportación de conceptos hacia este nuevo campo de investigación, tal es el caso de elementos como armas cibernéticas, ciberguerras, ciber-terrorismo, hactivismo, ciber-comandos, cibe-erejercito, ciber-delitos, ciberseguridad, y todo un nuevo argot que busca dar nombre y explicar de forma precisa que ahí ocurre.

El proceso de militarización del ciberespacio está en función de la necesidad de los Estados de subsanar sus vulnerabilidades en el mundo virtual. Esta situación ha impulsado a las grandes potencias tecnológicas a elaborar estrategias para contrarrestar cualquier amenaza surgida en el espacio cibernético, lo que en esencia justifica la incursión de los ejércitos nacionales en el Ciberespacio. Respecto al uso de la teoría realista en el estudio de la militarización del ciberespacio, autores como McEvoy (2010) ya señalan la existencia de analistas Ciber-realistas y Ciber-institucionalistas, los cuales tienen una forma muy particular de entender el mundo virtual (p. 382).

Por otra parte, según el Diccionario de la Real Academia Española, define la internet como: “Red Informática mundial descentralizada formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación”. Cabe señalar que la RAE acepta el uso indistinto de los artículos “el” o “la”, aunque en este trabajo se empleará el artículo femenino, ya que internet se refiere a “la red” y este se encuentra en femenino” (Real Academia Española, 2005). Asimismo, la RAE define el Prefijo “Ciber” como el acortamiento del adjetivo cibernético, que forma parte de términos relacionados con el mundo de las computadoras u ordenadores y de la realidad virtual, se recomienda su uso en la creación de nuevos términos pertenecientes al ámbito de las comunicaciones por Internet (Real Academia Española, 2005).

Para entender mejor el ciberespacio es importante tener claridad de cómo funciona la internet. En este caso se trata de una herramienta tecnológica que fue diseñada con fines militares. Su aparición ocurrió durante la Guerra Fría (1945-1990), un período de la historia mundial cuando los dos bloques rivales, el comunista y el capitalista, emprendieron una

carrera tecnológica que dio como resultado las tecnologías de la información que hoy son parte esencial de la vida cotidiana.

Una de las tecnologías de mayor avance fue la telecomunicación. A principios de la década de 1970, el ejército estadounidense ya daba uso militar a las diferentes formas de telecomunicaciones, sobre todo con el desarrollo de radares o sistemas de localización global. Entonces, el ejército estadounidense ya innovaba en el desarrollando de los primeros sistemas computacionales sofisticados y simultáneamente estructuraba una red de transmisión de información digital conocida como *Advanced Research Projects Agency Network* (ARPANET, por sus siglas en idioma inglés), que fue el inicio de lo que ahora conocemos cómo internet (Jordan T. 1999, p.3).

ARPANET fue ideado por el *Defense Department's Advanced Research Project Agency* (DARPA) con el fin de entrelazar nodos y puntos de conexión entre una computadora maestra capaz de recibir, almacenar y distribuir la información de una forma segura (Derek, 2011, p. 239).

Posteriormente ARPANET evolucionó en uno de las herramientas más representativas del nuevo proceso de globalización: la Internet. Hasta 1990, ARPANET estuvo reservada para el ejército y la industria militar de Estados Unidos, y en menor medida para la clase política y las personas con alto poder adquisitivo de ese país. El mundo empezó a transitar hacia la nueva era tecnológica (Jordán, 1999, p.23).

En sus inicios, la internet fue utilizada para agilizar y proteger la información mediante algoritmos y datos cifrados en caso de un ataque nuclear. La importancia de estar comunicados para combatir la amenaza soviética en tiempo real era una de las necesidades básicas de los aliados en occidente. Aunque el uso primario de la internet fue agilizar y proteger la información, y en caso de ser necesario utilizarla como arma estratégica, a principio de la década de 1990 encontró un uso importante en el comercio. Fue entonces que fue introducido la famosa WWW (*World Wide Web*). (Jordán, 1999, p.26).

La internet es el motor de la globalización. A principio del siglo XXI, la mayor parte del mundo ya está conectado a la Internet, al tiempo que los Estados con un alto desarrollo tecnológico diversificaron y ampliaron sus usos. La exclusividad cedía paso a la expansión mundial de la red. Las personas de todos los sectores sociales ya hacían uso de esta tecnología. Lo mismo ocurrió para las empresas, universidades, bancos, hospitales,

organismos del sector público, organizaciones civiles. De esta forma, la evolución tecnológica de la internet ocurre de forma acelerada, facilitando con ello el acceso a la información a gran parte de la población de la mayoría de los países. Al respecto, según estimaciones del Banco Mundial (2010), Estados Unidos el número de usuarios de internet creció 30% entre 1990 y 1997; entre 1998 y 2007, ese porcentaje llegó a 74%; y a partir de 2008, creció más de 150%. Este dato permite dimensionar el crecimiento de la internet, y como esta tecnología ha penetrado en la vida de los ciudadanos estadounidenses.

Sin embargo, a escala mundial las cifras cambian. Tomando el informe del Banco Mundial antes citado, la población mundial de usuarios de internet pasó del 3.15% en 1998 a 32.77% en 2008. La cantidad de usuarios de Internet ha crecido poco más de diez veces y sigue en ascenso (Banco Mundial, 2012).

En la tabla número 1 se ilustra el alcance de la internet en las principales regiones del mundo, así como el porcentaje de usuarios como proporción de la población mundial. Según esos datos, las tres regiones con más usuarios de internet son Norteamérica, Europa y Asia; esta última incluye a las principales potencias tecnológicas en plataformas para la red (China, Rusia, India, Corea del Sur y Japón). Europa queda como la segunda región con más usuarios, en donde el ciberespacio ha sido tema importante dentro de la agenda de la Unión Europea. La región norteamericana tiene menor población que las otras dos regiones, aunque ahí está conectada a la red la mayor cantidad de usuarios; es claro que el liderazgo en este campo lo tiene Estados Unidos.

Tabla 1.- Estadísticas de uso y población usuaria de la internet

| Estadísticas de uso y población usuaria de la Internet<br>Actualizado al 31 de Diciembre de 2017 | | | | | | |
|---|---|---|---|---|---|---|
| **Regiones del Mundo** | **Población Estadística 2018** | **Porcentaje de Población Mundial** | **Usuarios de Internet Diciembre 2017** | **Porcentaje Integración de la población** | **Porcentaje de Crecimiento 2000-2018** | **Porcentaje de Usuarios de Internet** |
| África | 1,287,914,329 | 16.9 % | 453,329,534 | 35.2 % | 9,941 % | 10.9 % |
| Asia | 4,207,588,157 | 55.1 % | 2,023,630,194 | 48.1 % | 1,670 % | 48.7 % |
| América Latina y el Caribe | 652,047,996 | 8.5 % | 437,001,277 | 67.0 % | 2,318 % | 10.5 % |
| Europa | 827,650,849 | 10.8 % | 704,833,752 | 85.2 % | 570 % | 17.0 % |
| Medio Oriente | 254,438,981 | 3.3 % | 164,037,259 | 64.5 % | 4,893 % | 3.9 % |

| | | | | | | |
|---|---|---|---|---|---|---|
| Norte América | 363,844,662 | 4.8 % | 345,660,847 | 95.0 % | 219 % | 8.3 % |
| Oceanía | 41,273,454 | 0.6 % | 28,439,277 | 68.9 % | 273 % | 0.7 % |
| Total Mundial | 7,634,758,428 | 100.0 % | 4,156,932,140 | 54.4 % | 1,052 % | 100.0 % |
| Fuente: https://www.internetworldstats.com/stats.htm Revisado el 24/07/18. | | | | | | |

Justamente los países mencionados son aquellos que mantiene una clara ventaja tecnológica a nivel regional y se colocan como potencias tecnológicas, ya que estas trabajan en los medios y herramientas que les permitan el dominio del ciberespacio. En el terreno virtual se encuentra China y Estados Unidos como los principales protagonistas de ciber-ataques perpetrados entre ellos o lanzados a otros Estados.

Sin lugar a dudas, la internet ha revolucionado la forma de comunicarnos, ha modificado sustancialmente nuestra vida diaria y la forma en cómo vemos y entendemos el mundo. La información fluye ininterrumpidamente y más rápido que hace una década. Este avance tecnológico ha sido un parteaguas no sólo en nuestras vidas, sino también en los sistemas políticos, económicos, militares del planeta.

El ciberespacio es visto como un terreno clave a conquistar, así como primero lo fue el espacio terrestre, posteriormente el marítimo, a partir del siglo XIX se busca el dominio del espacio aéreo, a mediados del siglo XX el espacio exterior será el objetivo a alcanzar por las superpotencias de aquella época y ahora en el siglo XXI el mundo virtual se ha convertido en la manzana de la discordia principalmente entre China y Los Estados Unidos (Vercelli, 2000, p. 19).

El dominio del ciberespacio es una prioridad compartida por las potencias tecnológicas, especialmente de aquellas que aventajan al resto de los Estados. Al igual que en el sistema internacional, en el ciberespacio impera la anarquía, aunque de forma diferente, pues ahí participan otro tipo de actores que atentan contra la seguridad y la estabilidad de los Estados nacionales: por ejemplo, los *hacker*-activistas y ciber-terroristas. Por lo tanto, en el ciberespacio los conflictos no se limitan a Estados contra Estados, ahora es el Estado enfrenta amenazas como ciber-terroristas, *hackers, crackers,* hactivistas, y otras fuerzas de inteligencia de otros Estados. Nuevas amenazas y retos nacen para el Estado.

Uno de los primeros problemas identificados en el ciberespacio es la incapacidad de regular jurídicamente las actividades y las dinámicas que ahí ocurren. Más complejo aún es controlar el contenido compartido en la red, por ejemplo la propaganda política extremista.

Derivado de lo anterior, una de las primeras controversias surgidas es la implementación de algún tipo de legislación. El caso Napster de 1999, fue una plataforma que rápidamente se convirtió en uno de los servicios de distribución de música más importantes en Norteamérica. Mediante este programa, con arquitectura P2P (*people to people*) se compartían SIN COSTO archivos en formato mp3. La Asociación de la Industria Musical de Estados Unidos (RIAA, por sus siglas en inglés), acusó que las operaciones de Napster violaban los derechos de autor de los creadores de música, por lo que y arremetió legalmente contra las prácticas de la empresa. La demanda concluyó en 2001 con una resolución a favor de RIAA (Varcelli, 2004, p.37).

Otro caso similar ocurrió en 2010, ahora con el sitio de almacenaje y distribución de archivos llamado Megaupload. En este caso fue desarrollada una nueva legislación en el congreso estadounidense para proteger los intereses del sector privado, que a lo largo de casi dos décadas exigieron regulaciones para este tipo de empresas que operan no solo en Estados Unidos. Exigían restringir el modo en que internet es usado para distribuir productos sin el pago de derechos a sus creadores o propietarios de los derechos de comercialización – especialmente música, películas y libros. Curiosamente, el resultado de campaña y la consecuente prohibición de empresas como Magaupload, favoreció la creación de nuevas empresas como Netflix.

Mencionamos los casos de Napster y Megaupload porque a principios de 2010, el sistema de justicia de Estados Unidos no consideraba la idea de que el ciberespacio y lo ocurrido ahí llegara a convertirse en un peligro o amenaza potencial para la estabilidad política y la seguridad nacional de ese país. Ambos casos fueron disputas comerciales y de propiedad intelectual entre las grandes corporaciones, no por la protección del interés social o de la seguridad nacional.

A finales de la década de 1990 Estados Unidos priorizaba las necesidades económicas y el libre comercio, a través de tratados de comerciales con otros Estados. La situación económica nacional era su prioridad en la agenda internacional. Luego, en septiembre de 2001 para ser precisos, la seguridad nacional fue puesta en alerta por los ataques terroristas,

lo que forzó a un cambio en las prioridades de la política internacional de ese país (Palacio, 2004, p.10).

Después de los atentados de septiembre de 2001 es posible observar la vulnerabilidad de la potencia mundial. En las semanas siguientes a dicho evento, el tema de la seguridad se convirtió en el eje de las nuevas políticas estratégicas, dentro de las que destaca la "Agenda Digital" por la que el Ciberespacio se convirtió estrictamente en un campo político con agenda propia.

Las amenazas en el ciberespacio son tres principalmente. En primer lugar hay ingobernabilidad, pues no existe institución que sancione a los Estados que cometen ataques en el espacio virtual. La segunda es la ausencia de obstáculos que bloqueen el flujo de información o impongan límites los ciberataques realizados por Estados *o hackers*. La tercera amenaza es la presencia de ciberarmas contra las que no se dispone de instrumentos defensivos verdaderamente efectivos. Estas amenazas no pueden ser controladas jurídicamente, pues el desarrollo tecnológico avanza a gran velocidad, lo cual hace que una ley para el ciberespacio quede obsoleta en un corto tiempo (McEvoy, 2010, p. 3).

Tanto la ingobernabilidad, la ausencia de obstáculos y la presencia de ciberarmas convierten al ciberespacio en un lugar anárquico, y aunque cada vez más restringido, esta situación refleja el peligro que representa para la seguridad nacional de los Estados. Las amenazas son constantes, lo que estimula a los Estados a invertir grandes sumas de dinero para sostener, por ejemplo, la operación de los cibercomandos –más adelante trataremos con más detalle a esta nueva rama militar.

Ahora bien, no sólo los gobiernos enfrentan amenazas en el ciberespacio, también lo padecen las industrias y empresas transnacionales. Hasta ahora se han documentado cientos de casos de robo de información industrial, principalmente por parte de China y Rusia. Se trata de "espionaje Industrial" que tiene como objetivo robar información de grandes empresas de tecnología o descubrir secretos comerciales (Casar, 2012, p.12).

Al igual que sector privado es asediado por ciberataques, los servicios gubernamentales son atacados con regularidad. Por ejemplo, existen reportes de ataques a sitios *web* de embajadas que han logrado "colgar en la red" información escandalosa de altos mandos de la política, o pornografía en los sitios oficiales de gobiernos locales o congresos nacionales.

Debido a las acciones en la internet que atentan contra la seguridad nacional, la economía de las empresas o las actividades político-administrativas de los gobiernos es que los ejércitos ha incursionado en el ciberespacio, con el fin de proteger la información y la infraestructura estratégica, además de procurar contrarrestar ataques provenientes de cualquier parte de la geografía mundial y de forma anónima.

La teoría del colapso y la estrategia de ciberseguridad estadounidense.

Richard Clarke es uno de los más influyentes escritores sobre el ciberespacio y quien los identifica como un campo de batalla y un nuevo terreno de conflicto. En su libro *Cyber War* alerta de las posibles consecuencias de no procurar la seguridad en la red. También describe escenarios "catastróficos" por los que sugiere que un ataque cibernético tiene la capacidad de dejar en estado crítico a un país a tal grado de que esto pudiera ser la causa potencial de un conflicto nuclear (Clarke y Kanake, 2010, p.5).

Clarke expone en su obra que cuando en 2001 se desempeñaba como consejero presidencial en materia de seguridad del ciberespacio –fue el primer consejero de este tipo en Estados Unidos- él y su colega Robert Kanake, quien era un agente especializado en las nuevas amenazas del siglo XXI en el Departamento de Seguridad Nacional, coincidieron en desarrollar un discurso de corte militar conocido como la "teoría del colapso" (Clarke y Kanake, 2010, p. 3).

Según Rid (2013), la teoría expuesta por Clarke está determinada y claramente influenciada por la teoría de la disuasión, la cual fue parte de la estrategia militar estadounidense durante la Guerra Fría. La teoría de la disuasión consiste en la creación de posibles amenazas respecto al uso de armamento nuclear para alterar las posturas de las otras potencias (p. 16).

Por su parte la teoría del colapso consiste en una doctrina de corte militar dentro del discurso estadounidense de la seguridad nacional. Pretende legitimar la estrategia de control total de la internet como medida preventiva ante la emergencia de cualquier posible ciberamenaza. En la obra de Clarke se presume que las amenazas en el ciberespacio son reales, y que es deber del aparato gubernamental y militar hacerse cargo de la defensa de la seguridad nacional (Rid, 2013, p. 28). Desde la perspectiva internacional es cierto que

organizaciones como la del Tratado del Atlántico Norte (OTAN) advierten que la posibilidad de que la próxima guerra mundial se confronte en el mundo virtual es muy probable ya que, de acuerdo con datos de la Oficina Federal de Investigación (FBI, por sus siglas en inglés), 108 países contaban con la capacidad tecnológica para generar algún tipo de ciberataque (Germain, 2010, p.528).

Esos datos del FBI permiten valorar la magnitud del riesgo y de las amenazas que enfrenta la seguridad nacional de cualquier Estado: cualquier país puede ser blanco de un ataque, desde cualquier lugar del planeta, por cualquiera de los 108 Estados que cuentan con la capacidad de realizar un ciberataque. Es por esto que potencias militares y tecnológicas como lo son China y Estados Unidos se han dedicado a blindar el ciberespacio con el objetivo de minimizar cualquier amenaza latente proveniente de la red.

Clarke también reconoce la existencia de comandos militares especializados, los cuales ya operan en varios países desde principios de la década de 2000. Esos cibercomandos han sido creados de forma discreta, y algunos de ellos ya han comenzado a vulnerar y sabotear los sistemas de control aéreo militar de los gobiernos enemigos de los países para los que trabajan (Clarke y Kanake, 2010 p. 18).

Así pues, la militarización del ciberespacio es, para la teoría del caos, la única respuesta racional para encarar a las nuevas amenazas en el ciberespacio. El Estado no es el único actor que maneja ciberarmas, también existen grupos de expertos informáticos, patriotas, activistas, y los famosos *trolls*, que están discupestos y tienen la capacidad para realizar ciberataques. La vulnerabilidad de los sistemas tanto militares, como de servicios (electricidad, agua, oleoductos, gaseoductos, telecomunicaciones) el sistema bancario y financiero, plantas industriales, servicios de transportes, y los sistemas computarizados están a merced de cualquier sabotaje a su funcionalidad, generando caos nacional (Clarke y Kanake, 2010, p.20).

Para finalizar esta sección es importante señalar que Estados Unidos, en un informe de 2011 elaborado por el gobierno de Barack Obama y publicado por la Casa Blanca, menciona que todo aquel ataque perpetrado desde el ciberespacio y que atente contra la seguridad nacional será considerado como acto de guerra. Esta declaración deja clara la postura estadounidenses al respecto (Mehan, 2012, p.18). No hay que descartar que la ciberseguridad es ya un tema importante para los gobiernos nacionales de la Unión Europea,

así como para los gobiernos de Brasil, Corea del Sur, Corea del Norte, Rusia, Irán, Israel, India, Japón, entre otros. Este nuevo escenario de las relaciones internacionales contempla la posibilidad de una Ciber-Guerra Fría (Rid, 2013, p. 15).

## 1.3 Neorrealismo, amenazas, vulnerabilidades, riesgos, ganancias-pérdidas en la lucha por el poder en el ciberespacio

Es importante clasificar los objetivos de los diferentes tipos de ciberataques, pues estos cumplen diferentes propósitos. Al respecto, podemos identificar al menos tres tipos, a saber: el sabotaje, el robo de información, y el espionaje.

El sabotaje en el ciberespacio se refiere al daño en estructuras críticas de una empresa o parte de algún órgano de gobierno, empleando virus capaces de dañar todo un sistema completo computacional, o permitir el acceso a control remoto de alguna red de ordenadores (Espinoza A. 2010, p.1). Uno de los casos más famosos de sabotaje que han sido estudiados fue el ocurrido en Irán, en 2010. Este caso llamó la atención pues rompió con el esquema clásico de los ataques convencionales tierra-mar-aire. En 2010, el gobierno iraní desarrollaba un programa nuclear, el cual era visto como una amenaza a la seguridad regional e internacional de varias potencias. La política de desarrollo de tecnología nuclear iraní también generó controversia en diferentes organizaciones internacionales como la ONU, en la Agencia Internacional de Energía Atómica (AIEA) y en la Organización Internacional de Energía atómica (OIEA). En esos organismos se discutía si Irán debería continuar con su programa o suspenderlo hasta conformar que fuera para fines pacíficos (Espinoza A. 2010, p.1).

Mientras la controversia se mantenía en la agenda internacional, se presume que Israel, mediante uno de sus cibercomandos, desarrolló un virus sofisticado para afectar los sistemas computacionales de las instalaciones nucleares iraníes (Cymerman. 2010, p.1). El virus informático más letal creado hasta aquel entonces era conocido como *Stuxnet* el cual, según Thomas Rid, pudo ser conocido como el "Hiroshima" de la ciberguerra ya que daño más del 60% del sistema computacional de las instalaciones nucleares iraníes. Ese fue el

ataque informático más sofisticado y con mayor impacto en la historia de la internet (Rid, 2013, p.6). La empresa especializada en seguridad informática, *Symantec Corporation*s *Internacional*, declaró que los servidores iraníes fueron infectados y prácticamente dañados en los dos objetivos del sabotaje: primero, la planta nuclear en Natanz --encargada del programa de enriquecimiento de uranio—y: segundo, el reactor de agua ligera en la ciudad de Bushehr (Beaumont, 2010, p.1). Lo relevante de este caso fue que por primera vez en la historia se desarrolló e implantó un virus capaz de infiltrar en los sistemas de seguridad y control de infraestructura públicas. (Espinoza, 2010, p.1).

Otra forma recurrente de sabotaje, aunque más "primitiva", es la conocida como ataque DDoS, o "ataques de denegación del servicio". En este caso, el objetivo es masificar el número de visitas a un sitio web en particular y de esta forma saturar los servidores, generando un colapso de la página, e interrumpiendo los servicios de internet que ofrece a sus usuarios.

Por otra parte, el segundo tipo de ciberataque es el robo de información. Regularmente este tiene como víctima a las grandes corporaciones y multinacionales como *Apple, Microsoft, Sony*, Instituciones Bancarias y financieras, etcétera. El robo de información es gestado por "piratas informáticos", quienes roban información para eventualmente venderla a organizaciones criminales y grupos terroristas. Cabe puntualizar que este tipo de ataques cibernéticos pertenecen a catálogo de ciberdelitos, y la mayoría de las veces no afecta de forma directa a la seguridad nacional.

Finalmente, el espionaje ha desatado controversias en la escena internacional, pues no siempre es realizada por gobiernos, ahora también por activistas sociales. Uno de los ataques de ciberespionaje más famosos ocurrió en Estados Unidos y puso en jaque a la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) de ese país.

En el caso del ciberespionaje realizado por gobiernos, la justificación es que lo realizan basados en la necesidad de garantizar su seguridad nacional. Los servicios de inteligencia y contra inteligencia son las encargadas de estas actividades. Esas oficinas comprenden que el punto crítico del espionaje es la ventaja que se puede adquirir sobre el enemigo, adelantándose a los movimientos de este y conociendo tanto las debilidades como fortalezas del oponente (Maness y Valeriano, 2013, p.6-9).

Dentro de la línea del ciberespionaje, en 2010 el gobierno de Estados Unidos protagonizó uno de los más escandalosos y bochornosos momentos para su diplomacia. Ese año fueron filtrados a la prensa numerosos informes de las embajadas estadounidenses de todo el mundo, exponiendo y evidenciando la arrogancia y prepotencia de sus diplomáticos y funcionarios de alto nivel.

El caso, conocido mundialmente como *Wikileaks*, abrió las puertas de las oficinas de gobierno, mediante un trabajo de periodismo impresionante, y permitió conocer el sistema internacional desde la perspectiva estadounidense. *Wikileaks* comprometió la posición hegemónica estadounidense desde la comodidad de un ordenador en casa. El grupo que tramó la operación estuvo compuesto por un grupo de personas alrededor del mundo, la mayoría de las cuales aún se encuentran en el anonimato a excepción de su fundador, Julian Assange, preso en Inglaterra. Este ciberactivista de origen australiano posee en su poder información sensible como seguro de vida. Pasó más de dos años asilado en la embajada de Ecuador en Londres, y luego entregado a la policía británica por el gobierno ecuatoriano (Cuba Debate, 16 de agosto de 2018 p. 1).

El tema *wikileaks* es abordando con mayor detenimiento en el tercer capítulo. Ahí profundizamos en las consecuencias de este acontecimiento para el gobierno y la seguridad de Estados Unidos. Lo relacionamos en la serie de eventos que han marcado y dañado la imagen de los Estados Unidos en la escena internacional desde 2010.

Como se puede observar el uso de la inteligencia y los ciberataques son multipropósito, van desde el daño físico a los equipos, al *software*, o robar o conocer datos íntimos de la potencia rival. En esencia, consideramos, la Guerra Fría ha sido transferida al mundo virtual. Una guerra virtual puede estallar desde cualquier parte del mundo y, lo más preocupante es que se desatará en el anonimato de los perpetradores. El ciberespacio está cuasi conquistado por las potencias tecnológicas, lo que estimula el ambiente anárquico en la red. Como ha ocurrido en el escenario mundial, en la *web* nos encontramos un sistema multipolar y globalizado, en situación de ciberguerra permanente.

Derek Gregory (2011) define a la ciberguerra como *The Everywhere War*. Se trata de la guerra en la que cualquier persona con acceso a la red y un poco de conocimiento en informática se convierte en un enemigo potencial para el Estado y las empresas. Los ataques

realizados pueden ser ejecutado en cualquier parte del mundo y tener una repercusión a miles de kilómetros de distancia de donde fueron ejecutados (p. 240).

El ciberespacio no está exento de ser objeto de conquista por parte de los Estados, aquel mundo virtual en donde muchos vislumbraban ideales como la libertad de expresión, la privacidad, la facilidad de comunicación y demás ventajas que nos permite la internet ahora estás mismas libertadas son las que mantienen en jaque a potencias mundiales como China y Estados Unidos.

Los ejemplos y datos expuestos anteriormente nos permiten asimilar cuán importante es el internet en la vida social, política y económica, los peligros y amenazas que representan para los Estados. Hablar de 108 países con la capacidad de ejercer un ciberataque quiere decir que existen más países de involucrarse en una guerra en el mundo virtual que en el mundo físico.

El avance de las tecnologías y telecomunicaciones es más veloz que nunca. El desarrollo de dispositivos móviles a partir de la primera computadora lleva prácticamente de medio siglo. Durante todo ese tiempo es posible observar que no hay un organismo que regule los fenómenos desarrollados en el ciberespacio, dejando a los Estados y sus ejércitos a actuar según sus capacidades y responder en función de sus intereses a la inseguridad en el espacio virtual.

Es posible identificar elementos propios del realismo clásico, identificamos como el Estado como principal actor dentro y fuera del mundo virtual, además de una incompetencia de las organizaciones internacionales para resolver conflictos a nivel internacional, la seguridad y la soberanía son elementos de suma importancia para las potencias tecnológicas.

Tabla 2.-Tabla comparativa idealismo vs realismo y las perspectivas sobre el ciberespacio.

| | Idealismo | Realismo |
|---|---|---|
| Territorio | Extraterritorial, un mundo virtual sin relación directa con el mundo real. | Territorio que funje como parte extensión del mundo real y espacio de poder que pertenece al Estado |
| Poder | Estructuras subersivas de poder | Fortalecimiento de estructuras de poder ya existentes. |
| Identidad Nacional | Incorporeo y Grupos anonimos, Ciudadanos del Internet (*Netizen*) | Civiles desprotegidos, representantes de grupos |

| | | |
|---|---|---|
| | | terroristas, comunidades yihadistas, Internet es una nación en construcción. |
| Credibilidad | Irrelevante | Suma cero, espacio de protección. Puede ser propiedad |
| Información | Para ser compartida | Arma para disputa territorial, con derecho y legitimar los ataques preventivos. |
| Regulación | Normas comuntirias | Estados Unidos como Estado hegemónico. Quien propone las reglas. |

*Figura 2. Fuente: McEvoy 2010. p. 387.*

La hegemonía y el *status quo* estadounidense penden de un hilo. El poder económico, político y militar que mantiene China poco a poco ha ido superando al de Estados Unidos; el ejército y las agencias gubernamentales estadounidenses como la CIA, el FBI y la NSA, han apostado al ciberespacio como una herramienta de control, y protección a diferentes problemas que en la actualidad enfrenta Estados Unidos de América.

El ciberespionaje ha sido el arma de la que se ha valido el gobierno estadounidense para mantener su hegemonía, el conocimiento de las estrategias y planes de sus competidores políticos y económicos (China, Rusia, Brasil, India, Irán y Japón), para aventajarse al movimiento del rival.

El realismo explica y da razón de las acciones ejercidas por parte de los Estados Unidos tal y como se exhibe en la siguiente tabla la cual hace un contraste entre la postura idealista y realistas respecto al tema del ciberespacio.

La tabla número 2 permite observar que en la óptica realista, el ciberespacio es una extensión más del mundo real, por ende el poder es un elemento que también está ahí presente. Asimismo, es importante la protección de las ciberestructuras de las que dependen los sistemas eléctricos, financieros y militares. Además, se debe resguardar la información que circula en la red, redirigiendo mensajes que determinen o manipulen el comportamiento social. Se recalca que en este espacio las amenazas no son exclusivas de Estados sino,

también de civiles que pueden contar con la capacidad de vulnerar o sabotear maniobras del ejército en el ciberespacio.

Otro tema que preocupa a los actores internacionales es el desarrollo de armas en el ciberespacio. Como se ha mencionado, la vasta cantidad de información circulando en el puede llegar a ser falsa y tendenciosa de acuerdo al interés de quien la presente lo cual puede promover reacciones y movimientos sociales que atenten contra la estabilidad nacional.

Internet es un medio global de comunicación. Esto nos da la pauta para señalar que actores nacionales u organismos pueden recurrir a la manipulación de la información que circula en este entorno intensiones de legitimar alguna acción política o bélica en contra de cualquier Estado o grupo. Es posible difundir propaganda intensivamente y hacer viral un punto de vista o cierta interpretación de acontecimientos que favorezcan o perjudiquen la percepción sobre un hecho u otro. La internet también es conocida como el quinto poder por expertos como Rid (2012), Maness y Valeriano (2013) ya que supera el alcance de difusión de cualquier televisión, radio o medio impreso.

El juego político, las relaciones económicas, las formas de comunicarnos, nuestra cultura y el conocimiento se han extendido hasta el ciberespacio, es inevitable soslayar que existe un lugar más allá de lo que nuestros sentidos perciben, es complejo imaginarnos una serie de datos viajando a una velocidad inimaginable a través de una red tan extensa y completa.

En resumen, el proceso de militarización del ciberespacio es un fenómeno que no ha pasado desapercibido por los estudios realistas de la política internacional. La seguridad nacional, la soberanía, el derecho a la información, la privacidad, son elementos que se encuentran en juego y en conflicto por las nuevas amenazas generadas en este mundo virtual.

# CAPÍTULO II.- SEGURIDAD INTERNACIONAL EN EL CIBERESPACIO

El objetivo de este capítulo es identificar y explicar cuáles han sido las mayores amenazas que ha enfrentado el sistema internacional en el ciberespacio, así como los retos que enfrentan los Estados. Para esto, el capítulo se dividirá en cuatro apartados. En el primero se establece la importancia de la relación de seguridad internacional con el ciberespacio como nuevo campo de conflictos, en el segundo se destacan los antecedentes jurídicos que han pretendido normar este mundo virtual; en el tercer apartado se describen las causas y consecuencias de los conflictos más relevantes ocurridos en las últimas décadas en este espacio; y el cuarto y último apartado plantea los nuevos retos y amenazas que se divisan para el sistema internacional.

## 2.1.- El ciberespacio y la seguridad internacional

La seguridad Internacional ha sido una de las mayores preocupaciones de los Estados y Organismos Internacionales, desde finales de la Segunda Guerra Mundial, el desarrollo de armas nucleares, de alto alcance y químicas transforma constantemente el espectro de la guerra, las nuevas formas de enfrentar los conflictos armados manifiestan amenazas claras a la estabilidad del sistema internacional, así como a la paz mundial.

La idea de una posible guerra nuclear durante el período conocido como Guerra Fría (1945-1989) replanteó la idea de "seguridad". Este concepto ha estado adherido al de "paz internacional". Sin el protagonismo tradicional del Estado en la agenda internacional, los lineamientos de la política exterior cambian en cuanto a las estrategias, sobre todo al incluir nuevos aliados y nuevos enemigos no estatales.

El 9 de septiembre del 2001 es la fecha simbólica que marca el cambio del término seguridad consigue ser la máxima prioridad de todo Estado, así como de las agencias nacionales estadounidenses y los organismos internacionales convirtiéndose en el objetivo primario para Estados Unidos y la justificación de las políticas y medidas implementadas por el gobierno estadounidense en los próximos años y hasta la fecha.

Bajo la necesidad de supervivencia del estado de derecho y de los elementos que plantea el neorrealismo, los grupos terroristas se convierten en el principal antagonista y amenaza a la seguridad de todo el sistema internacional. Este agente desestabilizador y el peligro que representa se impuso a otras amenazas tales como la ambiental, la financiera, etcétera, que comprometen la estabilidad y el estatus quo del sistema internacional.

La seguridad como objetivo prioritario desató una guerra directa entre occidente y oriente medio siendo el primer paso a la reconfiguración de la escena internacional, y convirtiéndose en el panorama que se vislumbra entrado el siglo XXI, un mundo globalizado, tecnológicamente desarrollado, un nuevo enemigo en común para occidente identificado como "Terrorismo" (Mcevoy, 2010, p. 9).

Parte de las estrategias para garantizar la seguridad nacional, durante la administración de George W. Bush (2000-2008) se desarrolló, la doctrina del "Ataque Preventivo" una de las tácticas bélicas de la doctrina Bush, la cual consiste en eliminar una posible amenaza antes de que esta se gestara, neutralizando y minimizando la posibilidad de sufrir algún otro ataque (Pratt, 2004, p.122).

Vinculando a esta doctrina es el tema central de esta investigación: la militarización de la Internet. En este ámbito, las amenazas poco a poco fueron creciendo, hasta convertirse en al terrorismo y a la delincuencia internacional en dos de las más preocupantes. Ambas amenazas ha sido el medio el cual ha vulnerado todas las medidas de seguridad estadounidense y en los últimos años ha puesto en riesgo la hegemonía política de ese país, aunque actualmente se están maquinando políticas y acciones para el control de daños que ha generado este espacio.

En este contexto se comprende mejor la postura de Richard Clarke (2010) quien fue parte del diseño de la estrategia y de los lineamientos militares del ataque preventivo de la doctrina Bush. La lucha contra el terrorismo es la política internacional basada en la doctrina del ataque preventivo. De esta forma, la lucha contra el terrorismo en el ciberespacio también está diseñada con base en la doctrina del ataque preventivo.

Sin duda, el flujo de información en la internet se ha convertido en uno de los temas centrales de discusión para los países y las organizaciones internacionales, ya que el uso de esta tecnología defiende el ideal básico y fundamental del derecho humano a la "libertad de

expresión". Si bien la internet posibilita mayor flujo de la información a una escala global, este hecho parece representar una amenaza al sistema internacional.

Como parte de las medidas adoptadas para eliminar dichas amenazas, lo Estados han restringido el acceso a ciertos sitios, sobre todo a los que difunden propaganda extremista, tanto religiosa como política. También han limitado a los usuarios cierto tipo de contenidos e información; incluso han ampliado y perfeccionado los sistemas de vigilancia de los internautas. estas son acciones "justificadas por los Estados" en pro de garantizar la seguridad nacional". La seguridad es fundamental, pero ¿cómo legislar y hacer leyes para dispositivos y herramientas tecnológicas que van mejorando sus capacidades a una velocidad vertiginosa y se mantienen como amenazas constantes a la seguridad tanto del individuo como la del Estado mismo?

## 2.2- El ciberespacio y el Derecho

El ciberespacio es definido como un entorno virtual con un andamiaje en forma de código informático traducido por ordenadores. siendo este, el primer espacio no físico en el cual la sociedad converge e interactúa en tiempo real y de forma simultanea; Espacio en el cual se desarrollan nuevas problemáticas de orden jurídico, social, político, cultural, antropológico, comercial, y militar las cuales afectan de forma directa a la dinámica del mundo físico tal y como lo entendemos.

Estos grandes cambios y avances tecnológicos traen consigo beneficios a la vez que problemas que se convierten en los nuevos retos para los sistemas jurídicos tanto nacionales como internacionales, particularmente en materia legal sobre el uso de la internet y de las plataformas asociadas a esta. La sociedad moderna está compuesta de normas morales, y jurídicas que permiten la convivencia entre los miembros de la misma, así mismo sanciona a quienes transgredan dichas normas. Respecto a la situación en el ciberespacio es un cuanto distinta, el cual requiere de carácter urgente ser regulado, el problema en su regulación radica en la compleja naturaleza de este (Buzai, 2012, p. 273).

Es comprensible que el proceso regulatorio en cualquier rama del Derecho mantenga cierto dinamismo, en los procesos de legislación, adaptándose al constante cambio de la

sociedad, pero ¿Qué ocurre cuando las relaciones sociales se presentan en un espacio artificial, el cual muta a cada instante?

La temporalidad de las leyes es algo fundamental para tomar en cuenta si se busca regular uso y contenidos de la internet. Por ejemplo, los primeros Convenios de Ginebra de 1864 como parte del derecho militar "regulando", la forma de enfrentar los conflictos bélicos y que de este emana el Derecho Internacional Humanitario, actualmente a poco más de un siglo y medio, la realidad y circunstancias distan de corresponder a las problemáticas y atender el fin con el cual fueron creados dichos convenios, en donde la mayor parte de las clausulas han perdido vigencia. Basados en este ejemplo y de acuerdo a Verecelli existe una obsesión por el control y la vigilancia en entornos cada vez más complejos, que por su naturaleza es poco útil regular, como ejemplo se propone el Derecho Espacial, una rama del Derecho que comienza en los albores de la Guerra Fría, rama del derecho la cual se justificaba en la búsqueda de la legitimación de la superioridad militar, exponiendo la posible amenaza que representaría la instalación de satélites que permitan la geolocalización o lo que actualmente conocemos como (Global Position System, o GPS), pero por las condiciones que representa dicho espacio poco se ha avanzado en esta rama, la cual mantiene un paralelismo respecto los intentos de regulación que enfrenta el ciberespacio (Verecelli, 2004, p.12).

## El ciberespacio y sus antecedentes jurídicos

En la década de 1960 no había razón para extremar precauciones respecto a las legislaciones sobre el ciberespacio dado a que bastaba con colocar guardias para resguardar los servidores y grandes artefactos computacionales a los cuales solo personal autorizado tendría acceso, el desarrollo tecnológico de la era digital se mantenía primitivo para suponer la idea de algún tipo de amenaza electrónica (virus electrónico) (Mcevoy, 2010, p.385).

Es importante destacar que todo lo referente al desarrollo computacional, se mantenía exclusivamente para el área militar, hasta la década de los 1990s cuando ocurre una expansión tecnológica y de telecomunicaciones sin precedentes, la cual se ha mantenido en constante crecimiento, como parte crucial del fenómeno de la globalización. Actualmente el

mundo ya no es concebido sin ordenadores y la constante interacción a través de estos (Krepinevich, 2012, p. 18).

El primer antecedente que se mantiene como parte de los intentos de regulación en este campo, es registrado en los Estados Unidos, se comenzaba con la legislación de seguridad computacional la cual data de 1987; En esta acta se expone la importancia de la privacidad y los intereses de los ciudadanos respecto a la programación y el posible acceso a esta tecnología. Con este precedente, se enmarca la forma de convivencia dentro de este nuevo espacio y la correlación de la ciudadanía regulada y el Estado dentro del ciberespacio; asi mismo en dicha acta se buscaba garantizar la seguridad de los ordenadores y los sistemas computacionales gubernamentales con el objetivo de salvaguardar los intereses nacionales (*Computer Security Act of* 1987; Estados Unidos, 8 de enero de 1988).

Esta ley pretendía proteger los intereses nacionales. Bajo esta idea, la Agencia Central de Inteligencia (CIA) y otros departamentos dedicados a la protección de la seguridad nacional (NSA, DHS, NASA, DOD) protegían los archivos y programas clasificados, los cuales, en la de cada de 1990s se vieron vulnerados, como fue el caso del "*Moonlight Maze*"

A casi 30 años de la creación de aquella ley su validez parece nula, ya que no cumple con el propósito para la que fue creada. En poco más de una década perdió sentido lo propuesto en ella, como pudo ser observado en la década de 1990, cuando ocurrieron ataques a la red como el *Moon light Maze*.

La operación *Moonlight Maze* ocurrió en 1998 y mediante esta se logró tener acceso a información altamente clasificada de la Administración Nacional de Aeronáutica y del Espacio (NASA), así como del Buró Federal de Investigación (FBI). La Agencia de Seguridad Nacional (NSA por sus siglas en inglés) descubrió una intrusión en sus sistemas de archivo de los mapas de bases militares, los cuales fueron copiadas y extraídos. Los *hackers* también tuvieron acceso a información sensible para la seguridad nacional de Estados Unidos (Krepinevich, 2012, p. 23).

Así pues, a una década de presentada la ley de seguridad computacional, Estados Unidos recibió uno de los primeros ataques de espionaje a sus sistemas computacionales, dejando entrever el riesgo potencial que representaría el ciberespacio. Según lo descrito por Krepinevich (2012) no fue posible identificar a los autores de dicha infiltración y poco se sabe del total de la información que fue sustraída. La situación fue tratada con total discreción

por las autoridades estadounidenses, pero eventualmente quedaron convencidos de la necesidad de crear un cibercomando especializado en espionaje y las mejoras a los servicios de inteligencia para la internet.

En 1998 fue firmada la ley propuesta dos años antes, mejor conocida como la Ley de Derechos de Autor de la Era digital (DMCA). El gobierno estadounidense pretendía que esta ley fuera adaptada a la nueva era digital, protegiendo a las grandes industrias del entretenimiento así como los interese públicos en la red global de información (U.S. Copy Right office,1998).

El caso Napster es muy ilustrativo para explicar una de las amenazas que la industria del entretenimiento considera de las más dañinas. Primero, es importante saber que esa plataforma tenía una estructura "P2P", esto es una red entre pares por la cual se comparten información entre dispositivos sin pasar por filtros, o intermediarios. Esta arquitectura daba la posibilidad de intercambiar grandes cantidades de información tanto licita como ilícita. Napster, y otros sitios similares, empleaban este tipo de estructuras para la distribución libre y gratuita de material protegido con derechos de autor. Esto le permitió que en 1999 llegara a ser el sitio más popular para la descarga de archivos. Para empresas y asociaciones del entretenimiento y desarrolladoras de *software* el intercambio libre de archivos protegidos por derechos de autor les impulsó a establecer la persecución legal de Napster hasta lograr el cierre de la plataforma en 2001 (Einhorn 2003, p. 6).

A finales de 2010, se dio un nuevo paso en la regulación y restricción de intercambio de información por internet. Esta vez fueron la leyes *Stop Online Piracy Act* (SOPA, por sus siglas en inglés) y *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act* (PIPA). Ambas leyes lograron limitar y castigar a todos aquellos sujetos o grupos que fomenten la piratería en internet. Las leyes Sopa y PIPA fueron aprobadas por el Congreso estadounidense en 2011, lo que de inmediato generó un amplio e intenso debate público a escala internacional, además de protestas e impulsó la aparición de grupos subversivos contra la libertad de la internet (Huichalaf, 2012, pp.1-7).

Reguera (2015) propone que la idea de libertad en la internet está confundida con la idea de libertinaje, y que las restricciones no precisamente violentan o transgreden la libertad del individuo en el ciberespacio. Propone que la libertad se debe asimilar como en cualquier

otro aspecto de la vida y como en cualquier dimensión en donde existen las restricciones que la condicionan, como lo es la seguridad (p. 1).

En el mismo sentido, Lessing señala que en la década de 1990 el ciberespacio poseía esta falsa idea de la libertad, de manera que el internauta común debería someterse a ciertas condiciones establecidas los prestadores de servicios quienes para dar el servicio demandas registro del usuario, pagar para disponer de cierta información, y aceptación de este para ser rastreado o vigilado en cualquier momento, e incluso de la difusión de datos personales (Lessing,1998, p. 3).

Retomando el tema de legislación del ciberespacio, en 2011, en contraste con las leyes SOPA y PIPA, o la francesa HADOPI (similar a las dos anteriores), la ONU declaró como Derecho Humano el acceso a internet, instando a los gobiernos a facilitar el servicio gratuito a sus ciudadanos. Desde la perspectiva de la ONU; esta herramienta tecnológica favorece el desarrollo y el progreso de la sociedad (Carbonell, 2014, p. 20). Esta recomendación ha generado conflictos legales internos en varias naciones, pues las leyes de "internet para todos" van en contra de algunas medidas regulatorias extremas adoptadas por algunos gobiernos. Por ejemplo, la ley francesa HADOPI limitaba el acceso a los ciudadanos que fueran descubiertos descargando contenido ilegal; o China que restringe el acceso a diferentes sitios como Faceboook, o aislando de la red global el contenido de los internautas; en Irán y Egipto, por mencionar dos países de Medio Oriente, los gobiernos niegan el acceso a algunas páginas y censurado otras. Estos casos evidencian la contradicción entre lo recomendado por la ONU y lo que en realidad realizan los gobiernos (El Mundo, 09 de junio de 2011).

Navalón (2012), por otra parte, sugiere que es importante establecer ciertos criterios para identificar hasta dónde se transgrede la libertad del cibernauta, y como facilitar la regulación del ciberespacio. Propone que es necesario un punto medio para el desarrollo de las diferentes dinámicas del propio ciberespacio, y del acercamiento de la brecha digital. Entre estos puntos se encuentran:

- Establecer hasta qué nivel el uso del ciberespacio es un derecho y cómo debe ser protegido.
- Determinar hasta dónde el Estado puede intervenir en nuestras acciones en el ciberespacio.

- Coordinar las acciones legales que, a consecuencia de actos en el ciberespacio, afecten a varias jurisdicciones.
- Congeniar en el ciberespacio el derecho a la intimidad con la necesaria identificación de los delincuentes y la obtención de la evidencia del delito.
- Determinar qué nuevos delitos pueden existir que sean exclusivos de acciones en el ciberespacio.
- Acordar las limitaciones al posible uso del ciberespacio en los conflictos bélicos (p.5).

Con base en lo expresado por Navalón es evidente el vacío legal sobre la regulación de la internet. A pesar de las amenazas anunciadas por varios gobiernos, no existe como tal algún organismo capaz, al cual recurrir o que procure los tratados internacionales en esta materia y que proteja a los cibernautas o a los mismos Estados.

Reguera (2015) se opone a la idea de "libertad máxima" que rechaza toda iniciativa de regulación tachándola de "censura", sugiriendo que la autorregulación del ciberespacio no será posible entre los actores, dado que la sociedad en la dimensión física no puede autorregularse por sí misma, mucho menos lo hará en un espacio donde el anonimato y las amenazas se encuentran en todo momento (p. 2).

En 2002 la OTAN en la conferencia de Praga abordó el tema de la ciberdefensa mecanismo que busca reforzar las capacidades militares de este nuevo espacio. En 2010 en Lisboa se lleva a cabo una cumbre para señalar políticas y acciones en caso de ser atacados dentro del ciberespacio. Todas estás de acuerdo al tipo de O.I. al que pertenece y promoviendo el proceso de militarización en el ciberespacio por las potencias tecnológicas (CESEDEN, 2012, p. 24).

La OTAN organización de cooperación Militar, ha diseñado las reglas para el desarrollo de una guerra dentro del ciberespacio, definiendo este como un nuevo elemento estratégico para el desarrollo de los conflictos bélicos, esto después de los ciberataques perpetrados hacia el Gobierno de Estonia en 2007.

El Manual Tallin de 2011 es el resultado, de la cumbre de Lisboa de 2010 siendo este el referente más importante en el área militar cuando se trata de la defensa del ciberespacio, proponiendo medidas para la defensa del *software* y *hardware* de los países miembros en pro de una regulación. La OTAN además ha buscado establecer las bases con ayuda de un Grupo Internacional de Expertos (EIG) para facilitar algún tipo de convención similar a la de

Ginebra que permita regular la ciberdefensa desde el Derecho Internacional, y así como normar el conflicto en el ciberespacio; dicha organización observa que la guerra no deja de ser guerra si se lleva en el ciberespacio o no.

Por parte de la ONU han sido escazas las propuestas sobre un marco regulatorio a nivel internacional, las pocas que ha habido se han encaminado a aspectos concretos, como incitar a los Estados a promover leyes nacionales que protejan a sus ciudadanos de las amenazas en internet. Así como exhortar a los ciudadanos la responsabilidad y seguridad en este espacio.

López (2014) apoya la idea de la complejidad que representa la regulación del ciberespacio, señalando la lentitud y demora de los organismos internacionales, así como de los Estados para legislar un espacio que crece y cambia con rapidez, además las medidas presentadas para combatir el cibercrimen y la ciberdelincuencia muchas veces son ineficaces ya que con el tiempo que inhabilitan un sitio web muchos otros son abiertos (p.99). De acuerdo a Reguera (2015) y López (2014) quienes aseguran que la regulación de internet se convierte en una pesadilla jurídica, ya que elementos como la seguridad y la libertad se ven contrapuestos, así mismo la carencia de fronteras y el anonimato son elementos que conflictúa algún tipo legislación ya que se vería atentada la soberanía nacional, generando así un vacío legal incapaz de normar este nuevo espacio.

Como respuesta a esta situación los Estados se han visto en la urgencia de crear equipos de respuesta ante amenazas dentro del ciberespacio, ya sea policías cibernéticas que se dediquen a responder a crímenes perpetrados en el ciberespacio hasta escuadrones y comandos militares en el ciberespacio para minimizar los ataques ya sea de terroristas o algún otro Estado.

## 2.3.- Ciberconflictos. Causas y consecuencias de los conflictos en el ciberespacio.

El uso de las herramientas informáticas no son exclusivas de la ciudadanía ni de las empresas, también lo son para los gobiernos nacionales y sus ejércitos. Estos actores incluso les asignan objetivos estratégicos en materia de seguridad nacional. Las potencias tecnológicas han adoptado iniciativas para la modernización de sus ejércitos, haciendo uso y mejorando estas herramientas informáticas, (ordenadores, servidores, y sistemas computacionales

sofisticados) para el dominio del ciberespacio. Su objetivo es mejorar las capacidades de tácticas y estratégicas de orden militar (Dietz et al 2012 p.8).

La legitimidad y poder de los gobiernos actuales se percibe amenazada por los diferentes conflictos originados en el ciberespacio, pues en este nuevo campo los movimientos sociales y de insurgencia se pueden ver manifestada con la rapidez de organización a través de las diferentes plataformas en redes sociales. Es por eso que algunos los Estados nacionales como lo es el caso de China, su gobierno ha diezmado el uso de la red internacional y limitado el acceso a estos a la mayor parte de su población.

Observando los principios de la Convención de Ginebra de 1949 sobre cómo "debería" ser desarrollada y constituida la guerra, estos destacan el respeto al Derecho Internacional Humanitario. De esta forma, en el caso del ciberespacio existe un desapego tácito a esta Convención, pues en los conflictos desarrollados en este entorno virtual es complejo y casi imposible respetar las garantías legales, éticas y morales de la Convención (Reguera, 2015, p. 16).

Además, los ciberataques tienen un fuerte vínculo de los conflictos internacionales con el desarrollo de acontecimientos geopolíticos. Es posible formular filtros para los intereses emanados de este vínculo, pues no es posible observar de dónde provienen los ataques y reducir los propósitos de estos. Los ciberconflictos no son ajenos a otros temas de seguridad nacional.

Para poder abundar más sobre los ciberconflicto y la guerra es importante definir el concepto de este último concepto. Para Clausewitz, la guerra es un instrumento de fuerza cuyo único fin es imponer la voluntad ante el enemigo. Afirma que todo acto de guerra persigue un fin político, más allá de los objetivos o la imposición de la voluntad de algún bando son los propósitos los que realmente transcienden. Desde su punto de vista, la guerra es el acto político más violento que existe, aunque no por ello meno útil para alcanzar objetivos políticos (Clausewitz, 2010, p. 4).

Derivado de lo anterior, la ciberguerra es en esencia el uso y aplicación de los servicios de información computacionales de forma defensiva u ofensiva para el desarrollo y cumplimiento de operaciones militares, tanto para enfrentar amenazar, atacarlas o desplegar acciones de guerra. Estos usos se expresan y confirman el desarrollo de mandos

especializados como parte de la estructura de los ejércitos. (Dietz Larson, Liles y Rogers, 2012, p. 8).

La ciberguerra rompe con el esquema tradicional de "guerra" y de los modos en que los ciberataques se desarrollan, por ejemplo, no hay un uso mínimo de la fuerza, por ende, un ataque cibernético es más complejo que un ataque aéreo o terrestre, pero más allá del modo con el que se actué, Rid (2011) destaca, que el impacto de sus consecuencias, podrían desarrollar motivos legítimos para un conflicto armado en el mundo real (p. 6).

Actualmente existen dos posturas referentes a los conflictos desarrollados en el ciberespacio. Por un lado, se encuentra la teoría del colapso, descrita en líneas anteriores, la cual presupone que podría existir un gran caos generado por algún tipo de ataque cibernético. Por otro lado se encuentran los autores que rebaten dicha doctrina con argumentos y dimensionado los alcances de las posibles consecuencias de un ciberataque para el cual , insisten, hay razón para alarmarse.

La teoría del colapso refiere al aumento de la dependencia cada vez más marcada a las estructuras de telecomunicaciones informática que nos hacen más vulnerables a ataques cibernéticos, esta dependencia no es exclusiva del individuo, ya que el Estado, los bancos, las compañías privadas dependen cada vez más de la tecnología para desarrollar sus actividades. Y esto es un foco de atención para los equipos de seguridad e inteligencia de los Estados (Clarke y Kanake 2010, p. 41).

Parte de la teoría del colapso propone que la mayoría de los equipos de cómputo, así como los sistemas de comunicación y sistemas computacionales poseen una capacidad limitada, ya sea de almacenamiento, de conexiones, o de durabilidad la cual si es sobrepasada podría generar un fallo general del cual no sea posible recuperarse a la brevedad (Dietz et al. 2012, p.4).

Los opositores a la teoría de colapso como Lewis (2002), sugieren de forma moderada reconsiderar las ciberamenazas, y aunque el daño que pudieran ocasionar es real, aseguran que los ciberterroristas y los grupos de cibercriminales prefieren actuar en el mundo real, con atentados que generen miedo a la población y que provoquen terror a los gobiernos. Por ejemplo, a Al Qaeda o ISIS, quienes prefieren estallar un coche bomba a generar un ciberataque que sabotee la prestación de servicios públicos como energía eléctrica o agua (p. 18).

Tomando como referencia la definición de Clausewitz, la ciberguerra carece de una violencia marcada como es la guerra tradicional, hasta ahora y como se ha venido mencionando no ha habido alguna acción que atente contra la vida de nadie en el ciberespacio ni que determine el actuar de una potencia respecto a otra. Aunque por ahora no ha trascendido ninguno de los ciberataques o el ciberterrorismo no ha asestado un gran golpe a la seguridad nacional de ningún estado nacional, no hay que subestimar el riesgo potencial de esta ciberamenaza la cual se mantiene en constante mejora con el desarrollo y progreso tecnológico.

La seguridad nacional desde el ámbito cibernético requiere atención de los gobiernos e instituciones correspondientes, ya que las amenazas no son estáticas en tanto que constantemente mejoran las ciberarmas y aumentan las capacidades tecnológicas de las potencias. En esta cotidianidad se encuentran nuevas vulnerabilidades en los sistemas y redes computacionales, si bien por ahora el daño a la infraestructura física representa la mayor preocupación no hay que minimizar el riesgo. Bajo la postura de Thomas Rid (2011) se sostiene que la ciberguerra no es algo que veamos pronto, ya que los conflictos desarrollados en el ciberespacio no mantienen ni las características ni las consecuencias de un conflicto bélico tradicional, no aún. Lo cual expone son simplemente estrategias de disuasión de las diferentes potencias tecnológicas para mantener el control de las nuevas tecnologías (11).

En contraparte a lo argumentado por Rid, Clarke expone que lo ocurrido en el ciberespacio no debe ser descartado por analistas ni expertos en materia de seguridad; este plantea un escenario en el cual se expone la gravedad de las consecuencias de un posible ciber-ataque a las estructuras críticas, desde un choque de trenes, apagones, y hasta colapso de los sistemas de comunicación, serian eventos que podrían afectar con seriedad a la seguridad nacional (Clarke y Kananke, 2010, p. 54).

Thomas Rid, en su libro *At The Abyss: an Insder of Cold war*, destaca que uno de los ciberataques "más violentos" en la historia tuvo lugar en Siberia en 1982. Ese ataque fue realizado mediante un código malicioso infiltrado por la CIA en los sistemas de control de una tubería de gas. Ese virus informático ocasionó un mal funcionamiento en la presión de la línea de gas, provocando así una explosión en las tuberías, la cual tuvo como resultado una detonación similar a una pequeña bomba nuclear, dicha explosión pudo ser vista desde el espacio en palabras de Reed, nadie salió herido de este suceso. Es decir desde la Guerra Fría

Estados Unidos ya implementaba la tecnológica para una especie muy primegenia de lo que hoy entendemos como ciber guerra (Rid, 2005, p. 14).

Este acontecimiento, demuestra la capacidad de destrucción y las vulnerabilidades que pueden llegar a presentar los sistemas de control de plantas nucleares, así como los sistemas militares; por fortuna no se ha reportado alguno otro suceso con esta magnitud; por lo cual, lo expuesto por Richard Clarke y los seguidores de la teoría del colapso, dista de ocurrir al menos para Rid.

Para dimensionar la magnitud de una ciberguerra hay que poner atención en la diferencia de este concepto con ciberconflicto, ya que muchas veces suele interpretárseles de manera incorrecta. El ciberconflicto es la ante sala a una ciberguerra, y en este momento los gobiernos y las empresas emplean recursos tanto de forma ofensiva como defensiva. Lewis (2010) marca la diferencia entre un ciberataque y una ciberguerra. Al respecto señala que "un ciberataque es perpetrado por un individuo o un grupo de individuos con el objetivo de generar algún daño, destrucción o comprometer los sistemas de comunicación" (p. 4). Aunque la postura un cuanto alarmista y paranoica de la teoría del colapso todo acto ofensivo puede ser es considerado acto de guerra, postura que asumió el ejecutivo estadounidense en 2008.

Para Llongueras, la ciberguerra es el uso de la fuerza con el fin de causar daño, destrucción o comprometer los sistemas de comunicación con un propósito político ya sea orquestado por algún Estado o algún grupo político, ya sea con la intención de desestabilizar los sistemas militares o generar algún tipo de daño que comprometa la seguridad nacional (Llongueras, 2010, p. 1).

Por otra parte, Richard Clarke, en el libro *CyberWar*, mantiene una visión pesimista sugiriendo que existe la posibilidad y que mediante la toma del control de las diferentes redes pueda ser estas empleadas para el sabotaje perpetrando diferentes "auto ataques" los cuales destruyan ciudades y genere varias bajas (Clarke y Kananke, 2010, p. 56).

Lewis en contra parte, asume una postura más apegada a la realidad y con base en lo acontecido en la historia de la "ciberguerra", con una perspectiva neutra comprende los efectos o consecuencias que hasta ahora han ocurrido en el ciberespacio y la resume con la siguiente frase: "El impacto mediático y la alarma social no siempre son simétricos a la amenaza real" (Lewis, 2010, p. 3).

El conflicto entre las dos Coreas y el ciberataque ejecutado por corea del norte a Corea del sur en 2013 nos da un claro ejemplo de cuáles podrían ser los desafíos para los Estados, se sugiere imprescindible desarrollar mecanismos de defensa o acciones en el plano militar tradicional para minimizar estos conflictos. (Gibbs y Halliday, 2013 p. 1).

De acuerdo con la *Cyber Conflict Studies Association* (CCSA) hasta ahora no se ha presentado ningún problema físico por causa de algún conflicto en el ciberespacio, estos ciber-conflictos son pequeñas molestias para el Estado como que no pueden ser considerados terrorismo ni mucho menos actos de guerra, lo cual expone lo sobrada de la teoría del colapso (Billo, 2017, p. 36).

Aunque también es importante señalar los distintos ejemplos de conflictos en este espacio como el ataque a Estonia siendo uno de los ataques cibernéticos con mayor duración ocurrido en 2007, en donde un grupo de *hackers* rusos tanto en estonia como en Rusia, y empleando el ciberespacio como un sitio más donde protestar iniciaron los ataques a las principales páginas y servicios del gobierno estonio.

Este grupo inició el 27 de abril con los ciber-ataques más comunes los DDos (Distributed Denyal Service) denegaciones de servicio; estos ataques continuaron hasta antes del 1° de Mayo, en donde parecían no tener mayor relevancia o impacto ya que las herramientas empleadas en estos ciber-ataques eran bastante comunes y rudimentarias, las cuales se vieron mejoradas por grupos de *hackers* rusos quienes apoyando la causa prolongaron y atacaron no solo las páginas de gobierno, sino de empresas de Estonia; estos embates duraron hasta el 9 de Mayo de 2007 fecha en la cual se dio cese a la ofensiva. Este es uno de los acontecimientos con mayor relevancia e impacto en casi una década Como consecuencia nunca hubo evidencia contundente que confirmara la participación del gobierno ruso en los ataques (Hassan, 2009, p. 5).

Como resultado de lo ocurrido en Estonia, ese mismo año la Organización del Tratado del Atlántico Norte (OTAN) en Tallin se estableció un Centro de Cooperación de Ciber-defensa (Cooperative Cyber Defense Centre Of Excellence) esto con el objetivo de mitigar algún otro ciber-ataque en el futuro (Maness y Valeriano, 2013, p. 26).

Un año después de lo ocurrido en Estonia, por motivo de un pequeño conflicto territorial entre Georgia y la Federación de Rusia, el conflicto tuvo lugar en el sur de Osetia y el 7 de agosto del 2008 el Gobierno Georgiano responde las provocaciones y ataca a las fuerzas

separatistas del sur de Osetia, motivo por el cual Rusia interviene y responde con la incursión de su ejército tanto en tierra como en el ciberespacio. Lo destacable de este acontecimiento es que por primera vez tanto la intervención militar, así como un ciber-ataque ocurren de manera sincronizada y conjunta (Carrol, 2008, p.1).

Los efectos de dicho ataque realmente no fueron trascendentales ya que Georgia no posee una gran población además en 2008 la estructura critica, así como los servicios no se encontraban atados al internet por ende los Ataques DDoS no afectaron de forma importante al Gobierno Georgiano. Aunque es importante señalar que nunca hubo evidencia concluyente que confirme la participación del gobierno ruso en los ataques de este conflicto (Hollis, 2011, p. 6).

Por otra parte, la ciber-guerra no solo está compuesta de ciber-ataques, esta también se comprende del espionaje de alto nivel, no solo por parte de las grandes empresas en donde la filtración de información podría representar perdidas millonarias, también el espionaje entre los gobiernos representa una amenaza más, como se ha descrito en líneas anteriores con la operación "*moonlight maze*".

En esta operación los intrusos tuvieron acceso a esta información por más de dos años sin que ninguna de las agencias de seguridad notara su presencia, se logró rastrear hacia donde iba la información y todo señalaba que el gobierno ruso se encontraba involucrado; pero una vez más todo fue desmentido y sin pruebas concluyentes de la participación del gobierno ruso en lo sucedido (Llongueras, 2010, p.19).

Estos ejemplos sugieren lo expuesto por Rid (2011), quien propone que los ciber-ataques han incrementado en número y se han convertido en más sofisticados, pero se limitan a tres tipos de transgresiones: la subversión, el espionaje, y el sabotaje. Una vez descritos e identificados estos podemos asumir realmente los riesgos que implican las diferentes amenazas del ciberespacio.

Con base en lo expuesto por Rid, existe una línea delgada entre actos criminales y actos de guerra en el ciberespacio, si bien existen transgresiones las cuales pueden involucrar tanto actores gubernamentales como actores del sector privado; No existe la violencia como tal, aunque esto no les resta efectividad a las agresiones. Siendo un problema más el categorizar como "actos de guerra" lo ocurrido en el ciberespacio ya que no siempre las agresiones mantienen una razón política (Rid, 2011, p. 9).

*Ciber sabotaje*

Tomando como base los tres tipos de transgresiones que señala Rid es importante ahondar en cada uno de estos para comprender más la naturaleza de los mismos y asimilar las consecuencias de estos. El sabotaje es el intento deliberado de la destrucción o debilitación de un sistema computacional, la naturaleza del sabotaje es meramente táctico, objetivo que pretende la destrucción o corrupción de los sistemas sin el uso de la violencia como herramienta (Rid, 2011, p.11).

El sabotaje no puede ser visto como un acto de guerra ya que los autores del mismo evitan el enfrentamiento de manera abierta, además de no asumir autoría sobre tal acto. El sabotaje va dirigido hacia los sistemas computacionales y los sistemas de mando u otros elementos básicos de coordinación, y que son acciones propias de las operaciones militares y de inteligencia.

Como ejemplo la operación Orchard en 2007, en la cual las Fuerza Aérea Israelí navegaba sobre el espacio aéreo de Siria con la intención de analizar un reactor nuclear ubicado en Day Er-Zor ciudad ubicada al norte siria, sin que las Fuerzas Áreas Sirias notarán la violación de su espacio aéreo (Follat y Stark, 2009, p. 1).

Este ataque fue combinado con el uso de herramientas electrónicas que permitieron "cegar" los sistemas de defensa, así como la comunicación y los radares sirios, entrando y saliendo del espacio aéreo sin poder ser detectados. Cabe señalar que ninguno de los sistemas fue dañado, y hasta la fecha el objetivo de misión se encuentra como clasificado (Ehrami, 2013, p. 1).

Otro elemento que coincide en los dos casos expuestos, es la ausencia de responsables identificables de primera mano, ya que no hay evidencias concluyentes que infieran la participación de los gobiernos en las operaciones dentro del ciberespacio, para la manipulación y el sabotaje de los diferentes sistemas, ambos autores sugieren que el sabotaje es la parte práctica del espionaje (Follat y Stark, 2009, p. 9).

Un ejemplo más y que considero fue el más mediático entre casos similares es es el generado por el virus electrónico conocido como "*Stuxnet*", el cual el cual tuvo como consecuencia y una gran repercusión a nivel industrial ya que causó la destrucción y la infección de miles de ordenadores, así como docenas de servidores infectados de una planta nuclear iraní.

Hasta ahora el caso Stuxnet ha sido el ciber-ataque más sofisticado de la historia el cual tenía como objetivo sabotear los sistemas de las plantas nucleares iranís para retrasar y debilitar el programa nuclear de enriquecimiento de uranio que Irán ha venido llevando a cabo en los últimos años.

Las empresas de seguridad industrial lo han catalogado como la amenaza más avanzada y persistente, ya que *stuxnet* iba dirigido a sistemas computacionales no convencionales, totalmente diferentes a los que conocemos, ya que dichos sistemas industriales se encuentran aislados en cuartos especiales sin algún tipo de teclado o pantalla, solamente pueden ser programados durante cierto periodo de tiempo y conectados a computadoras convencionales con sistemas operativos comunes (ESET, 2010, p. 5).

Lo más destacable y alarmante fue la capacidad de reproducción del virus y el código malicioso que empleaba, ya que este le permitía reproducirse sin ser descubierto, así como modificar la configuración de los sistemas industriales en segundo plano de manera inadvertida sin el uso de alguna red interna ni mucho menos empleando internet.

*Stunext* ha sido el ciber-ataque más letal, ya que logro dañar más de cien mil servidores a lo largo de docenas de países, compañías de seguridad informática como *Symantec* sugieren que el virus fue transportado por una memoria usb aunque se desconoce el origen real de este y de su autor. Además, dicho virus tiene la capacidad de borrarse a sí mismo y así poder ser descubierto por ningún antivirus, el cual opera de manera silenciosa siendo capaz de borrar, copiar o esconder archivos sin que el usuario lo note. Generando así el malfuncionamiento de los rotores, turbinas y centrifugadoras causando así daño físico a los sistemas (Symantec, 2011, p. 3).

Además, el virus tiene la capacidad de interconectarse con otros equipos infectados sin la necesidad algún de tipo de red, lo cual complica su rastreo, y este que se reproduce empleando la estructura p2p, esto sin que el operador note la presencia del virus y tampoco se identifique su procedencia (ESET, 2010, p.12).

Aun no se descubre con certeza la misión de *Stuxnet*, aunque su creación pudiera datar de 2008 a 2010, periodo en el cual las diferentes compañías tanto de software como de seguridad digital hallaron parte de su historia, y lograron identificar las consecuencias de dicho virus sin realmente conocer al grupo o a la persona creadora de *Stuxnet* (Symantec, 2011, p.4).

*Ciber-espionaje*

El espionaje ha sido parte importante en el desarrollo de la doctrina militar a lo largo de la historia marcando una gran labor de inteligencia, de la que ahora se encargan las agencias de inteligencia y los servicios secretos de manera más sofisticada y con nuevos sistemas para adquirir, almacenar y proteger esta información (Rid, 2011, p. 6).

El ciber-espionaje a diferencia del ciber-sabotaje, suele ser más común y menos "complicado" ya que existen diferentes agencias dedicadas a la recolección e información de datos, así como grupos de individuos quienes se encargan de "piratear" bases de datos con el objetivo de venderlas al mejor postor. (Rid, 2011, p. 9).

Los Estados mediante el uso de las agencias de inteligencia o incluso de grupos subversivos, así como las grandes empresas se encuentran detrás de las grandes operaciones de espionaje a nivel global, aunque confirmar su participación y asumir la autoría no es posible, tal fue el caso de la operación *Moonligt Maze* y de otras ya descritas con anterioridad.

Un par de años antes de *Wikileaks* se presenta un caso ocurrido a la NASA, NSA, y FBI ya que en 2007 una fuente del pentágono asegura que China se infiltró en la red interna y secreta del Departamento de Defensa (DoD) para hacerse con más de 20 terabytes de información, probablemente información no sensible, aunque esto no puede ser probado (La Nación, 4 de septiembre de 2007).

Para comprender mejor la infiltración es importante entender como están compuestas las redes de los servicios de inteligencia, ya que estás manejan un protocolo diferente al que conocemos, siendo el más común el protocolo de transferencia de hipertexto el famoso "http" (hiper text transfer protocol) el cual es el protocolo más usado a nivel mundial, pero no significa que sea el único.

Los servicios de inteligencia manejan protocolos más avanzados que garanticen la seguridad en la transferencia de la información que se maneja, de acuerdo con Rid el pentágono maneja una red oculta con un protocolo sin clasificar el NIPRNET (Non-Classified Internet Protocol Router Network) a diferencia del servicio de inteligencia quienes junto con el Departamento de Defensa emplean el SIPRNET (Secret Internet Protocol Network) ambos protocolos proveen de conectividad entre los ordenadores de dichos departamentos sin comprometer la información que de ellos emane o transite Además no solo

la red se encuentra protegida también sus componentes físicos, como lo son sus servidores y toda la infraestructura que comprenda dichas redes, además de encontrarse separadas electromagnéticamente de redes inseguras (Rid. 2011, p. 21).

En 2009 la Universidad de Toronto dio a conocer un *malware* o mejor conocido como caballo de troya, o troyano, capaz de infiltrarse en las redes antes descritas anteriormente, esta era parte de una operación de espionaje la cual se asegura viene de China, y que, de acuerdo al grupo de especialistas, en dicha operación, lograron infiltrarse a más de mil ordenadores, de embajadas, de ministros y secretarios de relaciones exteriores, ONGs, OIGs, y medios de comunicación Por lo cual se tuvo acceso a información confidencial a escala global en donde al menos 103 países fueron monitoreados por dicho malware, el cual se le conoce como Ghostnet (Red Fantasma)

[The Sec Dev Group y University of Toronto, 2009, p. 20].

Además del acceso, Ghostnet podía activar cámaras y micrófonos para grabar y poder transmitir esta información a diferentes partes del mundo, además de descargar documentos, ingresar a cuentas personales, descifrar contraseñas de los ordenadores sin que usuario u operador estén al tanto de estas acciones.

China es uno de los Estados acusados de incentivar y promover el Ciber-espionaje, ya que no sólo ha sido acusado por las diferentes agencias de seguridad estadounidenses sino también por parte de miembros de la OTAN lo cuales sugieren, que de acuerdo al centro de defensa instalado en Tallin la mayoría de los ofensivas de espionaje provienen de China, y las víctimas y victimarios del espionaje son tanto entidades públicas como privadas. A pesar de la gran inversión y un sinfín de avances en materia de ciber-seguridad los esfuerzos aun no son suficientes ya que el ciber-espionaje se encuentra en auge (Foncillas, 2013, p.1).

*Ciber subversión*

El ejemplo más importante fue en 2010 donde la fuga de información llevada a cabo por *Wikileaks* este ejemplo fue el más conocido mediáticamente por el impacto de este, aparte de ser uno de los movimientos subversivos y de espionajes más importantes del siglo XXI, el cual generó un gran la controversia a escala internacional al comprometer las relaciones diplomáticas de los Estados Unidos con diferentes Estados a nivel internacional. Otra de las ofensivas y transgresiones generadas en el ciberespacio conocidas como activismo y al

menos para Richard Clarke o Rid lo catalogan como Subversión, en donde el blanco de ataque “no son los aparatos o los sistemas sino las mentes” (Rid, 2011, p. 9).

Esta es una de las actividades peculiares que se desarrolla y trasciende desde el ciberespacio como consecuencia de la rapidez del flujo de información, los ejemplos de Estonia y Georgia mencionados anteriormente, ya que parte de los ataques tienen un principio subversivo, aunque manifestado de otra manera, en donde el objetivo fue difundir información “patriótica” como fue el caso de Estonia en donde los “hacktivistas” rusos, atacaban los servidores por razones nacionalistas.

A diferencia del sabotaje o espionaje la ciudadanía tiene un rol importante en los ciber-ataques de índole subversivos; Caro sugiere que para alcanzar el éxito en estos ataques simplemente hay que juntar cientos de miles de personas alrededor del mundo con un mismo objetivo y una misma herramienta (Caro, 2013, p. 85).

El hecho de conocer o no de informática no siempre es un requisito para el desarrollo de los ataques de este tipo, ya que simplemente con poseer la intensión de pertenecer a este tipo de grupo y usar herramientas que se ponen al alcance de cualquier cibernauta para unirse a la causa. La más básica es financiando las actividades de este tipo de organizaciones o viralizando el mensaje.

Actualmente la subversión ha sido un elemento considerable en el desarrollo de revueltas sociales como el caso de la “primavera árabe” en 2011, en donde si bien no fue el origen del conflicto si un fue un factor en donde el uso de las redes sociales fue un la factor clave, aunque no determinante para la organización civil en las revueltas sociales ocurridas en la zona norte de África (Billo, 2004, p.21).

Este acontecimiento, es multifactorial, pero se rescata el actuar de la juventud en varios países árabes, quienes masificaron mediante la red y efecto domino se vio reflejado en varias ciudades como Tunes, Egipto, Libia, Siria, y Yemen, la exposición de estos acontecimientos en las redes sociales fortaleció, que dichas protestas generaran un movimiento social mucho más fuerte el cual atrajo la atención de medios de comunicación alrededor del mundo (Derek, 2011, p.7).

La subversión, así como la insurgencia son guiadas por motivos sociales muy fuertes en las cuales cualquiera que simpatice con estos se une a la causa ya sea como simpatizante, voluntario o activista, la constante actualización sobre los diferentes eventos y la basta

información que existe en el ciberespacio de estos, además de la facilidad en la intercomunicación entre ciudadanos de cualquier parte del mundo, ha promovido la creación de grupos de activismo o "hacktivismo" ya sea con razones políticas, culturales, o sociales, como es el caso de "*Anonymous*" (Maness y Valeriano, 2013, p.22).

*Anonymous* es un movimiento de activistas compuesto de un grupo de personas alrededor del mundo las cuales se identifican por la máscara de *Guy fawkes*, personaje de la novela gráfica V de Vendetta. Estos se denominan como una legión en contra de la censura y promotores de la libertad de expresión en internet, La mayoría de los voluntarios o "hacktivistas" que se identifican con *Anonymous*, participa por entretenimiento o por el simple gusto de ir en contra del sistema, lo cual le ha restado seriedad a dicho grupo, además que los ataques y operaciones de dicho movimiento son poco efectivos y de nula relevancia (Mehan, 2012, p.36).

Aunque por otra parte también dicho movimiento se ha adjudicado operaciones como el "Proyecto Chanology"; el cual consistió en generar diferentes ataques al grupo religioso de "cienciología". En 2008 este grupo religioso se dispuso a censurar un video en *youtube* el cual desacreditaba dicha iglesia, por este acto y como respuesta el grupo *Anonymous* reaccionó con ataques *DDos* a los diferentes sitios web pertenecientes a este grupo religioso (Infosec, 2011, p. 1).

Este movimiento de "hacktivistas" ha logrado infiltrarse en diferentes redes gubernamentales y diferentes corporaciones teniendo como fin desenmascara gobiernos y empresas privadas; hasta la fecha no se ha logrado nada sustancial por parte de este tipo de grupos, pero sus ideas fueron base para la creación de movimientos de "hacktivistas" alrededor del mundo, así como grupos como Lulzec o Antisec (Infosec, 2011, p.1).

Además de este tipo de actividades favorecen que algún movimiento ha sido replicado y empleado por redes terroristas el ejemplo más claro es la expansión global de la Jihad, quienes han empleado estas nuevas tecnologías para esparcir su ideología además del emplear la violencia como herramienta subversiva y difundir el miedo con contenido altamente violento y muy explícito que es fácil de hallar en la red.

La internet ha sido empleada como plataforma ya sea para grupos de "hackers" con propósitos sociales, o masificar mensajes de grupos terroristas y la promoción de su ideología, además la ciudadanía ha encontrado un espacio más para expresarse y manifestarse

contra sus gobiernos. En dicha red es posible encontrar foros dedicados a promover la insurgencia, la anarquía o propiamente el terrorismo, por ejemplo, se ha encontrado contenido en donde se enseña a fabricar artefactos explosivos, así como la planeación de genocidios.

Foros como *4chan* o *Reddit* han sido herramientas para la diseminación de ideologías extremistas, espacios los cuales no mantienen reglas de uso ni políticas como comunidad, ni siquiera existe algún tipo de regulación para sancionar estos espacios los cuales se rigen nada más que las reglas impuestas por sus moderadores, aunque muchas veces estas plataformas son monitoreados por agencias de inteligencia y a veces derribados, ya que en este tipo de espacios se encuentran constantemente la difusión de videos de los ataques terroristas más recientes en donde la censura no tiene cabida. (Maness y Valeriano, 2013, p.39).

El terrorismo es parte fundamental y el ejemplo claro que en el ciberespacio la idea de un gran ejército no es sustancial para hacer daño, al contrario, estos grupos pueden llegar a atentar contra los sistemas tal como se menciona en la teoría del colapso, aunque no existe algún hecho documentado que asegure lo expuesto en dicha teoría. Ya que los ciber-ataques a diferencia de cualquier acción de corte militar no requieren apoyo visible del Estado para ejecutarse.

Estas amenazas, son la causa de las leyes de censura y las diferentes restricciones que progresivamente ha limitado el acceso de contenido en internet, y que desde los gobiernos hasta las propias plataformas, ha condicionado a los hábitos de los cibernautas, quienes regularmente acceden mediante sus dispositivos móviles, con una capacidad limitada en comparación a la de un ordenador y el contenido se limita a un par de aplicaciones, ignorando más del 99% de todo el contenido vertido en la red al día (Mehan, 2012, p.65).

Aunque estas restricciones no han reducido el número de cibernautas sino todo lo contrario, el acceso de internet se ha masificado gracias a los *smartphones*, ya que de acuerdo con cifras de la asociación GSM hasta mediados de 2018 más de 5,100,0000 de personas acceden a internet por sus dispositivos móviles, y se espera que a finales de la década se cuente con 7 billones de usuarios conectados desde sus celulares alrededor del mundo. (Asociación GSM, 2018, p. 1).

## 2.4.- El ciberespacio en el contexto internacional

En la actualidad es posible determinar que en el contexto internacional se han presentado nuevas formas de interactuar dentro del ciberespacio desde el uso de nuevas monedas como los *bitcoins* así mismo como la disposición de nuevas herramientas tecnológicas y nuevas amenazas en comparación de cuando inicio esta investigación hace unos 5 años, aunque no todas las novedades son propias de mención para esta investigación, abordare brevemente algunas que considero relevantes para este trabajo.

Es importante destacar que la OTAN en 2014 anexa el concepto de guerra hibrida haciendo referencia a aquellos conflictos en los cuales las diferentes potencias pretenden desestabilizar a otros Estados empleando estrategias de propaganda mediante la viralización de esta información en las diferentes redes sociales y a través de las estructuras informáticas (Álvarez, 2017, p. 1)

Esta guerra hibrida ha tenido repercusiones importantes, tal como lo fue la investigación periodística del del *Panamá Papers* en 2016, donde personajes políticos de gran peso internacional se vieron involucrados en temas como la evasión fiscal, tal fue el caso del Presidente Ruso Vladimir Putin, quien acusó a la CIA de este tipo de acciones para comprometer la estabilidad política de su país (El Universal 04 de abril de 2016).

Álvarez describe la guerra hibrida como un conjunto de operaciones dirigidas por algún Estado que utiliza tácticas abiertas o encubiertas con el propósito de desestabilizar a un Estado o polarizar la opinión pública de la población civil, empleando estrategias subversivas de inteligencia, instrumentalización del crimen organizado, propagando y operaciones psicológicas y sobre todo desinformación (Álvarez, 2017, p. 1).

*Caso Panama Papers.*

Esta fue una investigación de carácter periodístico en el cual se descubrió una red de transacciones y triangulación de depósitos a paraísos fiscales, en donde personas, empresas y fideicomisos utilizaban este entramado financiero, para la evasión fiscal, el lavado de

dinero, sobornos y hasta pagos por posibles actos de corrupción (Obermaier y Obermayer, 2016, p. 19).

Es interesante observar el impacto de esta investigación y el carácter de la misma, parece coincidencia, que derivado de todo este trabajo periodístico la mayor parte de los personajes involucrados correspondan a adversarios políticos estadounidenses, como lo fue el caso del Presidente Ruso, Vladimir Putín, dicha investigación también incluye a la ex presidenta argentina Cristina Fernandez de Kirtchner por mencionar algunos.

Un entramado bastante detallado que involucra a varios países considerados paraísos fiscales, destapando una red internacional de empresas pantalla, o sociedad "*offshore"* empleadas para el lavado de dinero, y la evasión fiscal, sin duda lo expuesto por Obermayer y Obermaier a detalle en el libro "Panama Papers: El Club Mundial de Evasores de Impuestos", es importante para dar a conocer este tipo de corruptelas a escala internacional, se puede percibir que este tipo de investigaciones persiguen un interés político, pese a ser en apariencia una filtración de un buffete de abogados en Panamá facilitada al Consorcio Internacional de Periodistas de Investigación (CIPI) el cual mantiene su sede en Washington D.C.

*Criptomonedas*

El desarrollo digital ha transformado el mundo como lo conocemos en muy poco tiempo, era inevitable que el sistema financiero y la banca internacional no se vieran incluidas en estos cambios, ya que, a partir de la crisis financiera de 2008 a nivel internacional, es donde nace la concepción de la cripto moneda una opción a la que muchos países actualmente se encuentran considerando apostar para el fortalecimiento de su economía, la más importante de ellas es la conocida *bitcoin,* cripto moneda que desde 2009 ha ido tomando terreno en el sistema financiero internacional (Mora, 2016, p. 2).

Sorprende observar como en menos de una década existe una divisa con una mayor cotización a la de cualquier moneda del mundo, además lo interesante de esta moneda es que no existe un banco central que regule la emisión de estas y mucho menos es posible identificar quienes son los portadores de dicha divisa, ya que las transacciones realizadas con bitcoins se realizan mediante la red empleando un sistema como casas de moneda que se encarga de

hacer las conversiones así tanto el vendedor y el comprador quedan en el anonimato así como la ruta del dinero ya que no es posible trazarla.

A consecuencia de las características enunciadas, esta moneda es empleada para el pago de ciberdelitos, originalmente esta moneda fue desarrollada en la *Deep Web*, como una forma segura en la que los criminales podían ser contratados conservando el anonimato, actualmente dada la burbuja económica creciente sobre este tipo de monedas un bit coin es posible cotizarlo en poco más de cien mil pesos mexicanos, y con una tendencia al alza estimación realizada el 15 de agosto de 2018 (Mataf, 2018, p. 1).

Existen posturas diversas sobre este tipo de divisas, ya que algunos expertos en materia económica perciben que en esta figura recae la adaptación del dinero en esta nueva era digital, mientras otros sugieren que es una moda pasajera dentro del sistema financiero sin mayor relevancia, pero no está demás mencionar que para 2016 al día se hacían más de doscientas mil transacciones alrededor del mundo con bitcoins (Mora, 2016, p. 4).Dadas las características de este tipo de moneda se encuentra sin regulación escapa a las reglas del sistema financiero internacional, es por ello que la especulación financiera particularmente la de bitcoin genera una burbuja financiera, donde Mora señala a que es posible que pronto se vea una caída en los mercados financieros que apuestan a este tipo de divisas.

Este tema lo abordo con ligereza, aunque merece una investigación más profunda desde el estudio de las relaciones internacionales, ya que afecta de forma directa el sistema económico de todo un sistema internacional, que transita sin orden aparente a una nueva era en donde el sistema financiero se verá obligado a normar y en donde naciones como Estados Unidos, Alemania, Suiza poco a poco se han ido integrando al mercado de las cripto monedas.

Destacamos su importancia ya que el protocolo con el que estas nuevas monedas se emplean son ajenas a la figura institucional, siendo sus creadores anónimos, y bajo el seudónimo de Satochi Nakamoto quien en 2008 crearon bitcoin encore, países como Venezuela, Rusia, China pretenden crear su propia criptomoneda, siendo un hecho sin precedentes que invita a pensar el futuro del sistema económico y financiero a nivel internacional. (Mora, 2016 p.9)

Nuevas Amenazas informáticas:

El desarrollo de nuevos virus informáticos y códigos maliciosos han sido el arma de grupos delictivos que emplean el *Ramsonware,* siendo programas dedicados al "secuestro" de ordenadores y dispositivos móviles, en los cuales se cobraba por el "rescate" de estos para poder recuperar la información y el equipo dañado (Ernest y Young, 2017, p. 4).

En un informe de 2018 realizado por la compañía ESET encargada de elaborar informes sobre las nuevas amenazas en materia de ciber-seguridad, se establece que en 2018 nuevos casos relacionados con ciber ataques a estructuras críticas, también la revolución del *Ramsonware,* sin pasar por alto los nuevos mecanismos del ciber crimen y las estrategias de ciber seguridad por parte de la ciber policía, así como destacar el posible *Hacking en* los diferentes procesos electorales en las democracias. Los avances en materia legislativa para la protección de datos de los usuarios, estos dos últimos elementos se detallarán en el capítulo tercero (ESET, 2018, p. 9).

Por mencionar parte de las amenazas los ciber delitos relacionados al *Ramsonware* cada vez son más frecuentes, si bien la ciber amenaza más común en el periodo abordado eran los ataques DDos actualmente se han sofisticado, desde la dimensión política, ya que se ha combinado este tipo de archivos con los famosos *Worms*, que facilitan la propagación de infección de los diferentes tipos *Ramsonware* como el ya mencionado *I Wanna Cry* (ESET, 2018, p. 7)

Respecto a los ciber-ataques dirigidos a la estructura critica, se detalló que compañías de energía ucranianas vieron vulnerados sus sistemas en diciembre de 2015 dejando sin el servicio de electricidad a un gran número de hogares, observando que se trataba de un *Malware* que pretendía manipular los sistemas de control industrial, los cuales al detectar dicha amenaza y por cuestión de seguridad se inhabilitaron. (ESET, 2018, p. 12)

La piratería cibernética es otra de las ciber-amenazas actuales ya que la filtración de material audiovisual sigue siendo uno de los grandes retos que enfrentan las industrias del entretenimiento como es el caso de Netflix, una de las compañías que de acuerdo a ESET se mantiene a la vanguardia en lo que respecta minimizar la vulnerabilidad de su contenido ofrecido en sus plataformas.

Los procesos electorales también se han visto afectados como parte de estas nuevas amenazas, mediante el *hactivismo,* forma indirecta para la propagación de ideas o propuestas a favor o encontrar de algún candidato, como se mencionado anteriormente y se detallará en el siguiente capítulo, siendo una de las amenazas claras a las democracias, dado a que dichos procesos pudieran llegar a ser vulnerados de forma directa ya sea interviniendo el resultado como ha quedado demostrado con el caso de *Cambridge Analytica*.

Lo expuesto por Richard hace eco, al ver que el progreso tecnológico ha desarrollado consigo amenazas poco previstas incluso por el mismo Clarke, por lo tanto, es importante el desarrollo de medidas para este entorno, aunque los costos políticos de estas pueden llegar a ser altos, proponiendo un nuevo reto para el Estado tal y como hasta ahora lo entendemos.

## Ciber-conflictos en el actual escenario internacional

Los conflictos internacionales, trascienden y transmutan hacia una nueva forma que se encuentra en vías de ser comprendida, el ciberespacio es un complemento más para el desarrollo de conflictos ajenos a este espacio y propios del mundo físico, existen diferentes ciber-conflictos que se han desarrollado en los últimos años en este nuevo espacio, a continuación, se describen algunos de las más recientes para destacar la importancia que cada día adquieren las ciber amenazas.

Los principales puntos de ataque suelen ser los mismos que atacan, tal es el caso de los Estados Unidos, Rusia, China, Irán, y Corea del Norte quienes son los Estados Nacionales que se encuentran bajo constante asedio en lo que a conflictos en el ciberespacio respecta, siendo estos ataques principalmente disruptivos, robo de información, o espionaje (Sulmeyer, 2019, p.1)

Hay quien expone que los ciberataques más usuales son los relacionados a grandes empresas al menos en 2018, ya que estos representan grandes ganancias para los actores criminales, algunos de los Estados mencionados se han visto involucrados en este tipo de delitos, como lo fue el caso del robo de información a diferentes Universidades y empresas estadounidenses, incluso la ONU en donde el robo de información se estima fue de casi 31 terabytes de información con un valor de casi 3 billones en propiedad intelectual , fueron

señalados diferentes grupos terroristas iraníes con lo que trasladaron al ciberespacio parte de la tensión entre Estados unidos e Irán (Hay, 2019, p.1).

En junio de 2019 Estados Unidos emprende una ofensiva en el esfera del ciberespacio como represalia ante un dron derribado por parte de Irán, siendo el presidente quien declara la autoría del ciberataque, las razones fueron una demostración de poder por parte del gobierno estadounidense sobre su capacidad tecnológica y militar de sus cibercomandos, los cuales de incluso accedieron a los sistemas de control de lanzamientos de misiles iraníes, sobre la efectividad es complejo determinarla a menos que Irán intente enviar un misil, siendo este un elemento de sabotaje a las operaciones militares iraníes (Barnes y Gibbons, 2019, p. 2).

Estas tensiones se han agravado dado a la decisión del presidente Trump en la salida del acuerdo nuclear alcanzado en 2015 por la administración de Barack Obama, ahora se pretende ahogar todas las exportaciones de petróleo iraní, como estrategia ofensiva comercial para debilitar la economía de Irán (Barnes y Gibbons, 2019, p. 3).

Irán ha identificado diferentes redes de espionaje por parte de las agencias de inteligencia estadounidenses, las cuales operan desde 2011 en Teherán, esto fue descubierto por el gobierno iraní al revisar, errores y el mal funcionamiento de sus redes nacionales por un corto periodo, ya que estas redes de espionaje no fueron acompañadas de otras acciones en algún escenario como el aéreo, terrestre o marítimo, no hay un daño aparente o que afecte parcial o totalmente las capacidades militares de Irán (Barnes y Gibbons, 2019, p. 5).

Estados Unidos de acuerdo con Sulmeyer es el principal blanco de ciberataques, desde el caso de la supuesta intervención rusa en las elecciones presidenciales de 2016, en donde el sistema electoral fue vulnerado por una ciber operación, la cual se presume favoreció al actual presidente Donald Trump para su triunfo en dichas elecciones. Bajo este antecedente las agencias de inteligencia estadounidenses advirtieron la posible intervención rusa en las elecciones intermedias de 2017 (Sulmeyer, 2019, p.3).

Aquel acontecimiento ha puesto en duda realmente las capacidades de los cibercomandos de una potencia hegemónica como lo es la estadounidense golpeando incluso hasta en su democracia tema que en el siguiente capítulo se detalla, lo cual muestra como la influencia de Rusia será clave para las relaciones bilaterales entre estas dos potencias que mantienen la tensión por el control global.

Las acusaciones y advertencias establecidas por las agencias de inteligencia estadounidenses no fueron del todo equivocadas, ya que en noviembre de 2017 Rusia fue acusada del ciberataque más costoso de la historia, en líneas anteriores describíamos el ataque de grupos de *hackers* rusos, inhabilitando servicios del gobierno de Estonia en 2007 y casi una década después se desarrolló en 2016 el conocido *Petya Ransomware* un malware con similitudes al *malware I Wanna Cry*; la distribución fue muy sencilla mediante ingeniería social compartiendo un correo era la forma de infectarse usando plataformas de almacenamiento digital como *Dropbox* para expandirse, el objetivo era el secuestro del disco duro solicitando "rescates" que consistían en pagos en *bitcoins* para la liberación del disco duro, a grandes rasgos así funciona *Petya* (Harán, 2018, p.8).

El ciberataque ruso conocido como *NotPetya Attack*, tiene como atencedentes los conflictos entre Rusia y Ucrania desde 2015 con la anexión de Crimea y ahora el Mar de Azov siendo esta una guerra hibrida entre el mundo real y el ciberespacio, la superioridad militar rusa es más que indiscutible, y en un paralelismo podemos notar esa demostración de capacidades ofensivas con el ataque más reciente como el *NotPetya,* el cual venía gestándose desde 2016, justo por el mismo grupo de *hackers* del Kremlin que atacó los servidores y reveló los correos de varios políticos del partido demócrata estadounidense (Banerjea, 2018, p.7).

El ataque fue dirigido a decenas de organizaciones gubernamentales de Ucrania, además de diferentes compañías, en donde detonaron bombas lógicas destruyendo incuantificables terabytes de información, empresas como *Fedex* prácticamente perdieron bases de datos completas en Ucrania y el recuperar toda esa información costará millones de millones de dólares (Banerjea, 2018, p.11)

Es interesante observar las similitudes de las potencias tecnológicas en esa forma demostrar sus capacidades militares en el ciberespacio, e incluso pudiera asumirse como provocaciones para desencadenar un conflicto a mayor escala, y aunque los intereses, así como el contexto en que se desarrolla cada conflicto es diverso.

# CAPÍTULO III.-ESTADOS UNIDOS: EL PROCESO DE MILITARIZACIÓN DEL CIBERESPACIO 2008-2016

El objetivo de este capítulo es analizar las estrategias y medidas de corte militar por parte de los Estados Unidos en la última década. Esté capitulo está dividido en cuatro apartados, en el primero analizamos desde la perspectiva estadounidense el rol dentro de la escena internacional, así como las capacidades técnicas y militares de los Estados Unidos. En el segundo apartado se enumeran y destacan las políticas y estrategias de defensa implementadas por el gobierno y ejército estadounidense. En el tercer apartado se analiza la efectividad y consecuencia de las medidas tomadas. Finalmente, en el cuarto y último apartado se describen los principales retos en materia de ciber-seguridad que enfrentó la administración de Barack Obama incluso a finales de su mandato.

## 3.1.- Proceso de militarización en el ciberespacio estadounidense

La internet y la abstracción que representa el ciberespacio fue resultado de un gran esfuerzo y trabajo del ejército estadounidense durante la Guerra Fría, lo cual fue parte de su consolidación como potencia, pretendiendo garantizar su poderío militar, en un escenario hostil, en un periodo de tensión entre dos grandes potencias como lo fue la Guerra Fría, creando lo que hoy en día entendemos como internet.

Estados unidos a partir de la Segunda Guerra Mundial ha sido un actor con un rol activo dentro de la escena internacional, y actualmente el ciberespacio no está exento de ser un campo en el cual se demuestre la capacidad y el alcance de esa potencia; la incursión de Estados Unidos en el mundo virtual es claramente comprensible con base en lo que se ha tratado en esta investigación, dado a que no ha sido inmune a las amenazas de este nuevo espacio, siendo también la potencia que ha enfrentado más ataques en dicho entorno.

Desde una industria tan significativa económicamente como lo es la industria del entretenimiento hasta agencias con gran importancia estratégica como la NASA, y la NSA, CIA entre otras han sido atacadas, saboteadas o sufrido ataques de espionajes por actores no tradicionales y presuntamente por otros Estados, quienes se resguardan en el anonimato que este espacio ofrece, siendo 2016 también un año donde el uso y manipulación de esta nueva

estructura conocida como redes sociales, fue un factor determinante en una elección presidencial.

Asimismo, esta potencia ha sabido emplear y sacar provecho de las nuevas plataformas tecnológicas, siendo sus agencias de inteligencia las más reconocidas a nivel internacional las cuales han tomado cada vez más protagonismo, así como sus divisiones dedicadas a la seguridad en el ciberespacio, las cuales ha incrementado el número de ciber-comandos de carácter militar para la defensa del ciberespacio.

Además, se ha desarrollado una de las doctrinas de mayor impacto dentro de materia de ciberseguridad como lo es la teoría del colapso, la cual ha trazado los ejes de las medidas a favor de la regularización del ciberespacio, así mismo esta doctrina busca legitimar cualquier política implementada por parte del gobierno estadounidense, con el motivo de salvaguardar la seguridad nacional. Siendo esta la que mantiene mayor aceptación entre los expertos de seguridad militar estadounidenses. Teoría la cual nos sitúa en la perspectiva estadounidense y da razón de las políticas emprendidas por la administración de Obama.

El sustento y la aceptación de dicha teoría deviene de los incidentes de sabotaje, robo de información y espionaje que se han explicado en el capítulo anterior, las condiciones tan particulares de este espacio complican el desarrollo correcto y funcional de un marco legislativo, encumbrando así este tipo de doctrinas, y la promoción de medidas de defensa, así como el desarrollo de este tipo de políticas.

El proceso de militarización del ciberespacio ha sido la respuesta a las amenazas que en este espacio se presentan, ya que, desde la perspectiva estadounidense imperante en la administración de Obama, la seguridad Nacional mantenía una vulnerabilidad en este entorno virtual, por lo cual se priorizó alcanzar un desarrollo tecnológico optimo que permita mantener la seguridad interna y por ende emplear dicho progreso para fortalecer su *status quo* en el escenario global (The White House, 2009, p. 3).

Aunque Richard Clarke destaca que la seguridad del ciberespacio comienza a tener importancia en 2003 dos años después del atentado a las torres gemelas, considerando el sabotaje de los mecanismos de control aéreo para facilitar el ataque, aunque es posible considerar importante este acontecimiento, poco fue el trabajo realizado en materia de ciber seguridad, hasta 2006 la estrategia por parte de las diferencias agencias de inteligencia y

seguridad estadounidense era el monitoreo continuo y la neutralización de alguna posible amenaza (Clarke y Kanake 2010, p. 29).

*Wikileaks* marcó un antes y después en los procesos de seguridad de las redes informáticas estadounidenses, es en 2010 donde el tema de ciber-seguridad polariza la agenda nacional estadounidense y se redoblan esfuerzos para proteger de cualquier vulnerabilidad el ciber-espacio, ya que en ese año se desarrolló "La Estrategia Nacional de Seguridad en el Ciberespacio" documento en el cual se expresan las funciones de las agencias ya existentes y creando otras con el propósito de la defensa nacional en el ciberespacio.

Según Srikrishna (2010), Estados Unidos se encuentran en problemas desde la aparición de internet a partir del proceso de globalización, durante el tránsito a la nueva era digital, Este país, asegura, se ha preparado desde el área militar para cualquier acontecimiento o amenaza que provenga del ciberespacio, dicha preparación es parte esencial de la formación del ejército estadounidense por décadas (p.4).

Algunos de estos comandos militares datan desde finales de la década de los 1970s. En la siguiente tabla se expondrán los comandos más destacados por parte del Ejército estadounidense encargado de la defensa y protección del ciberespacio, o cualquier amenaza derivada que afecte los intereses del Estado.

No es casualidad que la mayor parte de los comandos militares creados para la defensa del ciberespacio iniciaran a formarse en 2010, el año después del golpe político y diplomático que enfrentó los Estados Unidos con la filtración de información por parte de *Wikileaks* destacando la prioridad del gobierno de Estados Unido en protegerse de una segunda fuga de información.

A partir de ese año se han ido incrementando los comandos especializados en ciber-seguridad, de acuerdo a la información expuesta en la tabla en 2010 fue un año clave para las nuevas divisiones encargadas de esta área, es importante destacar que figuras como Clarke promovieron desde la administración Bush este tipo de divisiones dentro del ejercito como parte de la respuesta a las posibles amenazas externadas en la teoría del colapso.

También es importante comprender el contexto de la escena internacional en 2010, a casi una década de la invasión a Irak y Afganistán, Estados Unidos mantenía un desgaste político, económico y militar; además no sólo habría enfrentado el impacto generado por *Wikileaks* también se estaba recuperando de una gran crisis financiera a escala global.

*Tabla 3.- Ciber-comandos del ejército estadounidense*

| **Comando.** | **Año de Creación.** |
|---|---|
| INSCOM (Inteligent and Security Command) | 1977 |
| 780th Military Inteligence Bridge | 1998 |
| Air Force Cyber Command | 2008 |
| U.S. Cyber Comand (USCYBERCOM) | 2009 |
| 1st 10 Comand | 2009 |
| U.S. Army Cyber Comand | 2010 |
| NETCOM | 2010 |
| Fleet Cyber Command | 2010 |
| Marine Corps Cyberspace Command | 2010 |
| Coast Guard Cyber Command | 2010 |

Fuente: Elaboración propia con base en la información expuesta en la página de ciber-comandos del ejército estadounidense.

En 2010 ocurre un hecho que compromete la lealtad de este tipo de cibercomandos ya que en ese año fue capturado Bradley Manning, miembro del ejército estadounidense de la 10° División de Montaña 2° Brigada del equipo de combate siendo soldado de primera clase, quien fue uno de los responsables en la filtración de información equivalente a más de un millón de registros de la participación estadounidense en la guerra contra Irak desde 2008 (Van, 2013, p.5).

Michelle Van (2013) quien fue la encargada de contra inteligencia del Centro de políticas de seguridad estadounidense crítica y tilda como traición el actuar de Manning, expone que la información clasificada de operaciones de inteligencia que se llegara a filtrar podría representar un riesgo potencial para la seguridad nacional.

Es importante destacar que *Wikileaks*, fue que uno de los eventos coyunturales respecto a la incursión de Estados Unidos en el ciberespacio y el desarrollo del proceso de militarización, aunque la filtración tuvo origen en el mismo ejército, las iniciativas de corte militar y el acceso a esta información comprometió de sobremanera la hegemonía estadounidense, siendo un trabajo orquestado desde dentro.

La CIA por su parte elaboró un plan de control de daños estableciendo las medidas y las consecuencias para evitar este tipo de actos en el futuro, desarrollando un protocolo entre los miembros de las diferentes agencias de inteligencia y seguridad, así como las nuevas divisiones y comandos establecidos para la defensa del ciberespacio (Sellers y Shaw, 2015, p.4).

La ciber-guerra entendida como la infiltración, sabotaje y robo de información, la destrucción o corrupción del funcionamiento de los equipos que mantienen funcionando a la estructura critica, siendo este entorno virtual un campo más de conflicto donde con relativa facilidad es posible atentar contra los intereses nacionales todo esto manteniendo el anonimato del autor (Lewis,2010 p.3).

De esta forma el gobierno de los Estados Unidos como parte de la doctrina y estrategia militar mantienen a sus tropas bajo los siguientes conceptos tácticos:

1.- Objetivos: Todas las operaciones militares tienen objetivos claros y definidos.

2.- Ofensiva: Mantener y explotar la iniciativa al atacar.

3.- Concentrar y controlar el poder de la batalla en el momento y lugar adecuado.

4.-Economizar la fuerza: Emplear lo menos de fuerza en los combates, para tener respaldo en caso de un segundo combate.

5.- Maniobrar: Llevar al enemigo a un terreno en el cual permanezca con desventaja y se posea flexibilidad en el combate.

6.- Unidad: Todos los objetivos deben ser cumplidos por unidades guiadas por un comandante.

7.- Seguridad: Nunca permitir que el enemigo se haga de la ventaja de manera sorpresiva.

8.- Ataque sorpresa: Atacar al enemigo donde y cuando no esté preparado.

9.- Simplicidad: Mientras más claros y sencillos se mantengan los objetivos asegura mayor eficiencia en el cumplimiento de estos. (Dietz, 2012 p.176).

Muchos de estos conceptos tácticos corresponden a los comandos del ejercito tradicional los cuales trabajan de forma coordinada en cada operación, aunque se pretende aplicar y adaptar estos al ciberespacio por los comandos y fuerzas especializadas, aunque dado el sesgo y la ausencia en la regulación y gobernanza del ciberespacio de acuerdo a Dietz este tipo de estrategias militares por ahora se mantiene con un fin defensivo.

A su vez la efectividad de los ataques perpetrados dentro del ciberespacio rompe con parte de los conceptos y estrategias de la doctrina militar tradicional, ya que se debe contar con el equipo tecnológico más avanzado para así mejorar los mecanismos de defensa, además los ataques perpetrados en el entorno virtual resultan ser más económicos y sustancialmente generan más daño a estructuras críticas que los ataques convencionales. (Dietz et al., 2012 p.176)

China y Rusia han sido las potencias acusadas por el gobierno estadounidense de infiltrarse en las bases de datos para el robo de información, y se propone que ambos gobiernos contratan "ciber-mercenarios" para el espionaje, por lo cual al menos las principales potencias europeas con divisiones especializadas en los servicios de inteligencia del ciberespacio mantienen una constante búsqueda de estas redes de espionaje. (Foncillas, 2013 p. 8)

Por ahora el entrenamiento y los ejercicios de los ciber-comandos se encuentran como clasificados, no existen informes sobre operaciones, y Dietz asegura que la mayor parte de sus actividades se basan en servicios de contra inteligencia. Aunque no hay mucha información sobre las armas y herramientas que emplean es posible suponer que mantienen una gran ventaja tecnológica respeto a otros Estados. (Dietz et al 2012 p.9)

Esta nueva dimensión e idealización de la guerra, modifica la doctrina militar, así como la compresión estratégica, desde una cadena de mando, y una estructura jerarquizada y vertical hasta llegar una nueva reestructuración de los comandos operativos del ejército. Entender el proceso de militarización del ciberespacio es como entender el dominio del espacio aéreo durante la primera guerra mundial ya que aprovechando esta ventaja tecnológica el atacar la infraestructura critica fue importante para ganar estratégicamente las batallas, aunque por ahora nos encontramos en un proceso muy primitivo del dominio de la internet no pasará mucho para el control de este. (Dietz, et al 2012 p.169)

### 3.2- Políticas y medidas en defensa del ciberespacio

Como parte de las políticas gubernamentales establecidas en 2009 se comenzó con la implementación de la estrategia de ciberseguridad propuesta en 2003 por Clarke, tal como *The Comprehensive National Cybersecurity Initiative* (CNCI), siendo esta la primera iniciativa de la administración de Obama la cual pretendía establecer los mecanismos para la defensa de las armas de disrupción masiva, iniciativa en donde se abordaban 12 directrices que contemplaban la protección de las redes del ejército, de la población civil y de la redes de la infraestructura critica gubernamental, aunque el costo era la privacidad ya que se pretendía monitorear el tráfico de la red dada las criticas la iniciativa no prosperó (Stone M. 2010, p. 1).

También en 2009 se emitió el documento *"The Cyberspace Policy Review*" en el cual se pretendía establecer una estrategia en coordinación con la ciudadanía y la iniciativa privada con el apoyo gubernamental, para el desarrollo de infraestructura capaz de adaptarse a las diferentes amenazas que representa el ciberespacio es por esto que las agencias de inteligencia, así como la mayor parte de las dependencias gubernamentales, de seguridad y de comercio adoptaron iniciativas basadas en medidas preventivas que garanticen el buen funcionamiento de sus servicios en el ciberespacio en caso de una crisis o ataques a dicha infraestructura como lo propone en la teoría del colapso.

Existen al menos cinco documentos de gran importancia en materia de ciber seguridad, estos han sido elaborados y propuestos por distintos órganos del gobierno estadounidense, durante la administración de Obama; en estos se delinean los aspectos clave para el desarrollo de estrategias y la implementación de medidas que garanticen la seguridad y operatividad del gobierno estadounidense dentro de este entorno virtual, los cuales sin duda invitan a la discusión legislativa. Parte de estos documentos atienden a los nuevos retos que propone internet para la operatividad y funcionalidad de las instituciones gubernamentales estadounidenses. El primer documento fue elaborado desde el Departamento de Comercio al mismo tiempo que Departamento de Defensa estableció sus líneas de acción para atender los problemas y resolver las amenazas que resulten de en este espacio ambos documentos fueron presentados en 2011.

En ese mismo año el poder ejecutivo también desarrolló una propuesta de estrategia internacional para la defensa del ciberespacio, este documento será la base de la Orden

Ejecutiva 13636 de 2013. En estos se establece como prioridad la mejora de la infraestructura critica estadounidense desde el ciberespacio de forma defensiva y la prevención y atención de los ciberataques.

Por último, en 2015 La Secretaria de Seguridad a través el Departamento de Defensa desarrolló una Estrategia de ciberseguridad como parte del esfuerzo de la administración para la consolidación de la seguridad en el ciberespacio.

Respecto a las dificultades y el riesgo potencial que representan las amenazas antes mencionadas, Estados Unidos han puesto departamentos especializados en ciber-seguridad en las diferentes secretarias y agencias exclusivamente para lidiar con dichas amenazas, también se han desarrollado medidas con el fin de garantizar la seguridad en el ciberespacio.

Como parte de estas estrategias la Administración Nacional de Telecomunicaciones e Información (NTIA) y la agencia gubernamental como el Instituto Nacional de Estandarización de la Tecnología (NIST) son organismos que han colaborado para el desarrollo de la Estrategia Nacional en pro de garantizar el buen funcionamiento de los servicios ofertados en línea por los departamentos que componen el aparato gubernamental (Departament of Commerce, 2011, p.7).

Además, el Departamento de Comercio ha creado un equipo encargado de regular las políticas en internet, en los Estados Unidos, ya que de acuerdo con el "*CyberSecurity Green Paper*" creado por el Departamento de Comercio, con estas medidas se aspira a mantener la hegemonía económica de los Estados Unidos, ya que este departamento representa un elemento clave para la economía estadounidense, esta medida se adelanta a los retos que representan el ciberespacio en esta área (Departament of Commerce, 2011, p.11).

El departamento del comercio también consideró *un aspecto importante para la iniciativa privada ya que* de acuerdo con el Comité de economía del congreso de los Estados Unidos: "La violación a los Derechos de Autor (Piratería) reduce el crecimiento económico, por ende, se debilita la competitividad comercial de la nación y así mismo empobrece a la industria del entretenimiento ya que reduce la creación de trabajos en la misma". Esta violación a los Derechos de Autor ha ido en un aumento constante y acelerado, de acuerdo un informe del congreso estadounidense la industria del entretenimiento en los Estados unidos pierde al año más de un trillón de dólares a consecuencia de la violación a los

Derechos de Autor lo cual debilita parte de su economía perdiendo en 2010 1.1 trillones de dólares afectando la economía de grandes empresas (Departament of Commerce, 2011, p.29)

Manteniendo el antecedente en la defensa del sector privado por parte del mismo departamento en el congreso que en 2010 promovió la aprobación de la Ley SOPA y PIPA, buscando contrarrestar los problemas que representan para las diferentes industrias la violación a los derechos de autor, en aras de fortalecer la economía nacional, y combatir con este tipo de delitos.

Es notable que la industria privada posee una gran influencia en cualquier economía y por consecuencia se aspira a blindarla, es significativo observar que 2010, fue el año de la aprobación de dichas leyes por el congreso, sin duda se benefició por mucho a todo el sector privado que es en esencia es la base de la economía estadounidense, previo al año de electoral que se avecinaba. Tal vez siendo fundamental para el financiamiento de campañas que se iniciaban en 2011.

La premura por desarrollar este tipo de leyes recae en que de acuerdo con un informe del departamento de comercio estadounidense 75 de sus industrias se mantienen gracias a las patentes y a los Derechos de Autor siendo la industria del entretenimiento y de indumentaria la más afectada de las 313 industrias que operan el país. Estas 75 industrias representan el 34.8% del producto interno bruto estadounidense esto para 2010 (Departament of Commerce, 2011, p.45).

Es importante comprender las prioridades del Estado, así como proteger uno de los elementos de poder que lo sitúan como potencial a nivel mundial, dada la capacidad de su economía, el sistema económico imperante recae en la capacidad de competitividad y como se ha mencionado gran parte del PIB estadounidense proviene de industrias en donde la piratería ha dañado en gran escala sus ingresos lo cual a futuro podría generar problemas en el sector privado y por ende atraer problemas económicos.

El Departamento de Seguridad Nacional de los Estados unidos (DHS) se encarga de la protección de la infraestructura crítica nacional, pretende prever cualquier amenaza que atente contra sectores clave como el de salud, el bancario y el de telecomunicaciones en caso de alguna emergencia o ataque (The Departament of Defense, 2015, p.11).

Otro de los Departamentos que participan de manera importante para la seguridad de Estados Unidos ,es el Departamento de Defensa (DOD) encargado de la seguridad en

operaciones de orden militar, siendo el más importante ante los problemas ya librados dentro de este nuevo espacio (The Departament of Defense, 2015, p.12).

Por parte del Departamento de Defensa se ha priorizado políticas efectivas dentro del espectro de las amenazas hacia el aparato gubernamental, asi mismo se han elaborado estrategias que faciliten el alcance de los intereses nacionales en este nuevo espacio objetivo en el que ya varias agencias se encuentran trabajando.

La mayoría de las agencias de inteligencia se constituyen en los albores de la Guerra Fría, comprendiendo el contexto de la escena internacional, siendo estas agencias creadas como parte de las estrategias para salvaguardar la integridad nacional y garantizar la seguridad del Estado.

En la tabla número 4 se observar el despliegue técnico y el esfuerzo por el Estado justo después de 1945 por mantener la prioridad sobre su seguridad ante el progreso tecnológico que vendría presentándose en aquel periodo y aún en la actualidad, cabe destacar que en la información presentada se excluyó agencias y otras divisiones encargadas de seguridad por no estar involucradas de forma directa con la ciber-defenesa.

El departamento como mayor injerencia en materia de ciber defensa es el Departamento de Defensa, la cual mantiene mayor antigüedad y se ha sido la encargada de la creación de las diferentes agencias presentadas las cuales a su vez tienen la tarea de proteger y garantizar la seguridad nacional prácticamente desde la creación de los Estados Unidos.

Hasta ahora el Estado ha buscado maneras de sobreponerse pese a las amenazas ya expuestas, buscando mecanismos que garanticen el mantenimiento del *status quo*; Los campos con mayor prioridad son el campo militar y económico, esta incursión de los diferentes departamentos ya mencionados da muestra de la capacidad y el interés del Estado por mantenerse a la vanguardia de este desarrollo tecnológico pretendiendo así la supremacía en la escena internacional.

*Tabla 4.-*
*Agencias y departamentos de Inteligencia de los Estados Unidos*

| Nombre (Agencia, Departamento o Dependencia) | Año de creación | Funciones dentro del Ciberespacios. |
|---|---|---|
| Departamento de Defensa (DOD) | 1775 | Encargada de coordinar y supervisar las agencias y funciones relacionadas a la Seguridad Nacional y el Ejército. |
| Buro Federal de Investigación. (FBI) | 1908 | Mantiene un departamento encargado de combatir los ciber-delitos y el terrorismo. |
| Agencia Central de Investigación (CIA) | 1947.- Comienzos de la Guerra Fría, mantiene un rol importante en este periodo como agencia de Inteligencia. | Operaciones en cubierto, espionaje, sabotaje y principalmente servicios de inteligencia. |
| Agencia de Seguridad Nacional (NSA) | 1952. Agencias Secreta hasta 1970. | Monitorear todo lo relacionado en el campo de la seguridad de la información. |
| Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA) | 1958 | Encargada del Desarrollo de Nuevas Tecnologías para el Uso Militar (creadora de Internet). |
| Agencia de la Defensa de los Sistemas de Información (DISA) | 1991 | Encargada de Proveer Soporte técnico y la seguridad de los sistemas computacionales. |
| Agencia Nacional de Inteligencia Geo-Espacial (NGA) | 2003 | Cumple como labor de Apoyo a la NSA y el DOD. |
| Fuente: Elaboración propia con base en la información de la página oficial de la oficina del Director de Inteligencia Nacional. | | |

Además, el Estado reconoce la dependencia tan marcada que existe hacia estas nuevas tecnologías, ya que desde 2008 la seguridad del internet ha sido prioridad tanto para el sector público como privado, de acuerdo con Clark W. estas medidas han sido exclusivamente defensivas (Clarke y Kanake 2010, p. 72).

Bajo esta misma línea de pensamiento y sobre la incursión del ciberespacio de manera netamente defensiva la Agencia de Seguridad Nacional (NSA) se ha encargado de la creación de un centro académico para la ciber-defensa, basada en la iniciativa presidencial para la educación sobre ciber-seguridad presentada en 2009.

Dicha iniciativa mantiene como directrices establecer un orden y la creación de nuevos organismos encargados de vigilar y controlar en la medida de lo posible, lo que ocurre en el ciberespacio, de prescindir del robo de información desde y el sabotaje electoral, futuros eventos que dejarán entrever la efectividad de estas estrategias.

### 3.3 Resultados Ganancias y pérdidas de las medidas implementadas

A pesar de todas estas medidas, en 2013 Edward Snowden, contratista de la NSA reveló hacia donde van encaminadas cada una de las políticas internas de este país, sugiriendo que estas pretenden crear una gran red de vigilancia, la cual estaría encargada de monitorear todas y cada una de las interacciones desarrolladas en la internet, lo cual como ya se ha mencionado en el apartado anterior donde se contrapone el dilema de la seguridad contra la privacidad (Alvarez, 2013, p.27).

De acuerdo con Álvarez, Edward Snowden pertenecía a un selecto grupo de personas con acceso a información "privilegiada" del aparato gubernamental estadounidense, miembro de aquellas nuevas divisiones encargadas de la ciber defensa, su caso se suma a los casos de filtración de información ya que en 2013 expuso secretos de inteligencia de alta confidencialidad.

Van como parte de los equipos de contra inteligencia estadounidenses desde la administración de Bush, condena totalmente y con repudio el actuar de Snowden, ya que comprometió documentos altamente clasificados, así enemigos declarados hacia los Estados Unidos, sin darse cuenta el daño interno que dejó a la NSA, fortaleciendo las capacidades de China en materia de ciberespionaje asumiendo que son los ciber depredadores por excelencia, así mismo facilito el trabajo de adversarios políticos para los Estados Unidos como Rusia quien mediante *wikileaks* encontró información sensible para situar a Estados unidos en una posición de vulnerabilidad (Van, 2013, p.5).

También es importante recalcar que las filtraciones de Snowden no fueron cables diplomáticos, ni información de las operaciones de corte militar como las de Manning pero

reveló parte clave de los intereses y las pretensiones globales del gobierno de en el desarrollo de las políticas ya antes mencionadas.

Según Bonifaz (2017), Edward Snowden fue agente de la CIA así como de la NSA, lo cual le permitió tener acceso a información clasificada que por convicción y motivos "éticos" decidió revelar; alertando y dando a conocer la gran red de espionaje global de los Estados Unidos, además de filtrar datos importantes sobre el programa de vigilancia conocido como PRISM (p.5).Una de las criticas constantes desde la propuesta de la CNCI, fue la privacidad, tema incendiario para la opinión pública estadounidense ya que esta se vio atentada no solo por el gobierno sino por grandes empresas y compañías que venden los hábitos de consumo y preferencias de la población lo cual como se ha discutido en el capítulo anterior se carece de una ética dentro del ciberespacio y el individuo blanco de ofertas, dicha información es vendida al mejor postor.

En 2015 la administración del Presidente Barack Obama, desarrollo el Plan de Acción de Ciber-seguridad Nacional (CNAP), el cual remarca la posición del Estado en la escena internacional sobre la militarización del ciberespacio, en la cual, con autorización del congreso, el ejecutivo desarrolla esta iniciativa con tres ejes primarios:

- Establecer una comisión encargada de la ciber-seguridad a nivel nacional, la cual determine un marco regulatorio que facilite el trabajo de las Agencias y Dependencias Gubernamentales en el ciberespacio, además esta comisión certificará y brindará mayor y mejor seguridad de los ciudadanos estadounidenses ante las amenazas exteriores. Esto representa modernización en la forma que aborda la seguridad a nivel nacional.
- La empoderación de los cibernautas estadounidenses protegiendo aún más sus cuentas y la navegación dentro de la red, empleando nuevos mecanismos de autenticación como el uso de huellas dactilares, y el escáner de retina.
- Aumento al presupuesto destinado en el desarrollo de programas y comandos especializados en la seguridad del ciberespacio, priorizando y la imperiosa necesidad de estar preparados en este nuevo campo de interacción global. (The Departament of Defense, 2015, p.87)

Este tipo de medidas implementadas y desarrolladas por el ejecutivo, representan un riesgo potencial al menos para la privacidad de los estadounidenses, ya que al menos en el segundo punto se expresan mecanismos para mantener un mayor control sobre los cibernautas y el contenido que frecuentan. Lo cual genera conflicto entre garantizar la seguridad o proteger la privacidad ya que se cristalizan ideas como la de George Orwell en 1984, en donde el Estado tendrá acceso en cualquier momento que lo requiera violando así la privacidad de sus conciudadanos confirmando lo expuesto por Snowden.

Con estas medias el gobierno buscó fortalecerse y minimizar algún riesgo potencial contra la seguridad nacional que ponga en riesgo sus intereses, además de plantear la posibilidad de cooperación con organismos privados fortaleciendo así la figura del Estado, además de ser pionero en la implementación de estas medidas en la escena internacional.

Por lo contrario, Greenwald (2014) sugiere que Estados Unidos luego de los acontecimientos del 11 de Septiembre de 2001, bajo la amenaza terrorista y en pro de la seguridad ha abusado de poder, polarizando muchas medidas del ejecutivo con intensiones que van más allá de la seguridad, exponiendo que el presidente George W. Bush mantenía virtualmente la autoridad ilimitada para hacer lo que fuese por la seguridad nacional (p.15).

En la administración de Obama si bien se busca la legitimidad de las medidas adoptadas para el ciberespacio se asume de forma más tenue y que las políticas desarrolladas por Bush, ante un contexto diferente, pero buscando los mismos objetivos reducir el riesgo potencial del terrorismo y garantizar la seguridad nacional.

Esta atmosfera que conducía al abuso de poder por parte de la potencia norteamericana la cual sin escatimar costos se ha envuelto en la búsqueda y perfeccionamiento constante de mecanismos de control poblacional, y en un pensar completamente paranoico ha extremado sus políticas como se ha venido mencionado.

### 3.4 Contexto internacional principales retos de la administración de Barack Obama

El sistema internacional en la última década ha venido enfrentando cambios de forma drástica, los conflictos ya existentes se han agudizado, y como se ha mencionado con anterioridad, el ciberespacio representa un sitio más en el cual el conflicto puede ser

trasladado, por la característica del mismo, ya que resulta económico y el daño que puede generar es mucho.

Bajo la reducción del costo en los ataques, también se han fortalecido e incrementado el número de actores ajenos a la figura de Estado, desde los grupos terroristas hasta hactivistas o ciber-mercenarios quienes son parte de estos nuevos actores, figurando en un sistema que por tradición era exclusivo de los Estados al menos desde la perspectiva tradicional realista.

Los actores no estatales ahora forman parte activa dentro de la realidad internacional y de la agenda de seguridad, así como de la dinámica de poder que poseen los actores tradicionales; Considero que es importante señalar e identificarlos porqué jugarán un rol muy importante en el desarrollo de un conflicto dentro del ciberespacio tal y como lo han venido haciendo.

Por otra parte, organismos como la ONU, la OTAN y la Unión Europea han buscado establecer mecanismos de defensa previendo la capacidad de daño que podría representar un ciber-ataque, existen esfuerzos en conjunto para asegurar la capacidad de respuesta ante cualquier ataque que se perpetre por esta vía.

La ONU y la Unión Europea han tratado de establecer un marco jurídico que permita establecer normas que regulen el uso de las plataformas y redes tecnológicas garantizando la seguridad tanto del usuario como del propio Estado, esto sin mucho éxito, ya que estas amenazas si bien son latentes y potenciales se encuentran en un segundo plano, y la realidad inmediata requiere de la atención de problemas de otra índole por ende los esfuerzos han sido significativos pero insuficientes.

Es importante recalcar que internet nace como un experimento aislado en donde se buscaba mayor efectividad y seguridad en las telecomunicaciones dentro del campo militar, actualmente los gobiernos no cuentan con una política que regule lo que en el ciberespacio ocurre, hasta ahora legislativamente todo ha sido Laissez Faire dejar pasar (Deibert, 2015, p. 10).

Aunque desde la perspectiva militar y como se abordó anteriormente, la OTAN ha sido la organización internacional que exclusivamente mediante un conflicto bélico o un ciberataque de gran magnitud ha desarrollado protocolos y mecanismos de defensa, contando con un manual el cual fue elaborado exclusivamente para establecer las pautas del desarrollo

de una ciberguerra y si fuese necesario responder con una agresión militar en el mundo físico. Así mismo esta organización cuenta con una división militar exclusivamente creada para la formación de efectivos especializados en ciber-ataques, la cual facilita la cooperación y el desarrollo tecnológico para sus Estados miembros.

En la teoría neorrealista este tipo de cooperación es una relación más de poder, donde los actores tradicionales buscan fortalecerse en el ámbito militar, es notable observar el progreso dentro de esta área en comparación al área jurídica e institucional que no posee la capacidad de lidiar de forma efectiva con estas nuevas amenazas.

Como se ha descrito con anterioridad el ciberespacio y lo que en este acontece no responde a los conceptos tradicionales como el de soberanía, frontera, territorialidad dada la inexistencia del espacio físico donde estos fenómenos se manifiesta, por lo cual esto cual representa un conflicto en el actuar de los Estados quienes poco a poco se han ido adaptando a las consecuencias del desarrollo tecnológico.

Este nuevo espacio se encuentra en proceso de colonización por las potencias tecnológicas las cuales han previsto la importancia en caso del desarrollo de algún conflicto, siendo esta una vía tanto táctica como estratégica reitero exclusivamente por las potencias tecnológicas las cuales poseen la capacidad militar y tecnológica para ser parte de un conflicto de esta naturaleza, reduciendo así la incursión de Estados con un mediano desarrollo económico y tecnológico, siendo esta una limitante para la capacidad de poder de un Estado al menos en este tipo de conflictos. por otra parte, el hecho de que los costos sean menores para el desarrollo de un conflicto bélico, El Estado con un ejército reducido podría emplear los ciber-ataques como ofensiva o defensiva como respuesta a las amenazas de otro Estado.

Todo está contextualización nos conduce a comprender y analizar desde la perspectiva realista el proceso de militarización del ciberespacio, teoría que sin dudas impera de forma activa en la política exterior estadounidense

En el ciberespacio, las relaciones de poder se mantienen presentes, pese a no existir propiamente una zona de influencia determinada dentro de este espacio, esta misma se configura de acuerdo a la escena internacional física la cual es determinante para la comprensión de la dinámica dentro de este nuevo espacio (Rebinad, 2008, p. 89).

Estados Unidos como se ha mencionado ha mantenido un gran despliegue en relación a la defensa de sus instituciones y su seguridad nacional, al ser una de las potencias

tecnológicas ha podido desarrollar una gran capacidad tecnológica y militar que le permiten garantizar la seguridad nacional ante cualquier amenaza.

Para los Estados Unidos la internet se ha convertido en un elemento clave del desarrollo económico y tecnológico que han tenido en estas últimas décadas, al ser una potencia tecnológica se ha creado una dependencia indivisible entre su desarrollo y crecimiento tecnológico con la constante amenaza que atentan contra su seguridad, ahí recae la importancia de la urgencia en normar lo que ocurre en el ciberespacio.

Las relaciones de poder gestadas presentes en el mundo virtual son determinadas con la dinámica de poder que se conoce en el mundo físico, siendo el mundo virtual un espacio más para dominar o ser dominado, es claro que la figura del Estado es el blanco de ataque desde diferentes Flancos y por diferentes actores desde cualquier parte del mundo en cualquier momento.

La naturaleza hostil y anárquica del sistema internacional, obliga al Estado a sobrevivir, el ciberespacio se ha convertido en parte intrínseca de la naturaleza del sistema ya que es un elemento que promueve las relaciones de poder, así mismo no se encuentra regulado de forma clara y funcional, siendo este un reflejo del propio sistema internacional carenciado de regulaciones efectivas.

Estados Unidos tiene clara esta idea, la creación de un ciber-ejército ha sido una necesidad dada las condiciones de este nuevo espacio, por otra parte, el dominio de este espacio representa de forma clara la capacidad de poder de un Estado, la disputa por este espacio se limita a la capacidad militar y económica del Estado.

La administración de Obama fue la que implementó y desarrolló un mayor número de políticas internas a favor de la ciber-seguridad, con el fin de proteger a las estructuras críticas que sugiere la teoría del caos, y así aumentando notoriamente su ciber-ejercito. El incremento en la capacidad militar deviene como réplica a las filtraciones y la amenaza al status quo ha representado la incursión de nuevos actores como Julian Assange con *wikileaks*.

Poco efectivas las medidas adoptadas por la administración de Obama, ya que la mayor parte de los conflictos que ha atravesado el Estado norteamericano, al menos los dos casos de mayor impacto durante la administración tuvieron origen de forma interna, siendo miembros del mismo ejército y de las propias agencias de seguridad nacional quienes han atentado contra la hegemonía de este país.

En el proceso del cierre de la administración de Barack Obama y la transición al nuevo gobierno se suscitaron diferentes conflictos una vez más relacionados con internet y este entorno virtual, en los cuales adversarios como Rusia volvieron a ser el foco de atención y a su vez se demostró la ineficacia de las medidas desarrolladas durante dicha administración.

*Facebook, plataforma de espionaje y propaganda política: Caso Cambridge Analytica*

Como se ha expresado existe un dilema constante de seguridad el cual padecen los internautas en la red a costa de la privacidad, cada vez las plataformas de internet han establecido condiciones de uso en las cuales mantener el anonimato es casi imposible, las redes sociales se han convertido en uno de los instrumentos de viralización de información personal, aunque las políticas de privacidad de dichas redes carecen de seguridad, tal y como se demostró con el caso de *Cambridge Analytica*, caso que forma parte del entramado en la supuesta intervención en las elecciones de 2016 en Estados Unidos. Ya que estas plataformas son fácilmente manipulables y sus usuarios fácilmente influenciables.

Siendo Facebook una de las plataformas interactivas con mayor demanda e influencia a nivel mundial, esta empresa se caracteriza por emplear elementos de marketing como el *big data,* el cual consiste en reclasificar gran cantidad de información y hacerla comercial, en este caso categorizar en diferentes tipos de usuarios, comprendiendo el rango de edad, su ubicación, sus gustos, su orientación, sexual, política, ideológica, de credo etc. con el fin de vender esta información a grandes empresas y llegar a una mercado específico (Observatorio Electoral UNAM, 2018, p.2).

De acuerdo al informe del observatorio electoral de la UNAM, durante las elecciones de 2016 en Estados Unidos se tuvo acceso a datos personales e información sensible de más de 50 millones de internautas, siendo la mayoría de estos usuarios de Facebook, plataforma empleada para la promoción del candidato Republicano a la presidencia, la Información la fue obtenida mediante una aplicación parecida a la de un test de personalidad en donde los usuarios cedieron los permisos sobre el uso de su información sin darse cuenta como sus datos iban a ser empleados. Una vez obtenidos estos datos la empresa estableció el sector poblacional al que iban los mensajes dirigidos a favor de un candidato o de otro. Siendo una

herramienta de la política digital que como muchos de los ejemplos de este trabajo aún se encuentra sin regulación (Observatorio Electoral UNAM, 2018, p.4).

Dado este sesgo jurídico, la empresa *Cambridge Analytica* establecida en Londres y de acuerdo con un informe presentado por la misma empresa, esta empleó diferentes algoritmos que le servirían para diseñar más de 10 mil tipos de anuncios para diferentes sectores poblacionales y así poder distribuirlas mediante las redes sociales como Facebook, Twitter, Instagram y Snapchat por mencionar algunas, alcanzando a diferentes audiencias y siendo estos mensajes vistos por millones de personas en favor del entonces candidato Dondald Trump. Por lo cual esto infiere una clara influencia a la virtual victoria del candidato republicano. De acuerdo a información del periódico "El Diario" en su versión digital se ejemplificaron como el uso de estas herramientas en las diferentes plataformas, *Cambridge Analytca* confirmó al menos el convencimiento de más de 35 mil usuarios por el candidato promocionado (The Guardian, 23 de marzo de 2018).

Marck Zuckerberg creador de Facebook, plataforma donde se obtuvo la mayor parte de la información de los usuarios, se vio obligados a comparecer en el Congreso de Estados Unidos, en donde este asume el error en su plataforma sobre la carencia de la protección de datos y la privacidad de sus usuarios, que en lo personal sostengo son el principal activo de este tipo de empresas. El propietario de Facebook aseguró que Rusia es una clara amenaza para su empresa ya que sugirió que no duda haya existido intervención rusa en su plataforma (El País 11 de abril de 2018).

Rusia y las Elecciones en Estados Unidos 2016.

Este tema por si solo sugiere ser la continuación de este trabajo de investigación, de antemano polémico e importante para la vulnerabilidad de los sistemas de las democracias en la actualidad, este acontecimiento será analizado en forma en el capítulo siguiente, en este apartado me limitaré a describir dicho acontecimiento y destacar lo más relevante de este, ya que se encuentra fuera de los alcances de esta investigación.

De acuerdo a la NSA y a la CIA, la elección en 2016 para presidente en los Estados Unidos, fue saboteada por hackers rusos quienes intervinieron difundiendo mensajes al electorado a favor del actual presidente estadounidense, empleando plataformas como

Facebook la cual después de este incidente enfrentará un problema de nuevo con la forma en la que la propaganda política no puede ser controlada en esta red social, las *fake news* serán parte de la era de la post verdad. La influencia de mensajes patrocinadas por Rusia supone la ilegitimidad en una elección y un problema más a la democracia digital.

En un reporte de ambas agencias mencionadas se estableció que, con base en las investigaciones de los servicios de inteligencia, durante el periodo de campañas el cual dio inicio a finales del año 2015 y culminaron en el proceso de elección el 8 de noviembre de 2016 se presentaron diferentes incidentes en el ciberespacio en los cuales en diferentes redes sociales, como Facebook, twitter, Instagram y Reddit fueron vulneradas y se acusa a hackers rusos de promover ideas a favor de Donal Trump, el documento señala de forma textual que existen elementos clasificados que comprueban la participación del Presidente Ruso Vladimir Putin para evitar que Hillary Clinton alcanzara la presidencia lo cual supondría un problema para los intereses Rusos. (Office of the Director of National Intelligence, 2017 p. 7)

Además, el Departamento de Inteligencia Nacional estadounidense propone que el escandalo destapado del *Panama Papers* en 2016, en donde Rusia y varios países y personajes políticos se vieron involucrados, en la evasión fiscal y se expusieron la cuenta bancaria personal de estos, lo cual fue un duro golpe para el presidente ruso el cual acusó enérgicamente a la CIA de operar en contra de sus principales enemigos políticos para desestabilizarlos filtrando más de 2.6 terabytes de reportes financieros (Blum, Obermaier, Obermayer, 2016, p.1).

Con base en este acontecimiento el DNI asegura que la intervención rusa fue parte de la venganza de Putin por la filtración de información meses antes de la elección, además que Hillary Clinton candidata demócrata en 2011 y 2012 promovió revueltas en contra del régimen en Rusia, por lo cual si esta hubiese llegado a ganar pondría en riesgo la estabilidad en Moscú y diezmaría los intereses del kremlin en la escena internacional. Así mismo se establece que el apoyo a Trump fortalecería la figura de Rusia en Occidente (Office of the Director of National Intelligence, 2017 p. 12).

En el documento desclasificado se expresan y detallan las supuestas operaciones de ciber espionaje proveniente de Rusia, las agencias de inteligencia estadounidenses identificaron que también las filtraciones de los correos de Hillary Clinton en la recta final

de la campaña, comprometiendo la figura de la ex candidata, con un tema de Pedofilia de uno de los colaboradores más cercanos como Jhon Podesta, donde temas delicados inundaron la opinión pública durante el proceso, así mismo en estos mails se describen las aspiraciones de Hillary Clinton en temas de comercio internacional, . Una filtración que termino por desgastar la campaña de Clinton, la cual fue revelada por *Wikileaks.* Motivo por el cual se ha sugerido en diferentes medios que dicha plataforma pertenece a los servicios de inteligencia rusos (El Economista, 13 abril 2017).

También se dará continuidad al dilema del sacrificio de la privacidad para garantizar la seguridad, así también se explicará la venta de información personal como un activo para el nuevo sistema empresarial y político, señalando las formas en que las grandes firmas de hoy en día, ven en el individuo una producto o mercancía que está a la venta al mejor postor para fines de marketing político.

La información dirigida hacia un sector específico de la población puede influir y determinar el futuro de una nación, como lo fue en el caso de los Estados Unidos en 2016 en la elección del actual presidente, en donde los servicios de inteligencia de Estados Unidos aseguran hubo intervención rusa para influir en la decisión del electorado, cada uno de estos temas se explicará de forma breve dado a que estos merecen una investigación un cuanto más exhaustiva y que amerita darle seguimiento.

# CONCLUSIONES

Con base en lo expuesto a lo largo de la tesis, resulta importante identificar que parte de la doctrina propuesta en la teoría del colapso de algún modo se encuentra vigente con las advertencias expuestas desde 2003, así mismo es notable que el actuar estadounidense durante dicha administración se ha mantenido cauteloso, aunque sin mucho éxito en la defensa de las vulnerabilidades que le representa el ciberespacio y más por el último caso señalado.

Dentro del ciberespacio, las relaciones de poder se mantienen presentes, pese a no existir propiamente una zona de influencia determinada dentro de este espacio, esta misma se configura de acuerdo a la escena internacional física la cual es determinante para comprender de la dinámica dentro de este nuevo espacio. Adversarios políticos han tenido la oportunidad de influir hasta en el proceso democrático. Lo cual es alarmante.

Estados Unidos como se ha mencionado ha mantenido un gran despliegue en relación a la defensa de sus instituciones y su seguridad nacional, al ser una de las potencias tecnológicas ha podido desarrollar una gran capacidad tecnológica y militar que le permiten garantizar la seguridad nacional ante cualquier amenaza.

Para Estados Unidos, la Internet se ha convertido en un elemento clave del desarrollo económico y tecnológico que han tenido en estas últimas décadas, al ser una potencia tecnológica se ha creado una dependencia indivisible entre su desarrollo y crecimiento tecnológico con las constantes amenazas que atentan contra su seguridad, ahí recae la importancia de la urgencia en normar lo que ocurre en el ciberespacio.

Las relaciones de poder gestadas presentes en el mundo virtual son determinadas con la dinámica de poder que se conoce en el mundo físico, siendo el mundo virtual un espacio más para dominar o ser dominado, es claro que la figura del Estado es el blanco de ataque desde diferentes flancos y por diferentes actores desde cualquier parte del mundo en cualquier momento.

La naturaleza hostil y anárquica del sistema internacional, obliga al Estado a sobrevivir, El Ciberespacio es una nueva realidad que influirá en las relaciones de poder dentro del escenario internacional, así mismo el aspecto no regulado de forma clara y funcional, es un reflejo del propio sistema internacional.

Estados Unidos tiene clara esta idea, la creación de un ciber-ejército ha sido una necesidad dada las condiciones de este nuevo espacio, por otra parte, el dominio de este espacio representa de forma clara la capacidad de poder de un Estado, la disputa por este espacio se limita a la capacidad militar y económica del Estado.

La administración de Obama ha sido la que implementó y desarrolló un mayor número de políticas internas a favor de la ciber-seguridad, con el fin de proteger a las estructuras críticas que sugiere la teoría del caos, y así aumentando notoriamente su ciber-ejercito. El incremento en la capacidad militar deviene como réplica a las filtraciones y la amenaza al status quo ha representado la incursión de nuevos actores como Julian Assange con *wikileaks.*

Poco efectivas las medidas adoptadas por la administración de Obama, ya que la mayor parte de los conflictos que ha atravesado el Estado norteamericano provienen de forma interna, siendo miembros del mismo ejército y de las propias agencias de seguridad nacional quienes han atentado contra la hegemonía de este país, por mencionar las sufridas durante la administración, aunque a finales de esta el escándalo de la intervención de Rusia en las elecciones ha superado a las dos anteriores.

La idea y la percepción de la gravedad, así como la trascendencia que pudiera representar un conflicto en el ciberespacio de acuerdo a mi estudio, es falso ya que partiendo de las políticas establecidas en el periodo de la administración de Obama no ha ocurrido un enfrentamiento de forma directa que atente de manera grave la soberanía o la supervivencia del Estado, si bien han ocurrido sucesos de mediana trascendencia ninguno ha representado una amenaza real para el Estado.

La teoría del colapso ha sido la base de dichas políticas, aunque alarmista, dado a que nada de lo propuesto sobre el daño a las estructuras críticas o el sabotaje a en operaciones militares, ha sido la impulsora del desarrollo tecnológico de las potencias y la promoción de un sistema de seguridad tanto nacional como internacional para salvaguardar la seguridad en el ciberespacio.

Para Estados Unidos es prioridad desarrollar medidas y mejorar la capacidad del Estado en reducir el riesgo potencial de estas amenazas se propone y busca que tanto la población como el aparato gubernamental y el sector privado adopten una cultura de ciber-seguridad de una navegación segura en la cual no se comprometa la competencia económica

(robo de información industrial) la violación de la privacidad y las libertades de los ciudadanos así como proteger información gubernamental y militar que comprometa la seguridad nacional.

Este trabajo inició presentando la propuesta de que durante la administración de Obama y el proceso de militarización del ciberespacio, así como las medidas en materia de ciber seguridad desarrolladas por el aparato gubernamental, así como las políticas establecidas y aprobadas por el congreso mantenían como propósito establecer estrategias militares y de inteligencia como condición para el mantenimiento del poder militar global.

La hipótesis no es claramente comprobable durante el periodo en el que Obama fue presidente, si bien en al menos dos ocasiones Estados Unidos enfrentó la filtración de información sensible, bajo los servicios de contra inteligencia fue posible mantener un control de los daños, pero en vísperas del final de la administración se han venido enfrentando con temas cada vez más delicados de las amenazas provenientes del ciberespacio.

Actualmente este proceso tecnológico se mantiene, los ciber comandos han aumentado en número, así como las divisiones de inteligencia encargadas de la seguridad en el ciberespacio, además existen nuevas estrategias para evitar el riesgo potencial que representan las amenazas en el ciberespacio.

Considero importante darle seguimiento, a este nuevo espacio de las relaciones internacionales, el desarrollo tecnológico es importante para la configuración del escenario internacional, siendo parte intrínseca de la forma en la que ya comprendemos el mundo.
Por lo tanto, en torno a los elementos presentados por el gobierno estadounidense se obedecen a la legitimación de su actuar y sus medidas en torno a la ciber-seguridad; en esta investigación se descubre la urgencia de ese gobierno por acelerar el proceso de militarización en el ciberespacio, además de que evidencia, como que este nuevo entorno virtual será objeto de muchos estudios como lo ha venido siendo en estos últimos años,

En los 5 años que duró esta investigación, tuve la oportunidad de presenciar y seguir de cerca todo lo relacionado el con este nuevo campo de estudio para las relaciones internacionales, como parte de la disciplina el enfoque que te ofrece este nuevo entorno es por mucho enriquecedor ya que complementa el contexto actual en el que se desarrollan los diferentes acontecimientos de la escena internacional.

# REFERENCIAS


Álvarez, L. (2017*). Ciber Ataques, Antesala de la Guerra Hibrida*. Artículo en línea recuperado y consultado el 01 de Agosto de 2018 en: http://www.expansion.com/actualidadeconomica/analisis/2017/09/07/59b0245646163fdf1b8b457a.html

Álvarez, R. (2013). El caso Snowden y la Democracia en Disputa. En *Nueva Sociedad,* (247) pp. 27-35

Arenal, C. (1990). *Introducción a las Relaciones Internacionales*. Madrid: Ed. Tecnos.

Banerja, A. (2018). NotPetya: How a Russian malware created the world's worst cyberattack ever. Articulo en línea recuperado de: https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html

Barns, J. y Gibbons, E. ( 22 de Junio de 2019). U.S. Carried Out Cyberattacks on Iran. *The New York Times.* Recuperado de https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html

Beaumont, L. (30 de Septiembre de 2010). *Stuxnet worm heralds new era of global cyberwar, The Guardian*. Recuperado de http://www.TheGuardian.com

Billo, C. (2017). *Cyber Warfare An Analysis Of The Means and Motivations Of Selected Nation States*. Estados Unidos, Institute for Security and technology studies At Durmouth College.

Blum P. Obermaier F. y Obermayer B. (2016). *Putin´s Rich Friends.* Articulo en línea consultado y recuperado y consultado el 12 de Agosto de 2018 en: https://panamapapers.sueddeutsche.de/articles/56fec05fa1bb8d3c3495adf8/

Bonifaz R. (2017). *La NSA Según Filtraciones de Snowden*. Buenos Aires: Universidad de Buenos Aires Argentina.

Buzai G. (2012). *EL Ciberespacio desde la Geografía. Nuevos espacios de vigilancia y control global. Revista Meridiano*, (1), pp.266-276.

Carbonell J. (2014). *El Acceso a Internet Como Derecho Humano*. México: Biblioteca Jurídica Virtual del Instituto de Investigación Jurídica de la UNAM.

Caro, J. (2013). *Algunas Reflexiones Sobre la Ciberguerra.* España: Instituto Español de Estudios Estratégicos.

Carrol, W. (2008). *Cyber War 2.0 — Russia v. Georgia.* Artículo en Línea recuperado el 13 de 08 de 2014 Obtenido en http://www.defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/

Casar, J (Ed). (2012). *El Ciberespacio Nuevo Escenario de Confrontación.* Madrid, España, Centro Superior de Estudios de la Defensa Nacional. Editorial Ministerio de Defensa.

Clarke, R., y Kananke, R. (2010). *The Next Thhreat to National Security and What to Do About it*. Estados Unidos: Harper Collins Ebooks.

Clausewitz, K. (2008). *De la Guerra*. Terramar Ediciones.

S/A (16 de agosto de 2018). Julian Assange Cumple seis años en la embajada de Ecuador en Londres. *Cuba Debate.* Artículo en línea recuperado el 16 de Agosto de 2018 en: http://www.cubadebate.cu/noticias/2018/08/16/julian-assange-cumple-seis-anos-en-la-embajada-de-ecuador-en-londres/#.W39OJbiQwdV

Cymerman. H. (28 de septiembre de 2010). Irán sufre el mayor ataque cibernético de su historia. *La Vanguarida*. Recuperado de http://www.lavanguardia.com

Deibert, R. (2015). *The Geopolitics of Cyberspace After Snowden.* Current History. Vol. 768 (114). Filadelfia, Estados Unidos. pp. 9-15.

Delicia, M. (2002). *La Guerra Fría desde la óptica de las Relaciones Internacionales.* La Plata, Argentina: Universidad Nacional de La Plata.

Derek, G. (2011). The Everywhere War. En *The Geographical Journal* Vol. 177 (3). p.238-250.

Dietz, E. (Ed) (2012). *Applaying Traditional Military Principles to the Cyber Warfare.* NATO.

Donelly, R. (2000). *Realism and International Relations.* Cambridge. Reino Unido: Cambridge University Press.

Dougherty J. y Pfaltzgraff R. (1993). *Teorías en Pugna en Las Relaciones Internacionales.* Buenos Aires; Argentina: Grupo Editor Latinoamericano.

Dunne Timothy. (2001). *Realism; en John Baylis, Steve Smith, The Globalization of world politics: an introduction to international.* Oxford University Press.

Ehrami, T. (2013). *Reaching the tipping point of force in counter proliferation: Exploring conditions leading to the Israeli pre-emptive use of force in Osirak (Iraq) and Al-Kibar,(Syria) and its implications for Iran*. Países Bajos: Leiden University.

Einhorn, M. (2003). *Copyright, Prevention, And Rational Governance: File-Sharing And Napster*. New York: Columbia University.

*El Economista* (13 de Abril de 2017). "Wikileaks es un "Servicios de Inteligencia Hostil: CIA". Artículo en línea consultado y recuperado el 02 de mayo de 2018 en: https://www.eleconomista.com.mx/internacionales/WikiLeaks-es-un-servicio-de-inteligencia-hostil-CIA--20170413-0001.html

*El Mundo* (09 de Junio de 2011). "Naciones Unidas declara el acceso a Internet como un derecho humano". Artículo en línea Consultado el 26 de Agosto de 2012, Recuperado de http://www.elmundo.es/elmundo/2011/06/09/navegante/1307619252.html pág. 1.

*El País* (11 de Abril de 2018). "Las ocho cuestiones más difíciles que tuvo que Contestar Zuckerberg en el congreso de los EE.UU". Recuperado el 12 de Agosto de 2018 de : https://elpais.com/internacional/2018/04/11/actualidad/1523434511_157267.html?rel=str_articulo#1534383214762

Ernest y Young (2017). *"*WannaCry" Ransomware Attack*"*. Artículo en línea recuperado de: https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/$File/ey-wannacry-ransomware-attack.pdf

ESET. (2010). *Stuxnet Under the Microscope*. Informe Recuperado el 29 de Agosto de 2016: https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf

Espinoza, A. (28 de septiembre de 2010). "Irán sufre un ataque informático contra sus instalaciones nucleares". *El País*, Recuperado de http://www.Elpais.com

Foguel, J. (2007). "Veinte apuntes sobre el ciber leviatan". *Letras Libres*, 08-12.

Follat E. y H. Stark. (2009). *How Israel Destroyed Syria's Al Kibar Nuclear Reactor.* Artículo en línea recuperado el 28 de agosto de 2016 en http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

Foncillas, A. (2013, 15 de Abril). *La Guerra Fría digital EU-China.* Proceso. Artículo en línea recuperado el 17 de Agosto de 2015 obtenido en http://www.proceso.com.mx/338497/la-guerra-fria-digital-eu-china

Foucaul, M. (2006). *Seguridad, territorio, población. Curso en el Collège de France: 1977-1978*. Buenos Aires: Fondo de Cultura Económica.

Germain M. (2008). *The Art Of Cyber Warfare*. Artículo en línea recuperado el 08 de Noviembre de 2013 en http://www.technewsworld.com/story/62779.html

Gibbs S. y Halliday J. (13 Septiembre 2013). *North Korean hackers suspected of cyber-espionage attack on South*. The Guardian. Recuperado el 30 de Julio de 2018 de: https://www.theguardian.com/technology/2013/sep/11/north-korean-hackers-cyber-espionage

Harán J.(2018). "*Malware de la década del 2010: recordando a Petya y WannaCry"*. Recuperado de: https://www.welivesecurity.com/la-es/2018/11/26/malware-de-la-decada-del-2010-recordando-petya-y-wannacry/

Hassan, J. (2009). "*Cyber warfare", the truth in a real case*. Suiza: Linköping Universitetet.

Hay N. (2019). *The Worst Cybersecurity Breaches of 2018 So Far.* Recuperado de: https://www.wired.com/story/2018-worst-hacks-so-far/

Hollis D. (2011). *Cyber War Case Study: Georgia 2008. Small Wars Journal*. Articulo en línea recuperado de: www.smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Huichalaf P. (2012). *Minuta explicativa sobre Proyectos de ley SOPA y PIPA de EEUU y sus posibles efectos jurídicos en Chile*. Artículo en línea recuperado el 15 de Junio de 2015 Obtenido de http://www.culturadigital.cl

Infosec (2011, 22 Julio). *AnonyLulzyAntiSec: What Have You Done for Us Lately?* Artículo en línea Recuperado en: http://www.infosecisland.com/blogview/15379-AnonyLulzyAntiSec-What-Have-You-Done-for-Us-Lately.html

Jordan T. (1999). *Cyberpower: The Culture and politics of cyberespace and the internet;* Londres, Inglaterra: Routledge.

Keohane R. (1983). *After Hegemony Coopartion and Discord In The World Political Economy.* New Jersey, Estados Unidos: Princeton University

Krepinevich, A. (2012). *Cyberwarfare: A Nuclear Option*. Estados Unidos: Center for strategic and Budgettary Assesments.

La Nación (05 de septiembre de 2007). "Tensión Por El Ciber-Ataque Al Pentágono". Artículo en línea recuperado el 04 de Agosto de 2018 en: https://www.lanacion.com.ar/940981-tension-por-el-ciberataque-al-pentagono

Laswell, H. y Kaplan, A. (1950). *Power and Society: a Framework for political inquiry.* Connectitut, Estados Unidos: Yale University.

Lessing, L. (1998). *Las Leyes del Ciberespacio. Taiwan Net '98*, pp. 171-179. Taipei.

Lewis, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Washington D.C., Estados unidos.: Center for Strategic and International Studies.

Lewis, J. (2010). *Thresholds for Cyberwar*. Estados Unidos: Center for Strategic and International Studies.

Llongueras, A. (2010). *Moonlight Maze. The beginning of a new era*. Obtenido de http://www.academia.edu/6182336/MOONLIGHT_MAZE._The_beginning_of_a_new_era

Maness, C., y Valeriano, B. (2013). *What Do We Know about Cyber Conflict? Scope, Impact, and Restraint in Cyberspace*. Estados Unidos: University of Glasgow y University of Illinois.

Mataf.net (2018). *Casa de Cambio de Divisas por Internet.* Recuperado en: https://www.mataf.net/es/cambio/divisas-BTC-MXN

Mcevoy, M. (2010). *From Global Village to Virtual Battlespace The Colonizing of the Internet and the Extension of Realpolitik*. International Studies Quarterly, 381-401.

Mehan, J. (2012). *Are We Really in a Cyberwar? The Danger of Hype*. Estados Unidos: School Of cyber security Lunar Line.

Mora, E. (2016). *Monedas Virtuales Se Suman al Comercio Electrónico*. Universidad Militar Nueva granada. Bogotá, Colombia.

Morgenthau, H. (1986). *Política Entre las Naciones: La Lucha por el Poder y la Paz.* Sexta Edición. Grupo Editor Latinoamericano.

Navalon, R. G. (2012). *El vacío legal del ciberespacio*. *Revista de Aeronáutica y Astronáutica*, p. 849.

Office of The Director of National Inteligence. (2018.

Oro, L. (2009). *En torno a la Noción de Realismo Político;* Revista Enfoques, Vol. VII (10), pp.15-46.

Palacio, V. (2003). *La Imagen Imperial del Nuevo Orden Internacional ¿Es esto realismo político?* Revista CIDOB d´Afers Internacionals, (64), pp. 7-28.

Pascual G. A. (2005). *La Doctrina Bush del Ataque Preventivo.* Universidad Autónoma Metropolita, México: El nuevo Milenio Mexicano PP.74-84.

Petrollini D. (2012). *Realismo Ofensivo y Realismo defensivo: El Debate Realista.* Buenos Aires, Argentina: Centro Argentino de Estudios Internacionales.

Pratt M. (2003). *Asalto Rápido Ataque Preventivo: El Teatro Domestico de la Guerra y las Nuevas Disidencias. Nueva Sociedad, 185* p. 122.

Rabinad, M. G. (2008). La Soberanía del Ciberespacio Algunas reflexiones sobre el concepto de Estado, soberanía y jurisdicción frente a la problemática que presenta el internet. *Lecciones y Ensayos*, (85), pp.85-107.

Reguera, J. (18 de mayo de 2015). *Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario*. Obtenido de Grupo de Estudio de Seguridad Internacional Recuperado de: http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario: 1

Rid, T. (2005). *At The Abyss: an Insider of Cold war*. Estados Unidos. Presidio Press.

Rid, T. (2012). *Cyber War Will Not Take Place.* Journal of Strategic Studies, pp.5-32.

Salomón, M. (2001). La teoría de las Relaciones Internacionales en los Albores del siglo XXI: dialogo, disidencia, aproximaciones*; Revista CIDOB d Afers Internacionals*, (56). pp.7-52.

Sellers L. y Shaw E. (2015). *Aplication of The Critical-Path Metod to Evaluate Insider Risks. Studies International Security.* Studies in Intelligence Vol. 59 (2) pp. 1-8.

Stone M. (2010). *Obama´s Cybersecurity Plan*. New York, Estados Unidos. Columbia University, pp. 1-8

Strinde G. (2011) *Cyberwarfare: Connecting Classical Security Theory to a new Security Domain.* Suecia: Lund University

Sulmeyer M. (2018). *How the U.S. Can Play Cyber-Offense Deterrence Isn't Enough.* Revista Foreing Affairs Vol. 97 (2) p. 1

Symantec. (02 de 2011). *W32 Stuxnet Dossier Symantec*. Recuperado el 15 de mayo de 2016 en: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

The Departament of Defense (2015). *Cyber Strategy. The Secretary of Defense*, Washington DC, Estados Unidos.

The Guardian (23 de marzo de 2018). *Un Documento de Cambridge Analytica Revela la Estrategia de la Empresa de Trump para Conseguir la Victoria.* Recuperado el 16 de Agosto de 2018: https://www.eldiario.es/theguardian/documento-Cambridge-Analytica-estrategia-Trump_0_753125564.html

The Sec Dev Group of University of Toronto. (29 de 03 de 2009). *Tracking Ghostnet: Investigating a Cyber Spionage* Network. Artículo en Línea Obtenido en: https://www.nsi.org/pdf/reports/Cyber%20Espionage%20Network.pdf

The White House (2009). Cybersecurity Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington, Estados Unidos. pp.01-12

U.S. Copyright Office. (1998). *The Digital Milennium Copyright Act of 1998*. Obtenido de http://www.copyright.gov/legislation/dmca.pdf

Van M. (2013). *Myth Paradox and the obligation of leadership: Edward Snowden, Bradley Manning, And The Next Leak*. Center of Security Policy. Washington, Estados Unidos. P. 23-39.

Varcelli A. (2004). *La Conquista Silenciosa del Ciberespacio.* Buenos Aires Argentina: Creative Commons.

Waltz K. (2000). Structural Realism After The Cold War. *International Security* Vol. 25 (1), pp.5-41. Recuperado de http://www.jstor.org/stable/2626772?origin=JSTOR-pdf

Weber M. (2005). *El Político y el Científico.* Argentina: Alianza Editorial.