UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

La filtración de información en la guerra cibernética estadounidense (2006-2016)

TESIS

QUE PARA OBTENER EL TÍTULO DE

LICENCIADA EN RELACIONES INTERNACIONALES

PRESENTA:

ROSA LUZ FLORES PADILLA

ASESOR: HALYVE HERNANDEZ ASCENCIO

Santa Cruz Acatlán, Naucalpan, Estado de México, 2019

AGRADECIMIENTOS

A mis padres, quiero dedicarles esta tesis, ya que sin sus palabras de aliento y todo lo que nos brindaron a mis hermanas y a mí, en todos los aspectos, habría sido mucho más difícil llevar a cabo este logro en mi camino. Gracias por ser siempre mi luz, mi guía y mi apoyo. Sé que están orgullosos de mí y eso me llena de felicidad; en verdad espero seguir dándoles lo mejor de mí, lo tienen bien merecido por el gran trabajo que han hecho conmigo.

A mis hermanas, porque no encuentro palabras para agradecerles por todos los momentos que hemos pasado juntas, por todo lo que me han enseñado, todas las pláticas, las risas, las caídas y cómo siempre nos ayudamos a levantarnos en esos momentos difíciles. Las amo demasiado y mucho de lo que soy, es gracias a lo que he vivido con ustedes.

A mis tías, tíos y primos, por estar siempre ahí como mis segundos padres y hermanos, apoyándome y echándome porras para conseguir mis metas, por alimentar mi alma con momentos divertidos, así como con su apoyo y consejos en los momentos más oportunos.

A Rodrigo, porque tú me has impulsado estos últimos años a ser mejor cada día, a nunca dejarme de lado ni olvidar mis sueños y lo que quiero lograr. No sé qué nos depare el destino, pero agradezco infinitamente que hayas llegado a mi vida.

A Halyve, porque más que mi asesor y profesor, eres un gran amigo para mí. He aprendido mucho de ti y te tengo un enorme respeto y cariño. Gracias por aguantarme y tenerme paciencia en todo el proceso de mi tesis y por todo lo que me has enseñado sobre la vida, incluso fuera del salón de clases.

A mis amigos, los de verdad, porque no me han abandonado a lo largo de todos estos años, han estado a mi lado en las buenas y en las malas, han sido mi apoyo

incondicional cuando en verdad lo necesito. En especial, a Marlén, Gustavo, Susan, Andy, Jessi... Ustedes son la familia que escogí y simplemente no hay palabras para agradecerles y explicarles lo que significan para mí. Pero espero que todo lo que hemos pasado juntos, les haga ver lo mucho que los quiero.

Finalmente, no quiero olvidar a Dios que, aunque no sea la más devota y practicante de sus hijas, sé que nunca se ha olvidado de mí, me ha mandado muy buenas batallas y agradezco todo lo que he aprendido de cada una de ellas. De igual manera, le mando mi infinito amor y agradecimiento a los angelitos que tengo cuidándome en el cielo: mi abuelita Emma, que fue simplemente la persona más maravillosa que conocí en esta Tierra; a mis abuelitos Ramón y Antonio; a mis tíos abuelos Pepe y Ofe; a mis tíos Toñito y Pepito y a mi pequeña Charlotte, quien tantas veces se aparecía en mi cuarto mientras yo estaba haciendo este trabajo y aunque estaba tan tierna y me daban unas ganas inmensas de jugar con ella, trataba de contenerme y simplemente se quedaba ahí, haciéndome compañía, le agradezco también porque finalmente la tengo para que me ayude a cruzar al Mictlán cuando el momento llegue.

Título: La Filtración de información en la Guerra Cibernética estadounidense (2006-2016)

Capítulo 1
Marco teórico-conceptual

Capítulo 2
El mundo cibernético

Capítulo 3
La Guerra Cibernética en Estados Unidos

Capítulo 4
La filtración de información y sus implicaciones en la Guerra Cibernética de Estados Unidos

Introducción.

La presente investigación tiene como objetivo principal – bajo una metodología de tesis analítica-explicativa – dar a conocer el conflicto de la filtración de información dentro del fenómeno de la guerra cibernética estadounidense, lo cual ha comprometido diplomática y socialmente a dicha nación en casi todos los niveles del gobierno, así como respecto al deterioro dentro de la Opinión Pública, considerando la siguiente pregunta de investigación: ¿En qué medida el Internet puede ser una herramienta o un enemigo para los gobiernos y la sociedad internacional?

Esto tomando en cuenta la hipótesis de que el poder del internet en las Relaciones Internacionales está poniendo en tela de juicio el control que el Estado y los Servicios de Inteligencia pueden tener en la Política Exterior de un país. De esta manera, tomaremos el caso de los Estados Unidos durante el periodo 2006-2016, desde que aparecieron las primeras filtraciones de WikiLeaks hasta el final del periodo presidencial de Barack Obama; para así emprender una aproximación al tema, en un país donde esta situación es más frecuente de lo que imaginamos y que, desde entonces a la fecha, ha generado en la sociedad internacional una gran incertidumbre y todo tipo de cuestionamientos. Por mi parte, estos giran en torno a un posible nuevo orden mundial en el que pueda suceder lo siguiente: 1) que Estados Unidos posiblemente ya no sea la potencia mundial que ha sido en los últimos años; 2) que ya no se le encuentre dentro de las potencias más importantes del mundo; o bien, 3) que siga siendo un país poderoso, pero más autoritario y cada vez menos “promotor de las libertades civiles”, tanto internamente como al exterior.

Respecto a mi interés personal en el desarrollo del tema en cuestión, lo considero pertinente puesto que, al incluir como actor internacional al Internet y en general a

todo lo que deriva del mismo, estamos presenciando cómo el Estado va perdiendo poder e influencia, no solo dentro de sus límites, sino internacionalmente. Esto ya que al tratarse de una herramienta que permite conocer los eventos que ocurren todos los días de manera instantánea, se pierde poco a poco la oportunidad de analizar la situación y dar una respuesta oportuna por parte de los altos mandos de cada país.

De igual manera, debo aceptar que también tengo cierto interés personal por este tipo de temas desde que hace algunos años leí *1984* de George Orwell y, a decir verdad, no es mi deseo arruinarle la trama de la historia a quien aún no lo haya leído o se encuentre en proceso de hacerlo, pero simplemente diré que es un excelente libro y que fungió como una de las inspiraciones principales para esta tesis.

Antes que nada, es importante mencionar que la sociedad internacional se encuentra en un proceso de cambios vertiginosos, bruscos y que se dan con mayor rapidez de la que uno se puede imaginar. Esto ocasionado en gran medida por los constantes avances tecnológicos que permiten a toda la población estar "conectada" y comunicarse con gente de cualquier punto del planeta de manera inmediata. Cabe mencionar que el tener la posibilidad de saber todo acontecimiento que ocurre en el mundo en cuestión de segundos, puede ser beneficioso para nosotros pero no lo es tanto para los gobiernos, menos aún para los más represivos como las dictaduras o los países bélicos.

En el primer capítulo, cuyo objetivo particular es explicar el panorama general de la temática abordada, así como la teoría y los términos utilizados a lo largo del escrito, daré a conocer los elementos principales que se deben manejar para su debida comprensión, tales como el espionaje, la guerra cibernética o la seguridad nacional.

De igual manera, se explica la teoría de las relaciones internacionales que servirá de base para nuestro análisis: el neorrealismo estructural. Dicha teoría es una derivación del realismo político o *Realpolitik*, el cual deja de lado las doctrinas idealistas del periodo de entreguerras para así comprender mejor el actuar de las naciones considerando que más bien velan siempre por sus propios intereses. No obstante, lo rescatable del neorrealismo estructural es que permite la entrada de más elementos al análisis aparte del Estado, tales como el Internet, los medios de comunicación, los hackers, los *whistleblowers* (delatadores o reveladores de secretos) y los grupos de apoyo a los mismos.

Posteriormente, en el segundo capítulo, en el cual se tiene como objetivo el de introducir al lector en varios temas referentes al mundo cibernético y cómo este influye en la política mundial; se explica cómo el uso del internet ha modificado los paradigmas en la sociedad internacional pues existen ejemplos en los que tanto los movimientos sociales como las modificaciones a Constituciones o la convocatoria a elecciones en ciertos países tienen la posibilidad de ser orquestadas u organizadas en línea. De igual manera, se explica cómo el papel del Estado también se ha modificado a raíz de estos acontecimientos y se comienza a esbozar la clase de control que pretenden mantener ante la situación.

Más adelante, en el tercer capítulo, la propuesta es analizar algunos de los conflictos cibernéticos de los últimos años, explicar brevemente la guerra cibernética, así como la respuesta del gobierno de Obama ante la situación. De igual manera, se muestran algunos de los puntos más álgidos en el globo donde este tipo de conflictos han tenido mayor fuerza, así como un enfoque al papel o comportamiento que Estados Unidos ha manejado a partir de que los mismos comenzaron a presentarse.

Finalmente, llegamos al capítulo cuarto, en el cual se expone la relación de los personajes que han filtrado la información política de Estados Unidos, así como los intereses que se han visto afectados con ello para así cumplir con el objetivo de comprender el conflicto desde sus inicios y analizar cómo esta situación ha afectado a las relaciones diplomáticas y gubernamentales de Estados Unidos. En este capítulo, se muestran las principales actividades que los reveladores de secretos del gobierno o *whistleblowers* más importantes e influyentes han realizado para hacer llegar el mensaje a todos los puntos del planeta respecto a la libertad de expresión y el flujo libre de la información, sobre todo aquella que realmente afecta a los ciudadanos de todo el mundo como lo son:

1. Lo que pasa detrás de las puertas o muros que los gobernantes y diplomáticos han construido alrededor suyo en aspectos tan graves como el asesinato de personas completamente inocentes en los conflictos armados, por ejemplo. Esto gracias a Julian Assange, a su página *WikiLeaks* y a la información que el soldado Bradley (ahora Chelsea) Manning le hizo llegar.

2. Los programas de vigilancia masiva que el gobierno estadounidense (junto con sus aliados) mantiene gracias a sus agencias de inteligencia y seguridad y a los acuerdos que estas tienen con las principales empresas de telecomunicaciones. Esto gracias a lo revelado por el ex analista de la NSA, Edward Snowden.

Asimismo, resulta importante mencionar que Estados Unidos utilizó el argumento de los ataques del 9/11 y la guerra contra el terrorismo que comenzó a partir de entonces, para justificar sus actividades de vigilancia masiva, pero ¿acaso esto les daba autoridad ilimitada para ordenar el espionaje a los estadounidenses y al mundo entero? ¿O esto les daba el poder de perseguir a los que se atreven a delatar sus fechorías?

Estas acciones del gobierno de Estados Unidos, pueden ser resultado más bien de un sentimiento de frustración por estar perdiendo el control ante la situación, o de negación de la realidad actual en la que cualquiera puede quitar el velo de secretismo que por tantos años habían podido mantener. Por lo que puede resultar interesante analizar hasta qué punto los gobiernos en el mundo tratarán de mantener las cosas como están o qué tanta participación le permitirán tener al pueblo para poder decidir el rumbo que tomarán aspectos como la seguridad nacional.

¿Acaso la población del mundo entero va a permitir que sigan existiendo estos abusos del poder, mientras que tantos años de lucha por ser independientes, tener nuestra privacidad y que las autoridades respeten nuestros derechos, quedan en el olvido? ¿O es que en el mundo digital este tipo de atropellos a la libertad de expresión y a la privacidad serán permitidos? ¿Será esta la generación en la que las autoridades necesiten permisos para entrar a tu casa pero no para invadir tu intimidad espiando todas tus actividades en línea?

Capítulo 1
Marco teórico-conceptual

1.1. Teoría del Neorrealismo Estructural
1.2. Guerra Cibernética
1.3. Espionaje y espías
1.4. Seguridad nacional

1.1. Teoría del Neorrealismo Estructural

Como es bien sabido, tras las grandes consecuencias que trajo consigo la Primera Guerra Mundial, como fueron las pérdidas humanas y económicas, así como los cambios ideológicos y políticos, como la caída de casi todos los imperios que aún existían; la comunidad internacional sintió la necesidad de buscar maneras más pacíficas de resolver los conflictos internacionales, por lo que se comenzó el proyecto de la Sociedad de Naciones, de la mano con la teoría idealista de las Relaciones Internacionales, la cual abogaba por las buenas intenciones de los países para con el resto del mundo.

Sin embargo, al fracasar ambas decisiones, pudimos ver que el mundo se vino abajo una vez más, pero esta vez cayendo en un abismo aún más profundo que el anterior, dado que se vivió una Segunda Guerra Mundial, con mayores repercusiones, pérdidas y daños a la humanidad. Al ver que este evento no se pudo evitar con la teoría idealista y las buenas intenciones que tanto defendía, surgió una teoría de las Relaciones Internacionales mucho más afín a la realidad internacional y al comportamiento general de las naciones y sus gobernantes: El Realismo Político, del cual, posteriormente, surgió una variante llamada Neorrealismo estructural, la cual servirá de guía y apoyo para el presente escrito.

Para empezar, tomemos en consideración que en esta tesis se tocará el tema del mundo cibernético enfocado en el espionaje y los movimientos sociales que se han generado a través de las nuevas tecnologías, así como el relativo control que el Estado pretende tener sobre la población en todo el mundo por dichos medios. Es por esto que conviene comenzar con la explicación de ciertos términos como el espionaje y la seguridad nacional.

El espionaje, al ser una de las actividades más practicadas a lo largo de la historia en todo el mundo, constituye un tema crucial para la comprensión de la realidad internacional. Los Estados se han espiado desde hace siglos con el fin de saber qué reacciones están teniendo sus aliados o sus enemigos respecto a las acciones de política exterior implementadas, ya sea para ganar o, en el mejor de los casos, para evitar una guerra. No obstante, esto hizo que - con el paso del tiempo y al aumentar la cantidad de interacciones entre países - la búsqueda de información, el surgimiento de Agencias de Inteligencia y la formación de espías profesionales para la defensa del interés nacional de cada país, fueran también en aumento.

De igual manera, por hacer mención en este trabajo de términos como: Estado, Seguridad Nacional, Interés Nacional, Poder, así como Lucha por el Poder y Equilibrio del mismo; parece que la teoría que más se adecua para hacer el análisis de la problemática planteada es el Realismo Político de Hans Morgenthau. Sin embargo, hay una variante más actualizada de la misma, la cual permite integrar otros elementos o actores al estudio de los casos de Política Internacional además de los Estados: se trata de la teoría del Neorrealismo Estructural, la cual se irá desglosando a lo largo de este capítulo, aunque muy de la mano con la teoría del Realismo Político, al constituir esta su base general.

Ahora bien, comienzo dando una idea general de lo que es la teoría del Realismo Político o *Realpolitik*, para luego adentrarme en su variante actualizada: el Neorrealismo estructural. El Realismo político "parte de la premisa de que el estudio de la sociedad internacional no puede estar basado en saber que las intenciones o buenos deseos de los gobiernos de los Estados nacionales se asumirán éticamente para respetar las normas de convivencia internacional, por lo que es preciso entender la realidad en su exacta dimensión, en la […] de la política."[1] Por lo que, desde un principio, debemos dejar de lado a la teoría idealista, ya que esta expresa que el Estado guía su política exterior confiando en las buenas intenciones de los demás países, lo cual no se ha dado nunca en el mundo que habitamos.

Hay quienes encuentran el origen de esta teoría en Maquiavelo y su obra más famosa *El Príncipe* ya que en esta establece que el hombre y sobre todo los gobernantes son seres egoístas que buscan sólo satisfacer sus deseos, lo cual obtienen a través del poder; e igualmente sienta las bases para mantener el mismo al decir que "el príncipe virtuoso precisa de guías en las que pueda orientarse para conservar el poder del Estado en sus óptimas condiciones, las que suponen un conjunto de razones y exigencias que debe llevar a cabo tras interpretar cuál es la más adecuada"[2]. De aquí surge también el término de Razón de Estado, la cual permite lograr los objetivos y sobre todo justificar los medios que se utilizan para ello. Así, la Razón de Estado "se convierte en el fin último del mecanismo que se debe de seguir para alcanzar el mantenimiento del Estado."[3] Sin Razón de Estado, no hay bases para que el mismo pueda justificar sus acciones, las cuales en su mayoría pueden parecer injustas para el pueblo.

[1] Gutiérrez Pantoja, Gabriel. *Teoría de las Relaciones Internacionales*. Oxford University Press-HARLA México S.A. de C.V., México, D.F., 1997, p 195
[2] *Ibídem*. p 196
[3] *Idem*

De igual manera, se nos expone la siguiente idea: “el que una política sea cruel o injusta, debe ser indiferente para lograr el objetivo, aunque, como se da perfecta cuenta de lo que hace, se sabe que ello puede influir o no en su éxito”[4]. Aquí vemos cómo la falta de humanidad, tacto o algún tipo de consideración por parte de la mayoría de los dirigentes de un Estado se ve como algo completamente normal e incluso quizá necesario dentro de las cualidades que cualquier líder debe poseer, ya que de otra manera, se dificultaría el logro de todos los objetivos deseados por el Estado y como hay que ver siempre antes por el interés nacional, cualquier acción que pudiera tacharse de incorrecta puede ser aceptada siempre y cuando tenga como fin el cumplimiento de lo que el Estado se propone.

Ahora bien, no podemos ignorar el hecho de que el gobierno estadounidense vela únicamente por sus intereses y desde que existe como país independiente ha hecho lo necesario para adelantarse a los hechos, conocer los puntos de vista de aquellos con los que realiza negociaciones o Tratados, o con quien lleva a cabo ciertas políticas y decisiones en el plano internacional. Es por esto que la elección de la teoría del neorrealismo estructural será lo más conveniente para el análisis de esta problemática.

Por otro lado, tenemos a Hobbes quien es otro de los teóricos a los cuales podemos atribuir que aportaron varias ideas esenciales que después Morgenthau se encargó de retomar y organizar para formar su teoría. Esto dado que Hobbes, a lo largo de sus escritos realizó una descripción del hombre y sus ambiciones, lo cual lo lleva a mantener un estado de conflicto permanente con sus semejantes. Esta idea se puede concretar de la siguiente manera: “Por desear la satisfacción de sus pasiones busca la riqueza y el predominio sobre los otros hombres, pero también tiene temor del ataque de los demás y en la pretensión de su seguridad

[4] *Idem*

se confronta con los otros."[5] Esto se puede ver reflejado en los países que buscan siempre hacer la guerra con tal de imponer su poder ante el mundo y mantener sus intereses, ya sea directa o indirectamente, tal como lo hacen los Estados Unidos, que realizan invasiones o intervenciones argumentando que deben detener los intereses maliciosos que varios países o grupos de "terroristas" tienen; esto se vio ejemplificado cuando establecieron que sus intervenciones en los países islámicos eran a causa de que estos tenían armas nucleares, cuando en realidad lo hacían por motivos económicos.

Ahora bien, esta es la manera directa que tienen de imponer su poder. No obstante, también está la indirecta, en la cual hacen uso del *soft power*. Dicha técnica política consta de saturar el mercado de otros países con sus productos y cultura para lograr cierta uniformidad y que, inconscientemente, en dichos lugares se sientan identificados con el país que les llevó los mismos.

Otro autor que cabe mencionar es Emilio Cárdenas, quien se dio a la tarea de exponernos cómo se fue haciendo necesario - en el estudio de las Relaciones Internacionales - el buscar una nueva teoría, un nuevo paradigma que nos ayudara a comprender por qué la Sociedad de Naciones resultó en un enorme fracaso para lograr la paz entre las naciones; lo cual era porque no se podía sostener estas relaciones entre Estados sobre una idea de buenas intenciones, de respeto al Derecho, de apego a las reglas establecidas, en fin, sobre el idealismo.

Por esto es que "el punto de partida de la investigación dejó de ser la sociedad internacional al dar mayor énfasis al estudio de los objetivos e intereses nacionales presumidos como los primeros elementos del análisis."[6] Después de

[5] *Ibídem*. p 197
[6] *Ibídem*. p 200

esto fue que Morgenthau pudo establecer que su teoría era cierta y que los países no se preocupan más que por sus propios intereses.

Es entonces que en el texto de Morgenthau nos damos cuenta que "la escuela realista cree que el mundo es imperfecto desde el punto de vista racional, ya que es resultado de esas fuerzas que son inherentes a la naturaleza humana. Por ello, para mejorar el mundo se debe operar conjuntamente a esas fuerzas y no contra ellas."[7] Por lo tanto, podemos considerar que las relaciones entre las naciones siempre van a estar regidas por un constante conflicto por la búsqueda del poder que les permita lograr sus intereses y que en lugar de pelear con dicha idea, hay que aceptarla y trabajar para que nuestro país y sus intereses salgan victoriosos o al menos no en tanta desventaja, puesto que las condiciones naturales del ser humano no cambiarán ni dejarán de extrapolarse de la misma manera al ámbito de las Relaciones Internacionales.

Ahora que ya poseemos las bases del realismo político, podemos adentrarnos en una de sus ramas, la que mejor se adecua al tema en cuestión: el Neorrealismo estructural. En un artículo de José Guadalupe Vargas Hernández titulado "El realismo y el Neorrealismo estructural" este comienza haciendo una distinción de ambas teorías al especificar que "El acercamiento realista compite con el neorrealismo o realismo estructural y la teoría institucionalista. Las concepciones neorrealista o institucionalistas de las instituciones, consideran que estas son necesidades funcionales para generar orden"[8] Por esto es que la teoría neorrealista o institucionalista puede aplicarse al tema que se trata en esta tesis, ya que los Estados defienden sus instituciones ante todo y consideran que el mundo puede cambiar, sin embargo, las instituciones subsisten y deberán permanecer intactas, debido a que son el arma más fuerte que tienen para

[7] *Ibídem*. p 201
[8] Vargas Hernández, José Guadalupe. "El Realismo y el Neorrealismo estructural" en *Estudios Políticos*, Novena época, núm. 16, enero-abril, 2009. p 113.

defender todos sus actos, sean estos beneficiosos o no para los gobernados. Cabe mencionar que la mayoría de las veces pasa lo segundo pues, como decía Morgenthau: “En política, la nación y no la humanidad es el último hecho” (Morgenthau, 1967: 260). Así podemos comprender por qué es extraño que un país poderoso ponga el bienestar de su población antes que la defensa de sus intereses disfrazados de “seguridad nacional”.

De igual manera, en el mismo texto de Vargas encontramos que el autor hace una clasificación de las variantes del realismo como lo son el realismo clásico y el neorrealismo estructural, pero también el realismo ofensivo y defensivo. Respecto al realismo ofensivo (ampliamente utilizado por las grandes potencias, a diferencia de las economías emergentes o potencias medias, que hacen más uso del defensivo) vemos que nos explica que este “es denominado oportunismo tecnológico por Lieber (2005) desde cuya perspectiva la tecnología es algo que los Estados emplean para perseguir sus políticas. En el oportunismo tecnológico, los Estados rara vez ven los desarrollos de la nueva tecnología como medios para preservar el *status quo* o señalar intenciones benignas, sino como oportunidades potenciales para ganar ventajas políticas y militares sobre los rivales.”[9] Esto lo vemos claramente en el uso que le dan los países a los conocimientos que tienen sus *hackers* para intervenir sistemas informáticos de los países enemigos y causarles un daño sin que estos sepan siquiera de dónde provino el ataque.

Por lo tanto, podemos darnos cuenta de que en el arte del espionaje y la guerra cibernética que viene, no hay regla que valga y el hecho de que ciertos países se indignen por la práctica de estas acciones por parte del gobierno estadounidense resulta algo hasta cierto punto inconcebible y risible, pues no van a poder negar que ellos no lo hacen.

[9] *Ibídem*. p 113 y 114.

Sin embargo, lo que sí es un hecho es que Estados Unidos precisamente supo cómo sacar provecho de los avances tecnológicos que describe Lieber en su idea del oportunismo tecnológico, así como del profundo conocimiento que tienen los encargados de sus Agencias de Inteligencia para lograr espiar directamente a los grandes dirigentes. No obstante, lo que no consideraron fue que ellos también cuentan - incluso dentro de sus propias filas - con alguien que los descubriría y traicionaría, tal como Edward Snowden a quien le preocupó más la libertad de expresión y el derecho a la privacidad de la población estadounidense que seguir las reglas de las políticas establecidas en la Agencia de Seguridad Nacional para la cual trabajaba.

Ahora bien, volviendo a la teoría del neorrealismo estructural, dentro de los principales supuestos teórico-metodológicos de la misma encontramos que:

> La política internacional comprende más que la historia contemporánea y que los asuntos del día. El observador se ve rodeado por el escenario contemporáneo en su énfasis siempre variable y sus perspectivas cambiantes. Le será imposible hallar un terreno de sustentación, o bien hallar normas objetivas de valoración sin penetrar a los principios fundamentales; estos se revelan sólo por la correlación de acontecimientos recientes con un pasado más distante, y con las cualidades perennes de la naturaleza humana, que son subyacentes a lo uno y a lo otro.[10]

Esto nos permite hacer un análisis variable, maleable o versátil del conflicto trabajado en este escrito, ya que la sociedad internacional no es un ente perfecto que siga ciertas reglas de comportamiento o un sistema inmóvil y estricto que funcione sólo de una manera. Hay que comprender que existen infinidad de factores que pueden hacer que una suposición planteada - aún sobre las bases de cierta teoría - pueda sufrir cambios ocasionando que los resultados no sean

[10] Gutiérrez Pantoja, Gabriel, *Op. Cit.,* p 202

exactamente los que se habían previsto. Sin embargo, a pesar de esto se pueden tomar en cuenta experiencias ya conocidas y hacer una comparación histórica de alguna situación que nos permita tomar como base algo que ya sucedió previamente, para así poder prever los posibles escenarios que dicha situación podría presentar.

Dicho de otra manera, se pueden tomar en cuenta ciertas instituciones o marcos legales que sirvan a este tipo de análisis, pero no se les puede tomar como algo que va a determinar por completo el curso que vaya a tomar la situación, sino como un mero factor entre varios que hay que considerar, sabiendo que las acciones y decisiones políticas tendrán un peso mayor que las instituciones, organizaciones o leyes internacionales. A pesar de que su existencia, de acuerdo con los institucionalistas, ayude a lograr un orden, veremos que actualmente eso es cada vez más difícil de asegurar.

A continuación, debemos también mencionar a Kenneth Waltz, quien es uno de los exponentes más importantes del neorrealismo estructural pues defiende la idea de que la distribución del poder y el número de polos que tenga una estructura será lo que ayude a explicar su estabilidad y continuidad. También, para Waltz "los sistemas pueden ser nacionales e internacionales. El primero es jerárquico, con una división de trabajo entre las diferentes unidades y el segundo es anárquico, de autoayuda, en el que cada Estado aspira a maximizar el poder como un instrumento de sobrevivencia"[11] Igualmente, Waltz define la estabilidad como "la durabilidad del sistema y lo pacífico de sus ajustes internos…y existe en tanto el sistema permanece anárquico y mantiene su número de polos."[12] Esta es básicamente la teoría que explica cómo puede haber un orden dentro del caos.

[11] Vargas Hernández, *Op. Cit.,* p 120
[12] *Ibídem.* pp 120-121.

Además, también establece que "la estructura es la responsable de proveer la estabilidad óptima en un balance de poder que funciona como el rol crítico de guardián. De acuerdo a Waltz, si la seguridad es lo que el Estado quiere, imponen ciertos requerimientos en las políticas internacionales que pretenden ser racionales. Si se aparta del modelo racional, pone en peligro la sobrevivencia del Estado."[13] Aquí es donde EEUU se equivocó al intervenir los celulares de sus aliados más importantes y espiar sin escrúpulos a su propia población, puesto que no se trataba de terroristas o siquiera de amenazas potenciales; por lo que al apartarse de ciertas políticas o características óptimas de balance de poder y estabilidad, puso en peligro la supervivencia del Estado que nos expone Waltz.

1.2. Guerra Cibernética

Podemos definir a la Guerra Cibernética como "los ataques malintencionados perpetrados a través de cauces electrónicos contra las bases de datos"[14] de cualquier país desde algún punto del planeta, no importa qué tan desarrollado se encuentre este ya que los ataques cibernéticos son mucho más baratos y accesibles para cualquiera, a diferencia de un gran arsenal militar, el cual sólo puede ser costeado por los países con el mayor poder adquisitivo o con el mayor "apoyo" del exterior para dicho fin.

> Dependiendo de sus fines, se habla de delincuencia o terrorismo cibernético. Un intruso informático puede acceder y emplear información privada referida a determinado grupo al que no pertenece. De este modo, destruye la confidencialidad y, al mismo tiempo, la confianza en la seguridad que ofrecen las nuevas tecnologías, requisito básico para el correcto funcionamiento de la sociedad de la información. Más allá, el intruso puede manipular archivos

[13] *Ibídem.* p 121.
[14] Wegener, Henning. "La Guerra Cibernética" en *Política Exterior,* No. 80, Marzo-abril 2001, p 131. Recuperado de: https://www.unibw.de/infosecur/documents/published_documents/guerra_cibernetica Consultado el 19 de noviembre de 2014.

> introduciendo datos propios o alterando los existentes. Puede, también, reprogramar sistemas de información que controlan importantes procesos mediante la introducción de comandos falsos y destruir la integridad del sistema, o bien comprometer la disponibilidad de determinados datos suprimiéndolos o modificando los servicios que proporcionan, de modo que sistemas enteros dejen de funcionar.[15]

Por ejemplo, vemos que todo esto se puede dar a través del envío masivo de información para bloquear un servidor, también con virus informáticos que afecten el funcionamiento de cualquier sistema o por actividades de piratería que logren que la autenticidad de determinados archivos quede completamente destruida. De igual manera, puede darse por el medio que este trabajo analiza: la filtración de información de alta importancia para los gobiernos a través de la utilización de complejos sistemas informáticos que sólo pueden ser operados por expertos en la materia, lo cual deja en posición desventajosa a los altos poderes del gobierno cuando no logran controlar la situación.

Al mismo tiempo, otro concepto que debemos exponer es el del Crimen Cibernético, al cual podemos definir como el "acto criminal cometido mediante la utilización de computadoras como herramientas principales […] Para que exista crimen cibernético el computador no sólo juega un papel muy relevante sino que también deben darse profundos conocimientos informáticos por parte de quienes delinquen. Existe crimen cibernético si computadores han sido objeto, sujeto o instrumento del ilícito."[16] Dicho concepto representa la primera acepción que debemos tomar en cuenta para distinguir una de las principales formas de dañar a alguna comunidad a través de medios electrónicos.

[15] *Ibídem*. Pp 131 y 132.
[16] Uzal, Roberto. "Guerra Cibernética: ¿Un desafío para la Defensa Nacional?" (s.f.) Recuperado de: http://esgcffaa.mil.ar/numero7/40.html Consultado el 19 de noviembre de 2014.

Por otro lado, cabe mencionar al Terrorismo Cibernético, el cual tiene otros fines, actores y maneras de actuar, sin embargo, los elementos que se mantienen son las computadoras y el mundo informático en general. Así, tenemos que la definición de terrorismo para el FBI es: "El uso ilegal de la fuerza o violencia contra personas o propiedades para intimidar o ejercer coerción a gobiernos, población civil o, de la misma manera, a algún sector / segmento, para el logro de objetivos políticos o sociales."[17] De aquí podemos interpretar que el Terrorismo Cibernético es un "Crimen Cibernético pero realizado por motivaciones religiosas, sociales o políticas."[18] La diferencia que podemos encontrar de cualquier otro crimen cibernético es que este ya no se da por meras razones económicas, sino que tiene un fin más complejo, como el de organizar a un grupo con una ideología común, ya sea política, religiosa o social, para realizar un boicot de manera cibernética.

Por último, tenemos al Espionaje Cibernético, el cual, toma como base a los elementos ya explicados, pero finalmente mantiene el mismo propósito que siempre ha perseguido: el de recabar información suficiente de gobiernos, empresas o individuos del extranjero principalmente (ahora también nacionales) oportunos para la seguridad nacional o comercial del Estado o grupo secreto que realiza el espionaje. Ahora bien, al ser de carácter cibernético, este tipo de espionaje se vale de las nuevas tecnologías para realizar sus actividades, entre las cuales podemos encontrar la captura de datos del correo electrónico, teléfono móvil u otro tipo de comunicaciones electrónicas, información que en la actualidad resulta mucho más fácil de obtener que mediante los métodos de años atrás.

1.3. Espionaje y espías

El diccionario de la Real Academia de la Lengua define a la acción de espiar como: "Acechar, observar disimuladamente a alguien o algo. Intentar conseguir

[17] *Ídem*
[18] *Ídem*

informaciones secretas sobre un país o una empresa"[19] sin embargo, al buscar la palabra espionaje surge la idea de internacionalizar esa acción de observar, de acechar, agregando necesariamente el elemento de la secrecía, la seguridad nacional y la defensa de los intereses del Estado: "Actividad secreta encaminada a obtener información sobre un país, especialmente en lo referente a su capacidad defensiva y ofensiva. Actividad dedicada a obtener información fraudulenta en diversos campos."[20] Así, nos encontramos con que esta actividad resulta en un tema incómodo e incluso prohibido o ilícito, aun cuando todos en el mundo sabemos que es utilizada con más frecuencia de la que nos imaginamos.

Ahora, también cabe aclarar que para obtener información por parte de algún gobierno extranjero existen como opciones la vía diplomática y el espionaje. En la primera, se envían representantes del Estado para que mantenga reuniones con sus homólogos o con los Jefes de Estado o de Gobierno más que nada con el fin de conocer la posición que ese país mantiene respecto a cierto conflicto o situación y así realizar negociaciones en las cuales ambas partes obtengan beneficios, buscando siempre el mayor para sí mismos. Pero, por el contrario, el espionaje se hace más viable pues generalmente no se cuenta con la paciencia necesaria para esperar a que la contraparte (país receptor o "B") responda a las dudas que les presentan los enviados del país "A" y porque resulta prácticamente imposible obtener toda la información que se desea de la manera diplomática, puesto que siempre hay cosas que todo gobierno oculta a los demás, y sobre todo la información más decisiva y relevante.

Es por esto que, durante las guerras mundiales dicha actividad se realizó con un mayor auge y se diversificaron los métodos para llevarla a cabo, principalmente la infiltración y la penetración. "La infiltración es la técnica utilizada para introducir

[19] Real Academia Española. *Diccionario de la Lengua Española*. Tomo 1. Editorial Espasa Calpe, S.A. España, 2002, p 979
[20] *Ibídem*. p 981

unidades propias en las filas del contrario o blanco, para que suministren información de interés inmediato o potencial sobre las actividades, capacidades, planes y proyectos del contrario, cuyo cometido básico es ganarse la confianza de aquellos que poseen la información para tener acceso a la misma."[21] La segunda técnica es la penetración, la cual "consiste en lograr la colaboración consciente o inocente de un miembro de la organización o grupo contrario con el fin de que proporcione datos e información confidencial del grupo al que pertenece. Generalmente, esta actividad se realiza con personas que han sido persuadidas para trabajar en secreto en contra de su propia organización por diferentes motivaciones: ideológicas, económicas, morales, religiosas o personales."[22] Aquí podemos encontrar a todos aquellos trabajadores de algún gobierno que a pesar de haberle sido fiel al mismo en un principio, después de conocer los verdaderos fines de la organización para la que trabaja o por haberse dejado influenciar por la opinión de los contrarios a la misma, abandona en un momento dado la fidelidad que le solía tener para comenzar a trabajar en su contra. Dentro de esta lista, encontramos a personas como Edward Snowden o Chelsea Manning, de los cuales hablaremos más adelante.

Concretamente, respecto a las muchas cualidades que debe poseer un profesional de la inteligencia, es decir, un espía, estas se indican en el libro de David L. Perry, *Partly Cloudy*. Aquí se menciona que "requieren atributos comunes a muchas otras profesiones, incluyendo habilidades de comunicación verbal y oral excelentes […] deben conocer las últimas técnicas y métodos usados en la profesión, así como las tendencias y patrones del nuevo conocimiento."[23] Asimismo, también se establece que "como en toda profesión […] el compromiso ético entre los individuos y su trabajo debe ser llevado al frente si esa profesión busca ganar el respeto de aquellos que sirven a la comunidad de la inteligencia.

[21] Quees.la. *¿Qué es espionaje?* (s.f.) Recuperado de: http://quees.la/espionaje/ Consultado el 10 de septiembre de 2014
[22] *Idem*
[23] Perry, David L. *Partly Cloudy. Ethics in war, espionage, covert action, and interrogation*. The Scarecrow Press, Inc., Estados Unidos de América, 2009, p 9, Traducción propia.

Es también extremadamente importante para los profesionales de la inteligencia pensar en su conducta individual y qué tan lejos están dispuestos a llegar en la búsqueda de sus objetivos profesionales."[24]Así, ya podemos darnos una idea de lo serios y comprometidos con su trabajo que deben ser aquellos que se dedican a esta profesión, pues no se trata de cualquier cosa; están tratando con personas, actitudes, comportamientos y sobre todo con información importante para el gobierno para el cual trabajan.

Conviene subrayar que, aunque no es nuevo el que un espía trabaje para otros gobiernos de igual manera que puede trabajar para el suyo, lo que sí representa un fenómeno nuevo es la manera en que las nuevas tecnologías les permiten trabajar: esto quiere decir que ahora que el mundo está tan interconectado y que todo puede conseguirse con mayor facilidad, así como se pueden mantener ocultos los métodos utilizados y la información obtenida, también es gracias a los avances tecnológicos, el internet o los métodos de encriptación de mensajes y documentos que, los espías cibernéticos pueden "hackear" páginas del gobierno o hacer uso de infinidad de métodos para obtener información confidencial. Dicho sea de paso que esta es una cuestión que representa un problema cada vez más difícil de manejar para los gobiernos dado que día tras día más gente se prepara (con estudios o sin ellos) y se vuelven más hábiles en cuestiones tecnológicas haciendo posible el uso "malicioso" de sus conocimientos, perjudicando así a individuos, empresas o incluso gobiernos.

Es probablemente en este aspecto donde los trabajadores de las Agencias de Seguridad de Estados Unidos fallaron, pues no cualquiera se atreve a filtrar información importante para su gobierno y menos si se trata de ese país, donde es gravemente castigada la traición. De igual manera, representa mayor gravedad si es respecto a política pues les restan prestigio y presencia como potencia.

[24] *Idem*

Igualmente en el libro *Partly Cloudy* se hace un análisis de cómo han cambiado, a lo largo de los años, los objetivos que persigue Estados Unidos, los cuales encomienda a estas Agencias de Seguridad e Inteligencia. Se hace la aseveración de que "desde el fin de la Guerra Fría, la amenaza a la seguridad nacional de Estados Unidos ha cambiado de la guerra convencional a una guerra asimétrica. En lugar de recolectar información sobre tanques y aviones, la comunidad de inteligencia está buscando campamentos terroristas en terrenos extremadamente duros."[25] Sin embargo, esa no fue más que otra transición en los objetivos de Estados Unidos en cuanto a guerra se refiere, ya que actualmente, encontramos que los campamentos terroristas no se están buscando únicamente en territorios físicos, sino también en el mundo informático.

Por lo que se puede observar, se trata ahora de guerras menos declaradas y más bien ocultas, por llamarlas de alguna manera, son más complicadas de entender y de encontrarles tanto un origen como una resolución que sirva a todas las partes, ya que los grupos terroristas conocen muy bien su terreno de acción, los apoyos con los que cuentan, la manera de hacer política, cómo manipular a la población que los sigue y sobre todo cómo huir de todo aquel que quiera espiarlos o inmiscuirse de cualquier manera en sus asuntos. Sin embargo, Estados Unidos posee un gran poderío militar, del cual puede hacer uso cuando mejor le parezca, por lo que le resulta fácil espiar, vigilar y comenzar la búsqueda de todos estos grupos que representan un verdadero dolor de cabeza para los dirigentes occidentales, pero más que nada para dicha nación y sus intereses.

Por todo esto es que dicho país requiere de profesionales de inteligencia responsables, comprometidos, trabajadores e incluso, muy nacionalistas y respetuosos del gobierno para el que laboran. Mientras Estados Unidos no ataque este problema de raíz, no veremos un verdadero avance en cuanto a su espionaje,

[25] *Idem*

sus fuerzas de seguridad e inteligencia y en la manera en que estas trabajan sin afectar sus relaciones diplomáticas con otros países.

Seguridad nacional

Por ser uno de los objetivos principales de los Estados, si no es que el principal, resulta de vital importancia definir este concepto, que además es constantemente mencionado al realizar un trabajo acerca del espionaje, ya que la finalidad de dicha actividad es recabar información acerca de algún enemigo o aliado de algún gobierno para que así este sepa qué decisiones tomar y qué acciones llevar a cabo para la consecución de sus intereses. La mayoría de las veces se basan en la información recabada para así tomar la mejor decisión posible con respecto a alguna situación que ambas partes estén valorando en el terreno internacional. Así, podemos decir que:

> El significado de seguridad es el de estar libre de peligro o preocupación. Un sentimiento de inseguridad se gesta en un país vulnerable, incapaz de salvaguardar su integridad como nación. Los ideales presentes en la agenda de seguridad son las de equilibrio y paz, que se ven representados en capacidad bélica y habilidad para garantizar el control interno y externo en el país. La confianza de sus ciudadanos, la legitimidad, el prestigio ante otros países, y el mantenimiento del bienestar en un estado se correlacionan en gran medida con el concepto de seguridad nacional.[26]

Además, no podemos considerar a la seguridad nacional de un Estado, así como los objetivos que persigue y los motivos que lo orillan a protegerse interna y externamente de las posibles amenazas a su soberanía, como si fueran siempre los mismos, sino que más bien "la seguridad de un Estado se construye y adapta

[26] (s.a.) *Seguridad Nacional: Definiciones y conceptos*. (s.f.) p 9, recuperado de: http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/munoz_p_ba/capitulo1.pdf Consultado el 11 de septiembre de 2014

de manera circunstancial, modificándose de acuerdo a las necesidades de cada país y adaptándose a los contextos de historia, cultura y sociedad."[27] Esto quiere decir que la política exterior de un país así como los métodos que implementará para que la misma se lleve a cabo, no pueden ser estáticos, sino que se encuentran en constante cambio de acuerdo con lo que el mundo esté presentándole. En caso contrario, si un país se rehúsa a modificar o adaptar su política exterior de acuerdo a la coyuntura internacional actual, se arriesga a la pérdida de su poder e incluso el respeto de las otras naciones.

Igualmente, hay otras variables que deben tomarse en cuenta para lograr comprender las motivaciones de los Estados de defenderse contra otro, así como sus limitaciones: "Las diferentes capacidades de los Estados, su situación interna y la del entorno internacional hacen que la interpretación de las amenazas y los objetivos nacionales sean vistos siempre de diferente manera y motiven así, su reformulación constante."[28] Así, en cada Estado ha recaído la responsabilidad de defenderse de las amenazas extranjeras o incluso internas algunas veces, basadas en diferentes cuestiones, tales como aspectos religiosos, sociales, económicos, culturales, étnicos, territoriales, marítimos, de recursos e incluso ideológicos, con el fin de salvaguardar la soberanía del mismo, así como proteger su legitimidad como grupo al frente de la población de un Estado. Por lo que, si bajo cualquier circunstancia, un país se ve amenazado por otro y no sabe cómo responder queda como un país débil que no sabe ni siquiera controlar los conflictos que se le presentan y hacerles frente de la mejor manera posible.

Basándonos en la aseveración recién mencionada, se debe optar siempre primero por la diplomacia y las negociaciones pertinentes, pero si después de varios intentos de solucionar las cosas de esa manera, la contraparte no desea ceder en

[27] *Ibídem* p 8
[28] *Idem*

sus intentos por atacar y destruir el prestigio de la nación atacada, se debe recurrir al uso de medidas coercitivas e incluso la fuerza para hacerles saber que sí tienen capacidad de defenderse y que no lograrán intimidarlos ni restarles importancia en la escena internacional.

Para darnos cuenta de una manera más clara cómo se maneja esto, se puede tomar como ejemplo al Estado mexicano y su propio Servicio de Seguridad: el CISEN (Centro de Investigación y Seguridad Nacional, México) el cual nos dice respecto a la seguridad nacional que:

> La Ley de Seguridad Nacional la define como las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano que conlleven a:
>
> - Proteger al país frente a riesgos y amenazas.
> - Preservar la soberanía, independencia, territorio y la unidad de la federación.
> - Mantener el orden constitucional y fortalecer las instituciones democráticas de gobierno.
> - Defender al país frente a otros Estados o sujetos de derecho internacional.
> - Preservar el régimen democrático fundado en el desarrollo social, económico y político.[29]

Igualmente, respecto a las amenazas principales que el Estado mexicano considera deben tomarse en cuenta para salvaguardar la soberanía del mismo, se encuentra lo siguiente:

> Entre las responsabilidades del Centro está la de proponer medidas de prevención, disuasión, contención y desactivación de riesgos y amenazas que

[29] CISEN. *Seguridad Nacional*. (s.f.) Recuperado de: http://www.cisen.gob.mx/snSegNal.html Consultado el 11 de septiembre de 2014.

pretendan vulnerar el territorio, la soberanía, las instituciones nacionales, la gobernabilidad democrática o el Estado de Derecho.

Se definen como amenazas a la Seguridad Nacional, a los fenómenos intencionales generados por el poder de otro Estado, o por agentes no estatales, cuya voluntad hostil y deliberada pone en peligro los intereses permanentes tutelados por la Seguridad Nacional, en parte o en todo el país, y cuestionan la existencia del mismo Estado.

[…] se entienden como amenazas a la Seguridad Nacional, actividades relacionadas con:

Espionaje, sabotaje, terrorismo (incluyendo actividades de financiamiento), rebelión, traición a la patria, genocidio, tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva, y actos en contra de la seguridad de la aviación y la navegación marítima.

Actos tendientes a obstaculizar o neutralizar actividades de inteligencia o contrainteligencia.

Destrucción o inhabilitación de la infraestructura […] indispensable para la provisión de bienes o servicios públicos.

Interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano y actos que atenten en contra del personal diplomático.[30]

Así, encontramos que las posibles amenazas a la seguridad nacional de un país pueden ser extremadamente diversas y que no es posible encontrar dos Estados que presenten las mismas amenazas, ya que estas se adecuan a la realidad nacional e internacional de cada uno de los países que conviven (no necesariamente de manera pacífica) en nuestro mundo.

[30] CISEN. *Amenazas y riesgos*. (s.f.) Recuperado de: http://www.cisen.gob.mx/snAmenazasRiesgos.html Consultado el 11 de septiembre de 2014.

Lo que interesa analizar y comprender en este trabajo es cómo países como Estados Unidos salvaguardan sus intereses con la bandera de que defienden su "Seguridad Nacional" sin importarles qué derechos rompan o por encima de quien pasen. Sin embargo, cuando todos sus métodos salen a la luz y comienzan a haber revueltas, levantamientos o incluso ataques directos al gobierno, entonces sí se preocupan y tratan de defender sus actos basándose en leyes que quebrantan todas y cada una de las libertades o derechos civiles, pero que de alguna manera logran aprobarse para que desde un principio puedan llevar a cabo sus intervenciones tanto a los propios ciudadanos como a otros países, con "todas las de la ley".

Esto podríamos resumirlo en ciertas palabras que expresa Glenn Greenwald en su libro *Snowden. Sin un lugar donde esconderse*: "A los funcionarios de la Seguridad nacional no les gusta la luz."[31] Esto quiere decir que tanto a los servidores públicos como a los trabajadores de los Servicios Secretos les disgusta que se dé a conocer su manera de trabajar, ya que de esta manera se ven imposibilitados a llevar a cabo todas aquellas acciones que de diversos modos menoscaban los intereses y el bienestar general de la población.

Es por esto que actualmente encontramos grupos como *Anonymous* o personajes como Edward Snowden que buscan dar a conocer a través de redes sociales y varios medios de comunicación en línea, los verdaderos objetivos del gobierno y así lograr un consenso en contra de los mismos, el cual permita que la población se imponga a su gobierno y dejen de oprimirla con políticas "maquilladas" que aunque se presentan como benéficas para la gente, en realidad no lo serán una vez que se lleven a la práctica.

[31] Greenwald, Glenn. *Snowden. Sin un lugar donde esconderse.* Ediciones B S.A., Barcelona, 2014, p 24.

Capítulo 2
El mundo cibernético

2.1. El uso del internet en la política
2.2. La comunicación en la actualidad
2.2.1. Redes Sociales
2.2.1.1. Revoluciones digitales: El fenómeno de la manifestación social organizada por internet
2.2.1.2. Su significado mediático en la política internacional
2.3. El papel del Estado ante el mundo cibernético
2.3.1. Sociedad red y seguridad del Estado en un mundo interconectado
2.3.1.1. El "Big Brother" Orwelliano aplicado: Vigilancia de la población
2.3.1.2. El control de la red y sus límites:
2.3.1.2.1. Leyes
2.3.1.2.2. Compañías
2.3.1.2.3. Hackers

2.1. El uso del internet en la política.

El internet ha sido la innovación tecnológica que mayores efectos sociales ha provocado en la historia de la humanidad dada la inmediatez de respuesta que tiene y su crecimiento a gran escala. Encontramos así aseveraciones como la que Josep Ibañez hace en su artículo *Globalización e Internet: Poder y gobernanza en la sociedad de la información*: "El ciberespacio no está al margen de las relaciones y las estructuras de poder, y los riesgos derivados de internet generan una necesidad de gobernanza cada vez más acuciante en la denominada sociedad de la información."[32] Esto nos lleva necesariamente a analizar cómo el poder del Estado y el ámbito de la gobernanza en general se han tenido que replantear con la llegada de la globalización, las nuevas tecnologías y los medios de comunicación alternativos, ya que con el aumento de las conexiones y relaciones

[32] Ibáñez, Josep. "Globalización e Internet: Poder y gobernanza en la sociedad de la información" en *Revista Académica de Relaciones Internacionales*, No. 5, Noviembre de 2006, UAM-AEDRI, p 2. Recuperado de: http://www.relacionesinternacionales.info/ojs/article/view/38.html Consultado el 19 de noviembre de 2014.

a nivel global que vemos en la actualidad, es mucho más fácil saber lo que pasa en cualquier lugar del mundo y organizar grandes movimientos a partir de alguna crisis, por mínima que esta sea.

Esto ha descontrolado a las naciones de todo el mundo, ya que sus gobiernos tienen que invertir más en expertos que les ayuden a elaborar políticas adecuadas referente al tema de Internet y de cómo el mundo cibernético puede afectarles en sus relaciones gubernamentales, diplomáticas y de gobierno-sociedad.

Esto nos lleva a "plantear la globalización y la sociedad de la información como fenómenos históricos indisociables."[33] Referente a la globalización, Josep también da una breve explicación: podría ser definida como la "progresiva transformación de un conjunto de procesos sociales interrelacionados (económicos, políticos, culturales, medioambientales) cuya intensidad aumenta y se manifiesta en una escala geográfica que tiende a ser mundial."[34] Así, al homogeneizarse todos o casi todos los procesos de nuestra vida, los gobiernos a nivel mundial se enfrentan a otro tipo de retos y a una sociedad que comparte el sentir y las maneras de actuar con gente de otros países, quizá muy diferentes a ellos, situación que hace unos años no existía y no representaba conflicto para el Estado que desea aún gobernar a la población a la vieja usanza.

Por su parte, Manuel Castells hace la observación de que estas "tecnologías del procesamiento de la información y de la comunicación son […] el núcleo de esa transformación revolucionaria cuya esencia radica en la aplicación de ese conocimiento e información a aparatos de generación de conocimiento y procesamiento de información/comunicación, en un círculo de retroalimentación

[33] *Idem*
[34] *Ibídem* pp 2 y3.

acumulativo entre la innovación y sus usos."[35] Es importante destacar esto ya que la tecnología sí ha jugado un papel muy importante en la sociedad de los últimos años, sin embargo, no es en sí la tecnología la que hizo el cambio en los paradigmas de la sociedad y la política internacional, sino las personas que le han sabido dar cierto uso, ya sea desde el ámbito educativo o cultural hasta el político-social para lograr dichos cambios.

Considerando lo antes mencionado, Moisés Naím explica en su libro *El fin del poder* que no podemos centrar el análisis en el efecto completo que tienen las nuevas tecnologías en la política, en si el poder blando o el poder duro tendrán repercusiones en las mismas o viceversa, si harán uso de ellas en dado momento para lograr sus fines, pues a final de cuentas son más los elementos nuevos de los que podemos alcanzar a analizar. Dicha idea, el autor la resume de la siguiente manera: "Es como si una centrifugadora política hubiera tomado los elementos que constituyen la política tal como la conocemos y los hubiera esparcido por un escenario nuevo y más amplio."[36] Asimismo menciona que el poder está cambiando de manos, ya no lo ostenta una sola nación o un bloque económico o político; ahora sucede que el poder está con quien tiene más conocimientos, en las empresas jóvenes y dinámicas, se encuentra en el mundo cibernético que es un actor enorme y complejo, del cual se podría decir que es imposible de abarcar en su totalidad si lo que se desea es analizarlo.

Por esto es que en lugar de querer investigarlo a profundidad y formar teorías al respecto, las naciones deben integrarlo a su agenda diaria y saberlo manejar de manera dinámica para así lograr sus objetivos sin verlo como un enemigo sino como un aliado. Al respecto, Juan Pablo Adame Alemán nos expone que "aunque hemos insistido en que las tecnologías no transforman la realidad por sí mismas, su

[35] *Idem* p 3.
[36] Naím, Moisés. *El fin del poder*. Random House Mondadori, S.A., Barcelona, 2013, p.159.

utilización inteligente y creativa en las acciones sociopolíticas deberá ser crítica, entendiendo las limitaciones, alcances y formas en las que estas han reordenado la vida social." [37] Al convertirse en parte crucial de nuestra vida, más allá de un simple medio de comunicación, el internet ha cobrado un poder inimaginable del cual los agentes políticos ya existentes quieren una parte, por lo que deben hacer uso de él continuamente, pero sobre todo, deben aprender a utilizarlo correctamente.

Consideremos ahora a esta intención de los gobiernos por adaptarse a las nuevas tecnologías, a la implementación de la "agenda digital" la cual Juan Pablo Adame nos describe como "el conjunto de políticas públicas para el desarrollo tecnológico de un país, entidad federativa, región o ciudad. La mayoría de las estrategias, se enfocan en incrementar el uso del Internet para crear un impacto en el desarrollo económico y social."[38] Cabe recordar que no sólo se trata de incrementar el uso del Internet como lo menciona Adame, sino de hacerlo inteligentemente, por lo que se deben tener filtros de la información o consultarla en varias fuentes antes de tomar algo como verdadero, ya que muchas veces la inmediatez suplanta a la verdadera investigación, lo cual impide o complica la implementación de políticas perdurables y efectivas.

Por su parte, Josep Ibáñez expone los retos que tienen los gobiernos respecto al buen uso de los avances tecnológicos, tales como la rapidez de su crecimiento, su carácter transnacional y su capacidad de convergencia (casi todos los medios de comunicación ahora se encuentran en uno solo) como se explica a continuación:

> En apenas veinte años se han visto transformados por completo algunos sectores económicos, los hábitos de consumo, las formas de comunicación,

[37] Adame Alemán, Juan Pablo. *Ciudadanía digital ¿Oportunidad o amenaza?* Imagia Comunicación, S. de R.L. de C.V. México, 2015, p. 122.
[38] *Ibídem*, p. 124.

> las fuentes de información y un sinfín de actividades y recursos que afectan directamente al ciudadano medio de cualquier país industrializado. Este hecho ha provocado que (…) todo tipo de organizaciones gubernamentales, empresas, y organizaciones no gubernamentales se (hayan) planteado con inquietud cómo seguir el ritmo de los cambios, cómo gestionar las nuevas situaciones resultantes, cómo prever la evolución de los mercados, y cómo aprovechar las oportunidades que todo cambio inesperado puede ofrecer. Debido al carácter transnacional de la comunicación, los gobiernos que permiten los flujos de información –e incluso aquellos que intentan contenerlos– constatan las dificultades para controlar sus efectos sobre la sociedad, mientras que para las empresas, los mercados transnacionales constituyen una fuente de oportunidades de negocio a la vez que un espacio de competencia feroz. Para los gobiernos, la integración ha supuesto una dificultad insuperable para distinguir entre ámbitos de regulación pública, pues cualquier medida de limitación o de liberalización de la competencia automáticamente se transmite entre todos los sectores implicados en las tecnologías de la información y la comunicación.[39]

Ahora bien, en el ámbito político vemos que muchas veces la tecnología representa un medio de poder ya que es una forma de obtener conocimiento y si se logra restringir su difusión, se priva a la población mundial de conseguirlo y darle un uso que no le convenga a los altos mandos de cada país. En consecuencia podemos considerar que: "El control sobre esta estructura de poder determina qué conocimiento se adquiere, cómo es almacenado, quién lo difunde, por qué medios, a quién y en qué condiciones"[40] y es así como los gobiernos pueden ganarle la batalla al Internet, sin embargo, siempre hay personas expertas en esquivar dichas "estrategias" del gobierno, puesto que logran obtener la información y la hacen pública, tal y como se han encargado de hacerlo personajes como Julian Assange, Edward Snowden y Chelsea (antes Bradley) Manning, quienes ahora representan una amenaza pública para el gobierno de los Estados Unidos de América.

[39] Ibáñez, Josep. *Op. Cit.*, pp 4 y 5.
[40] *Ibídem*. p 6

Finalmente, Robert Cox afirma que “la tecnología es un elemento esencial en la estructura de poder global. La interacción entre fuerzas sociales y tecnología es tan estrecha que la evolución de ambas es indisociable: las fuerzas sociales conforman la tecnología y la tecnología conforma las fuerzas sociales.”[41] Es por esto que se han podido configurar grandes movimientos sociales a partir de la organización vía internet, los cuales iremos estudiando a lo largo de este capítulo, así como la respuesta gubernamental a dichos movimientos y al poder de los medios de comunicación electrónicos de hoy en día.

2.2. La comunicación en la actualidad

Hemos visto que desde los años setenta se ha ido desarrollando el Internet hasta alcanzar la inclusión que ahora tiene en nuestro día a día. Estamos tan interconectados en nuestras realidades virtuales que ya no podemos concebir un día de nuestras vidas sin conectarnos a la red, sin checar nuestras redes sociales, sin ver las noticias en línea, sin dar “*likes*” en *Facebook* o sin “*Twittear*” algo.

Así es como se ha configurado nuestra vida, somos entes virtuales y ahora todo lo que organizamos y casi toda la comunicación que mantenemos con amigos, compañeros laborales o conocidos es a través de un medio electrónico como los ya mencionados, siendo que tan sólo constituyen un pequeño mundo dentro del mar de posibilidades que existen actualmente para realizar dicha comunicación.

Esto se ha transportado al ámbito de los movimientos sociales, de las manifestaciones a causa de conflictos, principalmente políticos, que generan un gran descontento. Al verse esto reflejado en las redes sociales, adquiere mucha

[41] *Idem*

más fuerza que años atrás. Esto debido a que todo conflicto ahora puede llegar a gente de todo el mundo generando gran convocatoria para los movimientos mencionados.

El mundo en nuestros días se enfrenta a dos tipos de revoluciones que Moisés Naím nos expone también en su libro *El fin del poder* y se refiere a la revolución de la "movilidad" y la revolución del "más". Al respecto, dicho autor estipula que hay mucha más gente en el mundo por lo que exigen mucho más de lo que los gobiernos pueden ofrecerles, representando un reto importante para los mismos; y no solo son más, sino que se mueven más alrededor del mundo creando así un puente entre su país de origen y el que los recibe. Incluso menciona que en la campaña presidencial de Obama en 2012 los votantes hispanos fueron un factor importante a tomar en cuenta. El autor considera que "la movilidad internacional moldeó la realidad política de Estados Unidos, cosa que también está ocurriendo en muchas otras partes."[42] Las diásporas / minorías no sólo han cambiado el estilo de vida, la economía o las religiones profesadas en determinado país receptor sino que se valen de los nuevos medios de comunicación para hacerlo. Una de las razones es lo económico y fácil que resulta manifestar una opinión, vender algo, publicar sobre cualquier tema o incluso atacar a alguien valiéndose de los medios cibernéticos.

Sobre dicho tema, Juan Pablo Adame explica que "el ciberespacio como ágora digital contribuye a eliminar las barreras sociales y los monopolios en manos de las élites, ya que el bajo costo de participación hace más accesible a personas comunes la posibilidad de integrarse, disminuyendo simultáneamente el costo y las dificultades de aprendizaje, sobre todo en las nuevas generaciones para las cuales el uso de Internet y la comunicación a través de las redes virtuales es ya algo

[42] Naím, Moisés. *Op. Cit.,* p.97.

completamente natural y cotidiano."[43] Por esto es que los canales de comunicación ya existentes se han ampliado y se han creado muchos nuevos, presentando un reto más al Estado.

Así, se puede reflexionar también sobre lo que Abram Shulsky y Gary Schmitt revelaron: "Incluso antes de la llegada de la era de la información, gran parte de la información que llegaba a los hacedores de políticas era fuera de los canales tradicionales. No obstante, los cambios en el ambiente de la política internacional y aquellos asociados a la revolución de la información sugieren que más información generada fuera de los círculos de la inteligencia estarán disponibles en el futuro"[44] para la población en general, considerando de igual manera que una vez que la información se filtra en la "nube" no hay manera de que desaparezca; cualquier persona a través de diversos medios es capaz de guardar la información que aparece en la red, esparcirla entre sus contactos y / o publicarla en diferentes sitios en Internet haciendo que en segundos la misma información llegue a los oídos u ojos de millones de personas alrededor del globo, representando un problema álgido no solo para gobiernos, sino también para empresas, gente de la farándula y toda clase de individuos, sin embargo no nos detendremos en este aspecto dado que dicho tema se abordará más adelante.

Ahora bien, si nos remontamos a los orígenes del Internet, encontramos que "el primer antecedente de una red de redes, que daría posterior surgimiento al Internet como lo conocemos en la actualidad, se remonta a los años sesenta en Estados Unidos, en el Instituto de Investigaciones de Standford donde se compartían recursos, bajo el contexto de la Guerra Fría, con científicos del Departamento de Defensa de Estados Unidos que crearon a partir de esta iniciativa un proyecto denominado ARPANET (Red de la Agencia de Proyectos de Investigación

[43] Adame Alemán, Juan Pablo. *Op. Cit.,* p. 182.
[44] Shulsky, Abram N. y Schmitt, Gary J. *Silent warfare. Understanding the world of intelligence.* Brasseys, inc. Washington, D.C., 2002, pp 141 y 142. Traducción propia.

Avanzada, por sus siglas en inglés), cuyo objetivo era resguardar la información. A principios de la década de los setenta se financia un protocolo de transferencia de datos (TCP / IP) denominado Internet, mas es hacia mitades de los setenta que la parte científica y militar se separan de este proyecto, dando lugar a otras redes como la comercial *America Online* y es a partir de la década de los noventa, que después de una fase de experimentación las conexiones aumentan popularizando su uso."[45] Pocas veces a lo largo de la historia se ha visto una industria que haya crecido tan rápidamente con lo son ahora las de la información y comunicaciones.

Así, al digitalizar toda nuestra existencia encontramos que "los medios de comunicación que antes estaban separados hoy están convergiendo, y los periódicos impresos producen programas de televisión para sus páginas de internet y los canales de televisión producen contenido escrito para sus sitios web."[46] Demostrando de esta manera que lo más importante es llegar a la mayor cantidad de audiencia posible, atacando desde todos los medios, dado que ya no solo están en el juego de las comunicaciones la radio, la televisión y las computadoras, sino todo tipo de teléfonos móviles y tabletas, de la misma manera que diversos métodos de vigilancia como las cámaras (que se encuentran por doquier, incluso en gafas) o los drones.

De esta manera, podemos considerar que en la sociedad actual "las banderas del Foro Social Mundial, la pobreza, la violencia sexual, el SIDA, el calentamiento global, la expoliación capitalista y el endeudamiento compulsivo de los países […] son preocupaciones que están presentes […] en casi todo el catálogo de sus acciones sociales pero son abordados con otra lógica y con un plus de valor que los distingue vívidamente: la era digital les permite asociarse con empatía, uniendo

[45] Adame Alemán, Juan Pablo. *Op. Cit.,* pp 98 y 99.
[46] Naím, Moisés. *Op. Cit.,* p.310.

lo diverso y lo distante en un territorio nada despreciable, el planeta."[47] Por lo que podemos concluir que el porcentaje de personas comunicándose con otros cuya ubicación está a kilómetros de ellos, va en continuo aumento día tras día. Asimismo, las maneras en que lo hacen se diversifican en igual magnitud haciendo posible intercambiar ideas, estrategias, sentimientos, conocimientos y una increíble cantidad de bienes materiales e inmateriales de los cuales la gente se sirve para crecer profesional o personalmente o, como lo analizaremos en los siguientes apartados, para lograr organizar movimientos sociales, filtrar información delicada y poner en jaque al Estado de diversas maneras en cuestión de segundos.

2.2.1. Redes sociales.

Al presentarse las redes sociales en nuestras vidas, no sólo cambiaron nuestra manera de comunicarnos con seres queridos o de buscar entretenimiento, sino que se convirtieron en un verdadero modo de vida, en una vía de comunicación con personas tanto conocidas como desconocidas, han permitido la creación de grupos con ideas o intereses afines y han modificado por completo nuestra forma de ver el mundo, así como nuestras reacciones y respuestas ante lo que sucede en el mismo.

Siguiendo dicho orden de ideas, Fernando Peirone comenta que "los jóvenes participan de una nueva idea del mundo que se encuentra en su etapa deliberativa; y paradójicamente, aunque no se perciba, esa deliberación se hace a la vista de todos"[48] confirmando que el mundo se vive y se organiza ahora desde las redes y todo lo que sucede en las mismas no se queda ahí. De igual manera, dicho autor cita a Roxana Morduchowicz quien explica la importancia de la participación en

[47] Peirone, Fernando. *Mundo extenso. Ensayo sobre la mutación política global*. Fondo de Cultura Económica, Buenos Aires, 2012, pp. 243 y 244.
[48] *Ibidem*, p. 159

redes sociales y los resultados que se obtienen de la misma:

> En un mundo en el que la producción de saberes es colectiva, el diálogo en red es fundamental […] al participar en las redes sociales, a la vez que se expresan y generan contenidos, los adolescentes se forman cívicamente: descubren la existencia de múltiples perspectivas sobre un mismo tema, aprenden a respetar la pluralidad de opiniones, conocen nuevas normas sociales y comienzan a entender lo que significa negociar entre opiniones contrapuestas. Las redes sociales en internet los orientan en el complejo proceso de deliberación y negociación en la diferencia, cuando se quiere llegar a acuerdos y compromisos.[49]

Con base en esto, se puede considerar que es altamente recomendable que todos los actores políticos, económicos, sociales y de cualquier otra índole se involucren en estas redes ya que permiten dialogar y deliberar con infinidad de personas alrededor del mundo de manera instantánea, lo cual nos permite conocer diferentes puntos de vista. Prácticamente, se podría decir que todos los aspectos de nuestra vida se ven tocados o afectados por el mundo cibernético. De tal manera que, al otorgarle a las redes la importancia que se han ganado, no solo se amplían las oportunidades de la ciudadanía, sino de los propios gobiernos para llevar una relación más cercana con la población.

Bajo el mismo orden de ideas, Lori Andrews ejemplifica dichas oportunidades de la siguiente manera: “Un individuo ordinario puede ser un reportero alertando al mundo con las últimas noticias sobre un desastre natural o una crisis política. O un investigador, ayudando a la policía a resolver un crimen. Cineastas y músicos al comienzo de sus carreras pueden encontrar seguidores a través de las redes sociales. El poder de la gente es explotado en nuevas maneras en las redes

[49] *Idem*

sociales."[50] Al observar cómo ha cambiado el mundo en los últimos años, los movimientos que han surgido y sobre todo el origen que han tenido los mismos, se puede manifestar que la sociedad ha sabido aprovechar el poder antes mencionado - la mayoría de las veces a su favor - ya que es a través de los medios cibernéticos que se puede observar la opinión del grueso de la población. Dado lo cual, se observa a infinidad de individuos siendo partícipes del acontecer político, económico, social, religioso, educativo y prácticamente cualquier aspecto del día a día. Por lo tanto, una decisión viable para los gobiernos alrededor del mundo es adentrarse en dicho mundo y trabajar a partir de lo observado en el mismo.

Ya se han presentado ejemplos de este actuar en los últimos años. Lori Andrews nos menciona algunos: "La Casa Blanca consultó con sus seguidores en Twitter sobre una ley de impuestos. Un oficial del Consejo Económico Nacional (National Economic Council) publicó entonces un blog con ligas a las preguntas que habían planteado los seguidores de Twitter, provocando una discusión sobre la dirección que la política de impuestos debería tomar."[51] Y es gracias a acciones como esta que se puede verdaderamente presentar un mejor ejercicio de la democracia en nuestros días.

De igual manera, el mismo autor hace mención a una medida implementada por la ciudad de San Francisco en la cual, a través de la creación de una red social, los ciudadanos podían tomar fotos de desperfectos en la ciudad y enviarlos directamente a la oficina correspondiente para proceder con la reparación. Asimismo, es a través de esta misma red que personas con habilidades en RCP podrían ofrecerse como voluntarios para apoyar en una emergencia, así, cuando alguien tuviera un ataque al corazón, se reclutarían voluntarios para que se apresuraran a llegar al lugar a prestar su ayuda.

[50] Andrews, Lori. *I know who you are and I saw what you did. Social networks and the death of privacy.* Free Press, New York, 2011, p. 2. Traducción propia.
[51] *Idem*

Pongamos un caso más cercano, a partir de lo observado en la Ciudad de México, el pasado 19 de septiembre de 2017. Ya que la población mexicana tomó acciones como esta en el último gran sismo que sufrió la Ciudad de México, pues comenzaron a organizar a la gente para que fuera a las zonas afectadas que no contaban con el apoyo suficiente, supieran exactamente qué hacía falta para poder llevarlo, así como hacer denuncias de actos reprobables que estaban teniendo lugar en plena emergencia y cómo sortearlos. Actualmente, la ciudadanía despierta y actúa en consecuencia ante cualquier evento importante que suceda y lo hacen de manera inmediata.

De esta manera, vemos que las consecuencias que el gobierno afrontaría al no llevar una buena relación con la población en las redes pueden ser enormes. Esto lo explica Lori Andrews de la siguiente manera: “Cuando la gente se harta de su gobierno, pueden usar Facebook, Twitter y YouTube para incitar a otros a unírseles en las calles para protestar. Mientras formas de protesta política anteriores requerían un líder carismático, el cual podía ser asesinado o su cuartel destruido, es mucho más difícil detener a un grupo ampliamente disperso de antagonistas tales como los ciudadanos de la Nación Facebook”.[52] Es justo este tema el que se analizará en el siguiente apartado al hacer revisión de eventos como la primavera árabe, “Occupy Wall Street” o los indignados de España.

2.2.1.1. Revoluciones digitales: El fenómeno de la manifestación social organizada por internet.

Dentro del mundo cibernético se puede organizar lo que sea, incluyendo manifestaciones para mostrar inconformidad con alguna política implementada, con el resultado de las elecciones, o bien para derrocar gobiernos, tal como lo hicieron varios de los actores que serán mencionados en este apartado.

[52] *Idem*

Tal como lo expresa Juan Pablo Adame refiriéndose a las oportunidades que presentan las Tecnologías de la Información y Comunicaciones (TIC) para la población, tenemos que: "La esperanza en ellas reside en su capacidad para facilitar que el ciudadano se sirva de ellas para ampliar su margen de acción y participación, formar redes sociales y solidaridades compartidas, para debatir ideas y hacer propuestas plurales y novedosas, en fin, para fortalecer su presencia, incidencia y participación en el fortalecimiento de la democracia y el mejoramiento de la sociedad en su conjunto, incluida su forma de gobierno." [53] Sin embargo, para lograr esto, se debe dar mayor acceso a la población a las TIC, a las redes y en general a todos los medios masivos de comunicación utilizados en la actualidad.

Dicha aseveración la sustenta también Juan Pablo Adame al citar a su vez a "Hamelink" en su libro *Ciudadanía digital ¿Oportunidad o amenaza?* donde comenta que estas Tecnologías solo podrán generar movilización social efectiva en cuanto amplíen las oportunidades de los individuos y sean accesibles para todos pues, hasta ahora, sucede que "los que están en mejores condiciones de aprovechar las posibilidades de creación y comunicación en la Internet no son todos los que tienen acceso a una computadora (condición necesaria pero no suficiente), sino los que poseen un "capital informacional" […] la capacidad financiera para pagar la utilización de redes electrónicas y servicios de información, la habilidad técnica para manejar las infraestructuras de estas redes, la capacidad intelectual para filtrar y evaluar información y la habilidad de aplicar información a situaciones sociales".[54] Por otro lado, a esto podemos sumar que los jovenes han sido la mayoría de las veces los protagonistas de los grandes movimientos sociales que han agitado al mundo y esta vez no fueron la excepción. Por lo mismo es que los últimos movimientos han nacido y se han desarrollado en las redes, pues son los jóvenes quienes están más relacionado con estas tecnologías y han permitido que las movilizaciones se originen desde estas nuevas plataformas.

[53] Adame Alemán, Juan Pablo. *Op. Cit.*, p. 122.
[54] "Hamelink, 1995, citado por Winocur, 2004" citado por Adame Alemán, Juan Pablo. *Op. Cit.*, p. 121.

Considerando lo anterior, se puede comprender por qué los jóvenes alrededor del mundo han visto en las redes un gran aliado en todos los aspectos de sus vidas y es ahora también en el rubro de la movilización social donde observamos que estas tecnologías "han potenciado en forma extraordinaria estos procesos, la facilidad de interacción que estas permiten muestran la oportunidad de generar redes de forma más asequible, la difusión instantánea de los mensajes y su efecto multiplicador o viralizador"[55] a través de publicaciones en Facebook, Twitter y demás redes sociales o páginas de internet, las cuales representan grandes ventajas para la población inconforme con sus gobiernos y que además desean actuar de manera inmediata y efectiva cuando se trata de expresar su sentir e ideologías.

Por mencionar un ejemplo, tenemos a Stanley Milgram, profesor de Harvard, quien realizó un experimento en algunas ciudades de Estados Unidos con la finalidad de conocer qué tan conectados estamos como seres humanos con los demás y cual sería nuestra capacidad de asociarnos y organizarnos. En dicho experimento, midió la longitud de conexiones entre las personas y descubrió que nos encontramos a seis grados de separación, es decir, que "cualquier persona puede estar conectada con otra persona del planeta en no más de seis conexiones, situación que en la actualidad puede darse de forma más asidua a partir de una mayor penetración del internet y del nacimiento y auge de las redes sociales que ha contribuido a disminuir las distancias y aumentar la conectividad entre las personas alrededor del mundo."[56] Por lo que no nos sorprendería que ahora los grados de separación sean menores.

De igual manera, encontramos que la comunicación y la toma de decisiones en las redes se ve menos sesgada por otros factores aparte de la verdadera opinión pública, ya que "otro aspecto significativo resulta de la constatación de que los

[55] Adame Alemán, Juan Pablo. *Op. Cit.,* p. 101
[56] *Ibídem,* p. 180.

liderazgos en la red no se dan por medio de elecciones sino a través del mérito y la fuerza argumentativa y el contenido de las aportaciones"[57]. Si bien es cierto que no toda la población puede opinar igual sobre un tema y el lograr llegar a un acuerdo es igual de complicado tanto en las redes como fuera de ellas, al menos podemos conocer las verdaderas opiniones, hacer votaciones reales y expresarnos a través de diversos foros y páginas de una manera más inmediata y llegando a más gente que antes.

A manera de ejemplo, haciendo revisión a lo que se ha investigado referente a los movimientos que han hecho uso del internet para darse a conocer al mundo, organizarse y continuar desarrollándose, se nos menciona que "uno de los primeros […] fue el movimiento zapatista, lo que le permitió posicionarse de inmediato mediáticamente a nivel internacional, ofreciendo su mensaje a nuevas audiencias […] Su actividad en internet consistió en circular información sobre lo que sucedía en Chiapas a través de diversos sitios web, largas listas de correos y apertura de foros virtuales donde podía haber interacción y se recibían denuncias y peticiones de intervención a diversas organizaciones no gubernamentales, se hacían llamados a caravanas de ayuda y apoyo a proyectos, conferencias, protestas, marchas y manifestaciones."[58] De modo que, ya en 1994 podíamos ver la influencia de las redes en los movimientos sociales, sin embargo esto se acentuó con la aparición de las redes cibernéticas en nuestras vidas, como podremos observar en las siguientes protestas ya en el nuevo milenio.

De esta manera fue que nacieron diversos movimientos desde Islandia, avanzando hacia Túnez, Egipto y demás países árabes, los cuales a su vez llegaron a oídos y ojos de España, Estados Unidos y el mundo entero inspirando cada vez a más gente a levantarse contra las injusticias que se vivían en sus respectivos países

[57] *Ibídem,* p. 181.
[58] *Ibídem,* pp 103 y 104.

comenzando por hacerse oír y ver de manera inmediata a través de las redes. Al respecto, Castells nos presenta una completa descripción y análisis de todos estos movimientos en su libro *Redes de indignación y esperanza*, del cual podemos rescatar lo siguiente:

> Ocurrió cuando nadie lo esperaba. En un mundo presa de la crisis económica, el cinismo político, la vaciedad cultural y la desesperanza, simplemente ocurrió. De pronto, la gente derrocaba dictaduras sólo con sus manos, aunque estuvieran cubiertas con la sangre derramada por los caídos. Los magos de las finanzas pasaron de ser objeto de envidia pública a objetivo del desprecio universal. Los políticos quedaron en evidencia como corruptos y mentirosos. Se denunció a los gobiernos. Los medios de comunicación se hicieron sospechosos. La confianza se desvaneció. Y la confianza es lo que cohesiona a una sociedad, al mercado y a las instituciones. […] Sin confianza, el contrato social se disuelve y la sociedad desaparece, transformándose en individuos a la defensiva que luchan por sobrevivir. [59]

Con base en esto, observamos que uno de los primeros movimientos desarrollados en las redes, fue originado en octubre de 2008 por el cantante Hordur Torfason en Islandia. Al respecto Castells nos relata que "se plantó con su guitarra delante del edificio del Althing (el parlamento islandés) en Reikiavik y cantó su rabia contra los <<banksters>> y los políticos sumisos. Se le unieron unas cuantas personas. Alguien grabó la escena y la subió a Internet. En unos días, cientos y luego miles de personas manifestaban su protesta en la histórica plaza Austurvollur." [60] Después de esto, las protestas se intensificaron, tanto en el mundo cibernético como en las calles. Cabe mencionar que al contar el 94% de los islandeses con conexión a Internet y dos tercios con una cuenta de Facebook, el papel de estos fue decisivo en las movilizaciones.

---

[59] Castells, Manuel. *Redes de indignación y esperanza. Los movimientos sociales en la era de internet*. Alianza Editorial, Madrid, 2012, p. 19.
[60] *Ibídem*, pp 49 y 50.

Entre lo que los manifestantes solicitaban se encontraba:

1. La dimisión del gobierno y celebración de elecciones.
2. La refundación de la República (no subordinada a la élite financiera)
3. La redacción de una nueva constitución.

En las elecciones se derrotó a los dos grandes partidos conservadores que habían gobernado al país desde 1927 y se formó una nueva coalición con los socialdemócratas y los <<verdirojos>>, que subieron al poder el 1 de febrero de 2009. El nuevo gobierno se dispuso a trabajar en tres frentes: "limpiar el embrollo financiero y exigir responsabilidades por la gestión fraudulenta de la economía; restablecer el crecimiento económico transformando el modelo económico, estableciendo normas financieras estrictas y reforzando las instituciones de supervisión y, responder a la demanda popular iniciando un proceso de reforma constitucional con la participación de los ciudadanos." [61] Algunos incluso le llamaron a esta propuesta la "WikiConstitución" pues se valieron de diferentes medios electrónicos para consultar con la población, debatir y deliberar al respecto. Con dicho fin, se utilizó Facebook para debatir; Twitter, para informar sobre los avances y contestar dudas; YouTube y Flickr, para tener comunicación directa entre los ciudadanos y los miembros del consejo, así como para los debates que se realizaron a lo largo de toda Islandia. [62] Cabe mencionar que este trabajo se llevó a cabo en tan solo cuatro meses, por lo que a pesar de que Islandia tiene tan solo 334,252 habitantes (2016) se puede desmentir la idea de la ineficacia de la democracia participativa. No obstante, existen varios factores a considerar aparte de la población, puesto que tendríamos que implementar este método en países con diferentes condiciones, en todos los aspectos, para medir los resultados.

[61] *Ibídem,* pp 50 - 52.
[62] *Ibídem,* pp 54.

Por otra parte, considerando la “revolución de los jazmines” en Túnez con la cual se derrocó al régimen de Ben Ali quien gobernaba en el país desde 1987, podremos ver el poder que tuvieron las redes sociales para influir en toda una región que compartía casi el mismo descontento con sus gobiernos. En este movimiento de finales del año 2010 y principios de 2011, presenciamos las siguientes características distintivas:

1. La existencia de un grupo activo de licenciados en paro que lideraron la revuelta, obviando cualquier liderazgo tradicional o formal.
2. La presencia de una sólida cultura de ciberactivismo que llevaba más de una década haciendo una crítica abierta del régimen.
3. Una tasa relativamente alta de difusión del uso de Internet incluyendo conexiones domésticas, en colegios y cibercafés. [63]

Así, se puede observar que Islandia y Túnez fueron una referencia tan importante para movimientos como la “Primavera árabe”, “Occupy Wall Street” o “Los Indignados” en España, por solo mencionar algunos; dado que en la primera manifestación en la Plaza Tahrir de El Cairo se modificó la frase “El Islam es la solución” que se había utilizado en previas movilizaciones en el mundo árabe por “Túnez es la solución” pues al igual que en dicho país se perseguía el derrocamiento del régimen que había permanecido por décadas en el poder. Asimismo, las indignadas españolas proclamaban “Islandia es la solución” por ser el referente europeo más reciente de un profundo cambio en la sociedad. De la misma manera, después de las manifestaciones en Egipto, se bautizó al primer campamento próximo a Wall Street como “Tahrir Square” en honor a la Plaza bajo el mismo nombre del país árabe.

[63] *Ibídem,* p 45.

De esta manera, nos podemos dar cuenta de que todos estos países, a pesar de ser completamente diferentes, fueron capaces de transformar a sus instituciones y convertirse en un modelo a seguir para los movimientos que sacudieron al mundo posteriormente.

2.2.1.2. Su significado mediático en la política internacional.

Vivimos en una época de constante innovación. Las tecnologías de comienzos de siglo, parecen mucho más viejas y vemos que no pasa ni medio año que sale a la venta un nuevo celular, computadora o cualquier aparato electrónico, cuando ya se encuentran sacando el siguiente modelo.

A pesar de todo esto, existe un ámbito crucial en nuestras vidas que no se ha visto modificado en gran medida: la manera en que nos gobernamos o las maneras de intervenir como individuos en el proceso político. “Hoy, las campañas electorales se apoyan en métodos de persuasión más sofisticados y, por supuesto, más gente que nunca vive gobernada por un líder al que ha elegido y no por un dictador. Pero estos cambios, aunque bienvenidos, no son nada en comparación con las extraordinarias transformaciones en las comunicaciones, la medicina, los negocios, la filantropía, la ciencia o la guerra.”[64] Por esto es que los ciudadanos deben aprender de lo leído, observado o escuchado sobre los movimientos sociales de los últimos años, generados desde las redes sociales y en general, sobre los nuevos medios de comunicación electrónicos, para así descubrir la utilidad de la inteligencia colectiva y con esto consolidar la democracia en la que viven desde un nuevo ámbito, el cual será utilizado cada vez más para dicho fin: las redes cibernéticas.

[64] Naím, Moisés. *Op. Cit.*. P. 354.

Por esto es que Juan Pablo Adame nos menciona que “en la medida en que el ciudadano descubra la utilidad de la inteligencia colectiva, podrá enriquecer su participación y su papel en la consolidación de la democracia; al final existe una correspondencia innegable entre la calidad del compromiso y la participación ciudadana con la calidad de su gobierno.”[65] Por lo tanto, podemos observar que el cambio de mentalidad que está generando estos cambios es derivado de la nueva forma de ver el mundo que nuestra generación posee, lo cual Moisés Naím nos explica como las revoluciones del *más* y de la *movilidad*: el efecto de estas en nuestras vidas “ha sido una inmensa expansión del impacto cognitivo e incluso emocional del hecho de tener más acceso a los recursos y la capacidad de moverse, aprender, conectarse y comunicarse en un ámbito mayor y de forma más barata que nunca. Es inevitable que ese hecho agudice las diferencias generacionales de mentalidad y visión del mundo.”[66] Basándonos en esto, vemos que hoy en día, es posible buscar de manera inmediata el significado de alguna palabra, un hecho histórico que desconozcamos o las últimas noticias a través del internet e incluso se logra sólo “hablándole” al celular y solicitando busque por nosotros específicamente lo que necesitamos saber.

Ahora bien, es claro que no todas las naciones han logrado aprovechar estos nuevos métodos de comunicación y de utilización del poder ciudadano en un nuevo ámbito, e inclusive, en las naciones donde se ha visto con mayor frecuencia, vemos también que no toda la población lo sabe llevar a cabo. No obstante, es abrumadora la manera en que estas cifras van en constante aumento y que las naciones que antes no tenían un gran peso político, tienen ahora la posibilidad de influir cada vez más en los foros internacionales.

[65] Adame Alemán, Juan Pablo. *Op. Cit.,* pp 189 y 190.
[66] Naím, Moisés. *Op. Cit.,* P. 105.

De igual manera, Fernando Peirone nos explica que el territorio de acción de las personas alrededor del mundo no se limita a sus localidades, ni siquiera a sus países, sino que ahora su accionar tiene consecuencias globales: “Cuando los jóvenes tunecinos, después de la caída de Ben Alí, les escribían a los egipcios en sus twitters << Lo logramos, también ustedes pueden hacerlo >>, estaban asumiendo: 1) que comparten un territorio mucho más amplio que el de sus países de origen; 2) que las ideas o los derechos por los que estaban luchando eran los mismos para cualquier gentilicio y 3) que sus acciones trascienden los límites y los controles nacionales”[67] Así, vemos que los jóvenes y, de hecho cualquier persona que aprenda a hacer uso correcto de lo que el mundo cibernético le ofrece y entienda el papel que tiene en el mundo, pueden estar conscientes del alcance planetario que tienen sus acciones. Ahora su idea de lo político no se encuentra en las naciones o en los territorios que antes se disputaban los gobernantes, sino que el mundo entero es su campo de batalla y el lugar donde tienen la posibilidad de desplegar su accionar.

Ahora también, no es casualidad que la Primavera árabe haya comenzado en Túnez, puesto que dicho país es uno de los que mejor desempeño económico han tenido en el norte de África y que ha sabido posicionar a los pobres dentro de la clase media. Y es de hecho, la clase media la que por excelencia, está mejor informada y se encuentra más impaciente de ver avances antes de que el gobierno siquiera tenga oportunidad de explicarles lo que tiene para ofrecerles. Es entonces dicha intolerancia la que les ha permitido posicionarse como una importante oposición, convirtiéndose en el motor de las transformaciones políticas de nuestros tiempos.

A manera de contraste, si nos remontamos entre 30 y 40 años atrás a la retirada de los jóvenes revolucionarios de los 60’s – 70’s y la entrada del período neoliberal,

[67] Peirone, Fernando. *Op. Cit.*, p. 228.

nadie hubiera imaginado que un recurso que originalmente había sido pensado para defenderse, como lo era la Internet, más bien iba a poner al descubierto las debilidades del mismo sistema. Esto ha sido posible dado que "la irrupción de las nuevas tecnologías suministró la posibilidad de una interacción social sin precedentes, acentuando los rasgos de un proceso contracultural que a pesar de las muchas razones que lo asistían parecía en estado de hibernación. Fueron un detonante que puso en marcha un prolongado efecto dominó que por su cualidad multinodal y multimodal se volvió ingobernable."[68] Por lo que aparte de considerar a los jóvenes y a la clase media como factores importantes en los cambios sociales que se avecinan, debemos tomar en cuenta todo lo que el resto de la población tiene la posibilidad de observar y publicar en la red.

Es derivado de esto que Pierre Lévy hace mención a una especie de "ingeniería del vínculo social" la cual "se convierte en un arte de mantener colectivos inteligentes y de valorizar al máximo la diversidad de las cualidades humanas"[69] esto se puede llevar a cabo a través de la globalización del conocimiento con ayuda de las publicaciones de toda suerte de saberes en Internet, al alcance de todos y a bajo costo, sino es que gratis en ciertos lugares que cuentan con redes abiertas. De esta manera, se puede contener el ejercicio excesivo del poder y permitir el engrandecimiento de las potencialidades del talento humano para contribuir a resolver los problemas de la sociedad. Si bien se dice que dos cabezas piensan mejor que una, sólo es cuestión de imaginar lo que aproximadamente siete mil millones de cabezas pueden pensar.

Al aplicar esto a la política, nos encontramos ejemplos como el que narra Lori Andrews referente a cuando David Cameron se convirtió en Primer Ministro del Reino Unido y acordó una cita con otro jefe de estado un tanto peculiar: Mark

[68] *Ibídem*, p. 143.
[69] Adame Alemán, Juan Pablo. *Op. Cit.*, p. 182.

Zuckerberg. Sí, el fundador de Facebook. Respecto a esta aseveración, no hay nada más acertado, ya que se ha dicho que si Facebook fuera un país, sería el tercero con la mayor población tan solo después de China y la India, cada uno con más de mil millones de habitantes. Ahora, referente a la reunión mencionada previamente, Cameron le explicó a Zuckerberg los problemas financieros por los que atravesaba el país, a lo que el fundador de la red social recomendó usar a Facebook como una herramienta para incrementar la participación pública en el proceso político permitiendo incluso disminuir costos: "Toda esta gente tiene ideas grandiosas y un montón de energía que quieren aportar y pienso que para mucha gente solo es cuestión de tener un medio fácil y económico para comunicar sus ideas."[70] A lo cual Cameron atinó a comentar: "Brillante". Y no solo las redes sociales más populares pueden permitir tal comunicación entre gobierno y sociedad, sino que toda la gama de TICs tienen un valor estratégico ante el imperativo de cerrar la brecha entre las necesidades de la población y la manera en que son escuchadas y atendidas.

A manera de conclusión, vemos que el valor que tuvieron los movimientos sociales mencionados en el apartado anterior es que mostraron el desencanto de toda la población, pero sobre todo de la juventud y la renuencia de dicha generación a hacer uso de las vías tradicionales para negociar con el Estado. Ante este panorama, Moisés Naím argumenta que aunque no podemos aseverar que actores tan diversos como las organizaciones no gubernamentales, las iglesias, los terroristas, las asociaciones de inmigrantes, empresas privadas, inversores, entre muchos otros que tienen ahora la capacidad de hacerse escuchar a través de las redes, hayan dejado obsoletos a ejércitos, embajadores y gobernantes, pero sí han limitado lo que estos pueden hacer y se han permitido influir en la agenda internacional a través de los nuevos medios electrónicos.

[70] Andrews, Lori. *Op. Cit.,* p. 1

Asimismo, Juan Pablo Adame nos explica que "la reinvención del gobierno implica plantear un modelo de gobernabilidad donde la democracia se traduzca en la canalización de las demandas más que en la provisión de servicios, en la que se redefina la relación entre gobernantes y gobernados."[71] Por lo que se requerirán liderazgos frescos que en lugar de hacer menos a los gobernados, estén dispuestos a hacer alianza con ellos, además de que las instituciones actuales deberán mostrarse más flexibles y dispuestas al constante cambio que representa vivir en este mundo, pues no será posible continuar haciendo las cosas de la manera en que se acostumbraba y mucho menos quitarle a la población los medios con los que cuentan ahora para organizarse y manifestar sus opiniones sin que esto ocasione la mayor revuelta de nuestros tiempos.

2.3. El papel del Estado ante el mundo cibernético.

Para comenzar este apartado, introduzco algunas palabras expresadas por Hernán Casciari en una entrevista titulada *Más respeto que soy tu crisis* en donde pronuncia su sentir respecto al "viejo mundo":

> Cuando Casciari oye hablar de piratería, ley SOPA o ley SINDE, dice y sin tapujos: "Escucho al del noticiero decir esas palabras y enseguida me da sueño. Estoy convencido de que el cuerpo de todo ese mundo ya está muerto, los que hablan son los gusanos […] No hay que luchar contra el mundo viejo, ni siquiera hay que debatir con él. Hay que dejarlo morir en paz, sin molestarlo. No tenemos que ver al mundo viejo como aquel padre castrador que fue en sus buenos tiempos, sino como un abuelito con Alzheimer […] No hay que luchar contra el viejo mundo, sino divertirse, porque ese es su peor escarmiento."[72]

[71] Adame Alemán, Juan Pablo. *Op. Cit.,* p. 67
[72] Casciari, Hernán. "Más respeto que soy tu crisis" (entrevista) en suplemento *Radar,* 19 de febrero de 2012, p. 12.

Considerando lo anterior, conviene subrayar que a partir de aseveraciones como esta, se pueden formar mil y un opiniones a favor o en contra, sin embargo, es válido detenernos un momento a pensar en qué mundo vivimos, cómo nosotros mismos y los demás lo percibimos, cómo podemos cambiar las cosas y qué valores pueden quedarse y cuáles no. En otra entrevista, Casciari expresa que "el mundo nuevo se basa en confianza, generosidad, libertad de acción, creatividad, pasión y entrega. Todo lo que ocurra por fuera y por dentro de sus parámetros es bueno, en tanto la gente disfrute con la cultura, pagando o sin pagar."[73] Muy diferente del viejo mundo que nada o poco permitía a las personas si no contaban con los recursos suficientes.

De igual manera, Rop Gonggrijp nos da una opinión a tomar en cuenta sobre la situación que están pasando y sobrellevando los políticos y sus gabinetes con este nuevo mundo: "La mayoría de los políticos actuales se da cuenta de que ninguna de las personas que tienen en sus ministerios, como cualquiera de sus costosos consultores, puede decirles qué está pasando. Tienen un timón en las manos sin saber a dónde se dirigen. Nuestros líderes intentan tranquilizarnos diciéndonos que el barco sin duda logrará sortear la creciente tormenta. Pero si uno presta atención, verá que están poniendo a resguardo sus riquezas o que están yendo sigilosamente hacia los botes salvavidas."[74] Esto dado que la sociedad actual -la cual ha sido definida con diversos términos como "la cultura digital" por parte de Pierre Lévy, "la era de la información" por Manuel Castells o bien, "la sociedad conexionista" por Fernando Peirone- se encuentra atravesando por un proceso que este último autor define como "socialización divergente" a través de la cual podemos percatarnos de que la configuración social ya no puede limitarse a las fuerzas de poder que antes la regían, ya que el mundo se ha vuelto más moderno e interconectado y estas relaciones de poder deben actualizarse a la par, de lo contrario el Estado sufrirá las consecuencias.

[73] Casciari, Hernán. *Para ti, Lucía*. 21 de diciembre de 2011. Disponible en línea: http://orsai.bitacoras.com
[74] Gonggrijp, Rop. Discurso de apertura al 27° Congreso de Chaos Computer Club (CCC), Berlín, 27 de diciembre de 2010. Disponible en línea: http://rop.gonggri.jp/?p=438

Con respecto a la "socialización divergente" mencionada previamente, Peirone nos explica que existe una "estructura social en red en la que cada ciudadano del mundo se encuentra en situación de intervenir. Eso es la socialización divergente: un constructo social que - *de facto* - interpela lo dado y abre el juego a una nueva ciudadanía que refiere cada vez menos a una dimensión nacional y cada vez más a una dimensión planetaria."[75] Este tipo de política planetaria hace que aún las cuestiones locales tengan una dimensión y respuesta mucho mayor, dado que la cercanía ya no se refiere a distancias exclusivamente, sino a compartir puntos de vista u opiniones, sin importar el lugar en el mundo donde se encuentre la otra persona (si es que se trata de una persona) y respecto a la respuesta que debe tener el Estado ante estas nuevas maneras de hacer política, el autor refiere más adelante que el poder es algo que ya no se puede obtener por medio de armas, poder blando, poder duro ni ninguno de los métodos que se conocían hasta hace algunos años. Es tiempo de una reconfiguración de la política dentro del mundo interconectado y digital en el que vivimos.

De esta manera, se hace necesario que la denominada sociedad de la información realmente reciba la información que precisa para un buen ejercicio del régimen democrático en que vive o bien, para alcanzar el mismo. Asimismo, vemos que esta sociedad ha impuesto nuevas condiciones en cuanto a la economía y política de la mayoría de las naciones del mundo, puesto que la incorporación de la tecnología a nuestras vidas implica un replanteamiento de los procesos que siguen las organizaciones, las empresas y el gobierno para poder adaptarse a los cambios que se experimentan diariamente.

Por otro lado, vemos que cada vez hay una mayor desconfianza en los gobiernos electos, lo cual demanda ajustes a la democracia como la vivimos hoy en día, situación que "apremia la necesidad de difusión del poder hacia los actores no

[75] Peirone, Fernando. *Op. Cit.*, p. 211.

estatales, y en este aspecto el Internet se muestra como la alternativa a una buena parte de la población para el acceso a la información"[76]. Así pues, el Estado se ve obligado a mantener una relación de mayor apertura y transparencia con los gobernados puesto que el flujo de la información en Internet y otros medios nuevos, cada día aumenta y se renueva constantemente por lo que ya no es opción ocultar información. La ciudadanía digital y el gobierno abierto deben convertirse en una realidad para todas las naciones, sobre todo, para las que se hacen llamar democráticas, tal como lo aseveraba Sir Claus Moser desde el año 1980, ahora citado por Frank Webster:

> Las diferentes comunidades no solo tienen el derecho a recibir la información recolectada con los fondos públicos; es, en cualquier caso, una parte esencial para una sociedad democrática y del gobierno abierto que la información disponible debería ser ampliamente circulada y, uno esperaría, usada.[77]

Sin embargo, lo que el Estado teme naturalmente es el cambio drástico en las relaciones de poder que esta apertura traería consigo, pero es un riesgo que ya no se puede evitar; al contrario, se corre más peligro ocultando la información esencial a la población.

Así, vemos que al contar con dicha información se puede hacer realidad una frase mencionada por el antiguo consejero de seguridad nacional de los Estados Unidos, Zbigniew Brzezinski, quien al cavilar sobre los cambios que el nuevo orden mundial está siendo partícipe, comentó "Hoy es infinitamente más fácil matar a un millón de personas que controlarlas"[78]. Basándome en esta última frase, considero que nada podría ser más cierto, pues es bien sabido que a diario mueren miles de personas

[76] Adame Alemán, Juan Pablo. *Op. Cit.*, p. 69.
[77] Moser, Claus, 1980, p.4. Citado por Webster, Frank en *Theories of the information society*, segunda edición, Routledge, Londres, 2002, p. 187. Traducción propia.
[78] Naím, Moisés. *Op. Cit.*. P. 95.

alrededor del mundo como resultado de guerras, pequeños enfrentamientos entre la sociedad civil o contra los actores estatales, delincuencia y crimen organizado, enfermedades, falta de alimento y diversas necesidades básicas, pero pocas personas reparan en las enormes cantidades que de esto resultan. No obstante, es cuestión de segundos para que cierta “injusticia” en específico comience a tener respuesta en los medios de comunicación, redes sociales y que incluso, antes de que los causantes tengan la más mínima oportunidad de redactar algún comunicado al respecto, el tema ya se encuentre en boca de todos. Es de dicha inmediatez de la cual se deben cuidar no solo el Estado, sino todos los que gobiernan este mundo, como las grandes empresas y organizaciones.

2.3.1. Sociedad red y seguridad del Estado en un mundo interconectado.

Hasta hace algunos años, la mayor parte de la información que obteníamos llegaba a nuestros ojos y oídos después de haber pasado varios filtros del gobierno, los servicios de inteligencia y seguridad nacional o bien, las grandes empresas. No obstante, en los últimos años, el empoderamiento de la población - sin importar su nivel económico, educacional ni algún otro aspecto - a través de las ya mencionadas TIC’s, en particular en las redes sociales y los blogs en Internet han demostrado que se puede desestabilizar al Estado y aunque no constituyen en sí un poder instituyente como lo tenemos actualmente con los gobiernos alrededor del mundo, sí son la manifestación de un descontento generalizado que tarde o temprano puede convertirse en una alternativa, buena o mala, pero eso habrá que verlo para juzgarlo.

Como resultado de la libertad de expresión y la posibilidad de conseguir cualquier clase de información a través de los nuevos medios de comunicación, los servicios de seguridad nacional e inteligencia han tenido que trabajar para que sus métodos de obtención, publicación y manejo de información sean más eficaces y eficientes,

al igual que en los perfiles de los colaboradores que contratan, para así poder hacerle frente a varias amenazas actuales desde ataques (o posibles / futuros ataques) cibernéticos, filtración de información importante para el gobierno, así como la desacreditación que la población o los medios de comunicación puedan hacer de los mismos cuerpos de inteligencia.

De igual manera, se enfrentan a la cuestión de que "mientras una extraordinaria cantidad de trabajo ha sido destinada a desarrollar herramientas para el análisis, estas son generalmente ignoradas por los analistas a menos que sean fáciles de aprender y de usar, y que incrementen la cantidad de tiempo que tienen para pensar"[79] y a pesar de que esta sea una solicitud completamente normal para los integrantes de los cuerpos de inteligencia de cualquier nación, debido a la enorme carga de trabajo que pueden tener diariamente, sí debe haber un cambio de actitud en los mismos para efectivamente aceptar las nuevas alternativas que la tecnología ofrece para hacer dicho trabajo más sencillo, pues el mundo evoluciona a pasos agigantados y todos lo debemos hacer si queremos evitar ser rebasados por él.

Como resultado del aumento en el uso de las redes sociales para todo aspecto de la vida cotidiana, la milicia estadounidense comenzó a darse cuenta de los problemas que podría ocasionarles. Es por esto que el ejército estadounidense introdujo cambios importantes en sus procesos internos aproximadamente entre los años 2009 y 2010, al observar que varias organizaciones terroristas o grupos extremistas enemigos estaban haciendo uso de las redes sociales para publicar información operacional, detalles acerca del uso de armas y explosivos, así como recetas para fabricarlos, incluso en varios idiomas; y todo esto de manera pública, sin necesidad de hacerse amigo o "fan" de los grupos. Todo esto llevó a los altos mandos a inquietarse sobre los peligros que representaban las redes sociales para

[79] Berkowitz, Peter (ed.) *The future of american intelligence*. Hoover Institution Press, California, 2005, p. 171. Traducción Propia.

su propia seguridad y la de sus soldados, ya que si pueden ver la información publicada por sus enemigos y usarla a su favor, significa que estos también pueden seguir los pasos y adelantarse a los planes del ejército estadounidense tan solo siguiéndolos en Facebook u otras redes sociales.

Por esto, es que optaron por negarle a los soldados estadounidenses el uso de redes sociales. Sin embargo, esto ocasionó bajas, puesto que ya es lo suficientemente difícil que se enlisten de manera voluntaria, y esto disminuye aún más si los privan de los medios que tienen para comunicarse con amigos y familiares. En consecuencia, se creó una red privada para el ejército de E.E.U.U. llamada NIPRNET (Non-classified Internet Protocol Router Network) la cual les permite transmitirse información clasificada internamente de manera enrutada y segura. Esta red privada es la más grande del mundo y puede ser utilizada en zonas de guerra, en vehículos, aviones u otros medios de transporte militar.[80]

Ahora bien, hay otro aspecto que causa gran controversia: es respecto a la relación que se mantiene entre la protección de la privacidad de la población y la información que el Estado puede exigir izando la bandera de la seguridad nacional. Dicho tema siempre ha tenido cierto tinte de ambigüedad puesto que, históricamente, el acceso a información para los cuerpos de inteligencia a través de tecnología más y más sofisticada es controlado y manejado en una base de "necesidad de saber" (need-to-know). Sin embargo, como bien lo menciona Peter Berkowitz: "En un mundo de amenazas terroristas, uno puede no saber a quién tiene que conocer"[81] por lo que se ha dado un aumento en la intrusión de los cuerpos de seguridad e inteligencia en la privacidad de la gente a través de sus redes sociales, principalmente. O en todo caso, se ha dado a conocer este tema últimamente, aunque tenga más tiempo de llevarse a cabo.

[80] Andrews, Lori. *Op. Cit.,* p. 3. (Parafraseado y traducción propia)
[81] Berkowitz, Peter (ed.) *Op. Cit.*, p. 154. Traducción propia.

2.3.1.1. El “Big Brother” Orwelliano aplicado: Vigilancia de la población.

Actualmente, vivimos en un mundo más abierto y mejor comunicado, pero también con un precio que no muchos esperaban: la pérdida de la privacidad, sobre todo en cuanto a los datos más importantes para cada quien, como pueden ser resultados médicos, números de tarjetas de crédito o inclusive nuestra ubicación en todo momento. Lori Andrews lo expone de la siguiente manera: “A diferencia de en una democracia, Facebook está redefiniendo unilateralmente el contrato social – Haciendo lo privado ahora público y haciendo lo público ahora privado. Información privada sobre la gente está inmediatamente disponible a terceros…Puedes pensar que estás publicando información solo a miembros de tu familia, pero con un modesto cambio en un código de computadora, Facebook puede enviar esa información a cualquier lugar”[82]. Ahora bien, si actualmente nos sentimos con mayor comodidad de compartir más información sobre nosotros que se podría considerar privada o delicada, o con mucha más gente que como se acostumbraba en otras épocas, no quiere decir que queramos que la policía, los bancos o alguien que no conocemos se enteren también. Hay ciertos límites que aún en nuestros días se tienen que seguir respetando y eso es algo que gente como Mark Zuckerberg (fundador de Facebook) no ha terminado de comprender.

Al hacer este tipo de aseveraciones, uno puede sonar paranoico, extremista o como si todo fuera una gran conspiración salida de un libro de ciencia ficción. Sin embargo, hay ciertas razones para creer que sí pueden estarse dando este tipo de acciones entre los creadores de las redes sociales y las grandes empresas o el gobierno, para precisamente aprovechar las nuevas herramientas que se utilizan hoy en día a su favor. Hay mucha gente que considera que el acceso de terceros a su información personal es un pequeño precio que tienen que pagar por el uso de la red social, sin embargo no por esos pocos van a pagar todos los que sí consideran importante conservar su privacidad, o al menos cierto nivel de ella.

[82] Andrews, Lori. *Op. Cit.,* p. 5. Traducción propia

Actualmente, una segunda versión de nosotros se está creando en Internet basada en nuestras búsquedas en línea, la información que publicamos en redes sociales e incluso los datos enviados a seres queridos, conocidos o colegas de manera "personalizada o privada" sin que nosotros estemos conscientes de ello. Se puede ver cómo ahora las cortes de justicia, los reclutadores o bancos hacen uso de las nuevas tecnologías para determinar si obtienes un trabajo, un préstamo o incluso la custodia de tus hijos tomando como referencia lo que publicas en redes sociales, cuando se supone que eso debería ser algo privado, o bien, entre nuestros seres queridos y nosotros.

Este fenómeno se puede explicar observando cómo los proveedores de programas de inspección profunda de paquetes (deep packet inspection) defienden estos últimos diciendo que se usan para detectar ataques electrónicos, administrar el congestionamiento de la red o cobrar diferentes precios para diferentes servicios de internet. No obstante, algunas empresas de marketing comportamental han contratado estas "ISPs" para espiar y copiar lo que los usuarios envían a través de "compiladores de datos" (data aggregators).

Son, entonces, dichos compiladores de datos quienes "reciben los paquetes de información de las transmisiones que hace una persona y analiza el contenido para crear un perfil de los comportamientos en línea e intereses de la persona. Después puede vender esa información y análisis a otros, incluyendo publicistas que crean anuncios personalizados basados en los perfiles de comportamiento de dichas personas."[83] Es así como cada que entramos a Facebook o cualquier otra página en internet, aparecen varios anuncios relacionados con el último viaje que planeamos o las búsquedas que hicimos al respecto, con la música que hemos escuchado más recientemente o incluso relacionados con nuestros intereses políticos o de otros rubros.

[83] *Ibídem,* p. 25. Traducción propia.

En relación con este tipo de comportamientos intrusivos de empresas y gobierno a las vidas de la gente en internet, el senador Pat Leahy se pronunció de la siguiente manera:

> No es asunto de nadie lo que Oliver North o Robert Bork o Griffin Bell o Pat Leahy ven en la televisión o leen o piensan cuando están en casa… En una era de cables de televisión interactiva, de aumento en los check-in y check-out computarizados, de sistemas de seguridad y teléfonos, todo ubicado en computadoras, sería relativamente fácil en algún momento dar un perfil de una persona y saber qué compran en la tienda, qué tipo de comida les gusta, qué tipo de programas de televisión ven y quienes son algunas de las personas a quienes llaman… Pienso que eso es incorrecto. Creo que realmente ese es el Big Brother y creo que eso es algo de lo que nos tenemos que cuidar.[84]

Por consiguiente, vemos que la idea orwelliana antes vista como ciencia ficción, ahora bien puede ser una realidad contra la cual no tenemos ni defensas suficientes por parte de gobernantes ni legistas, así como alguna escapatoria, salvo la reclusión o aislamiento en uno mismo, sin publicar nada, sin llamar a nadie y alejándose de todo tipo de tecnologías, situación casi imposible en nuestros días. Y la idea no es generar miedo en la gente, sino consciencia de lo que está pasando e incentivarla a exigir mayor respeto y protección al respecto.

2.3.1.2. El control de la red y sus límites.

Para terminar este capítulo, se intentará introducir al lector en la disyuntiva que se genera entre gobierno y población respecto al uso apropiado o ético que se le debe dar a la nueva herramienta de nuestros días: las tecnologías de información y

[84] *Ibídem,* p. 54. Traducción propia

comunicación (TICs). Muchos argumentan que el gobierno debe poder hacer uso de las mismas para monitorear a sus enemigos y adelantarse a posibles amenazas, pero que también debe estar regulado dicho monitoreo porque de lo contrario puede resultar en violaciones de la privacidad de las personas a diestra y siniestra. Vemos así que, "por una parte, los individuos están perdiendo la noción de la exposición a la que están sometidos, y por otra los gobiernos se ven rebasados por la velocidad del cambio tecnológico que los desafía en un espacio de naturaleza pública, pero que origina situaciones en las que se necesita de la intervención para marcar pautas en la interacción y uso."[85] Por lo que, si los individuos se muestran más preocupados por publicar en sus redes sociales y conseguir más aplicaciones en sus teléfonos sin detenerse a pensar un poco en la información que están brindando y cómo esta puede ser utilizada en su contra, sin antes exigir las debidas medidas tanto a empresas como a autoridades para hacer respetar su privacidad, no llegaremos muy lejos antes de que la ficción nos alcance por completo.

Muchos consideran a Facebook como una nación debido a la gran población que tiene una cuenta en la red social, entonces si la empezaremos a considerar como tal, ¿no debería también contar con una especie de constitución o reglamentación que no sólo beneficie a la empresa si no a los más de mil millones de usuarios que la utilizan? Es el tipo de preguntas que surgen cuando se discute la regulación del internet. Respecto a ese tema, "no olvidemos que la intención del Departamento de Estados Unidos al momento de concebir Internet (Arpanet) fue justamente sostener las comunicaciones en caso de cualquier intento de control y sabotaje […] Es una herramienta […] que representa una gran autonomía y una capacidad de articulación e intervención sin antecedentes, tanta que ni sus propios creadores pueden ya desactivarla o destruirla. De allí que los…gobiernos, a pesar de su necesidad de control, aun no hayan conseguido dominarla."[86] Así, podemos decir

[85] Adame Alemán, Juan Pablo. *Op. Cit.,* p. 111.
[86] Peirone, Fernando. *Op. Cit.*, p. 127.

que se trata de una situación muy delicada, difícil de explicar y controlar por ambas partes (gobierno y población) sin embargo se debe poner sobre la mesa de discusión y llegar a acuerdos e incluso, leyes que ni coarten la libertad de expresión y publicación de información útil a varios, así como ciertos permisos al Estado para hacer uso de dicha herramienta con fines políticos y de seguridad (comprobables).

Hay diversas formas de controlar o regular el Internet, tales como "la privatización del servicio y limitar el acceso, incluso la misma gestión de la información pues en la práctica consigue su unificación en el espacio virtual, por ello vale la pena hacer una distinción entre regulación y censura" esto ya que "se visualiza al ciberespacio también como la promesa de espacio abierto, libre y alterno." [87] Es por esto que los intentos de controlar, limitar o definitivamente negar el ingreso a internet durante revoluciones o manifestaciones en varios lugares del mundo, como ya se ha mencionado, es una idea que habría que pensar dos veces, pues al contrario de servir al gobierno para que el exterior no se entere de asuntos internos, o cualquiera que sea la razón que ha orillado a ciertos políticos a tomar dicha medida, esto no hace más que afectar la opinión pública e internacional que se tiene del mismo. Esto ya que internet se ha vuelto algo, como tal, incontrolable y que de una u otra manera llegará a la gente para que hagan uso de él.

Ahora, lo que los gobiernos tienen que hacer es fluir con los avances en lugar de resistirse al proceso y aunque es muy importante poner en discusión la gobernanza en internet para lograr cierta institucionalización en un mundo inmenso de libertades, no se pueden coartar los derechos digitales, por lo que también es vital comenzar a definirlos para respetarlos.

[87] Adame Alemán, Juan Pablo. *Op. Cit.,* p. 112.

2.3.1.2.1. Leyes.

A manera de ejemplo, para introducir el tema de la creación o revisión de leyes para la regulación de Internet, haré mención de una previa investigación respecto a las nuevas tecnologías y su relación con la privacidad de la gente, la cual fue realizada en el año 1889 por los abogados Samuel Warren y Louis Brandeis, resultado de la llegada de la cámara portátil a las vidas de los ciudadanos estadounidenses:

> Antes de 1888, cuando Kodak introdujo la cámara portátil, tomar la fotografía de alguien era todo un trámite. La persona se arreglaba e iba a un estudio. Las fotos no eran tomadas sin el consentimiento de la persona. Pero la cámara portátil cambió todo eso…Warren y Brandeis comenzaron a evaluar el impacto de la cámara portátil en la vida moderna. Sugirieron que la gente ya no tenía el derecho de que los dejaran en paz porque las tecnologías podían ahora rastrear y registrar lo que hacían. En cambio, notaban que la intrusión de las tecnologías hacía aún más importante para las personas mantener el control sobre la información acerca de ellos mismos.[88]

Desde entonces, esta inquietud entre la relación tecnología – privacidad ha rondado el pensamiento de la población alrededor del mundo, por lo que nos encontramos con la necesidad constante de crear leyes o reglas que nos brinden cierta protección, pues el uso de las tecnologías para fines intrusivos avanza a un paso mucho más rápido que aquel de las legislaciones para protegernos contra los mismos. Así fue cómo en su tiempo, "Warren y Brandeis se inclinaron hacia ciertos valores constitucionales fundamentales, como el derecho a rehusarse a testificar contra uno mismo, y principios comunes de la ley, como el derecho a determinar…hasta qué extensión sus pensamientos, sentimientos y emociones serán comunicados a otros. Decían que estos derechos no dependían de la

[88] Andrews, Lori. *Op. Cit.,* pp. 49 y 50. Traducción propia.

adopción de algún método particular de expresión."[89] Por lo tanto, no importa el método que utilicemos para expresar nuestra manera de pensar y sentir a cierta(s) persona(s) ya que si nuestro deseo es que solo ellos se enteren de la misma, no hay razón para que alguien externo viole nuestra privacidad y se entere también, cuando nadie se lo estaba permitiendo.

Como resultado de las discusiones e investigaciones que Warren y Brandeis comenzaron, se publicó posteriormente su artículo "El derecho a la privacidad" en 1890 en *The Harvard Law Review* y "sus ideas fueron incorporadas a la ley a través de la creación de cuatro acciones legales diferentes acerca de la invasión de la privacidad: por entrometerse en la reclusión de alguien, por hacer públicos hechos embarazosos, por poner a alguien en una situación falsa o engañosa ante la opinión pública, y por apropiarse del nombre o intereses de alguien para uso comercial. La información y fotos de alguien puede ser distribuida si la gente así lo ha consentido o el asunto es legítimamente de interés público."[90] De esta manera, se logra que dichas acciones se puedan juzgar como legales o ilegales, y puede uno pensar que queda todo un poco ambiguo o que existe la posibilidad de que aparezcan huecos legales de los cuales los "culpables", por así llamarlos, se valdrían para librarse del problema y hacerlo ver como algo legal. No obstante, el hecho de tener un precedente de ley de protección a la privacidad haciendo referencia a la intrusión mediante el uso de las nuevas tecnologías, marca una pauta válida para continuar sobre ese camino y crear más leyes al respecto.

Ahora bien, revisando un tema más actual siguiendo la misma línea, vemos que en febrero de 2016 se lograron establecer ciertos límites a la obtención arbitraria de datos de ciudadanos europeos por parte de Estados Unidos. Se nos informó que en dicho mes "tras alcanzar…un nuevo pacto de intercambio de información…Una

[89] *Ibídem,* p. 50. Traducción propia
[90] *Idem*

explicación clara sobre qué información puede ser utilizada, para evitar su uso "indiscriminado" y "arbitrario", fue una condición clave del nuevo marco de protección de privacidad que permite a las empresas transferir fácilmente información personal hacia Estados Unidos…Washington acordó crear una nueva función específica dentro del Departamento de Estado para hacer frente a los reclamos y consultas enviadas por los organismos de protección de datos de la Unión Europea."[91] Y es que mientras más se den cuenta los países y sus ciudadanos de la intrusión tan exhaustiva y muchas veces innecesaria en la que incurren grandes potencias como Estados Unidos, sin el previo consentimiento de dicha invasión de la privacidad, más se va a buscar la creación de leyes para la protección de los datos y mientras más se violen dichas leyes, más conflictos internacionales se generarán.

En pocas palabras, no por la falta de familiaridad con las nuevas tecnologías, la ignorancia de cómo funcionan o la intimidación que se genera ante el crecimiento sin precedentes que tienen las mismas, se va a detener la creación de estatutos legales que protejan la privacidad que tantas tecnologías hoy en día están pasando por alto, lo cual afecta no solo al ciudadano común y corriente, sino a organizaciones, a grupos de choque, a activistas, a periodistas, e incluso, a los altos mandos del gobierno. Es un tema que nos compete a todos y en el que todos debemos aportar ideas y opiniones.

2.3.1.2.2. Compañías.

Ahora bien, respecto a las compañías que se ven involucradas en la cuestión tecnología vs privacidad, nos podemos referir a las redes sociales, principalmente. Y como lo haríamos con cualquier nueva nación, debemos cuestionarnos qué

[91] Reuters. "Ponen límites a espionaje a europeos" en *El Universal,* domingo 28 de febrero de 2016, sección Mundo, p. 27.

principios deberían gobernar en las mismas "¿acaso los principios sobre los que Estados Unidos y otras democracias fueron fundados aún resuenan en la gente? ¿Podrían ellos proveernos una guía para la gobernanza de las redes sociales?"[92] Así, muchos se han preguntado si debería haber una constitución para las mismas, dado que no hay que pensarla como un conjunto de reglas fijas y rígidas, sino como un referente, una expresión de valores fundamentales que nos servirán para juzgar actividades en las redes sociales de manera adecuada, o menos arbitraria que ahora.

A manera de ejemplo, podemos mencionar a Cynthia Moreno, una estudiante de preparatoria en Coalinga, California, quien escribió en su muro de *MySpace* (red social lanzada en 2003 que fue popular por algunos años) que su ciudad era aburrida y banal, lo cual uno pensaría que es una simple manera de expresar una opinión, sin embargo, la aseveración llegó a oídos del director de su escuela, quien hizo que se escribiera una nota al respecto en el *Coalinga Record*. Dicho acto le trajo varios enemigos a Cynthia y a su familia, a quienes incluso amenazaban de muerte y los instaban a abandonar la ciudad de inmediato. La familia pudo llevar el caso a juicio después de haber sido rechazados por docenas de abogados. Finalmente, un abogado aceptó llevar el caso y demandó al periódico por "inflicción intencional de angustia emocional" y por "invasión de la privacidad".[93]

Ante este tipo de situaciones, las Cortes están abandonando su responsabilidad de defender a las personas por el uso indebido (y sin su previo consentimiento) de las publicaciones que hacen en redes sociales. Lo que argumentan es que no se puede esperar que se respete la privacidad en Internet pues nada de lo que hay en red está seguro de los hackers o un "compilador de datos". No obstante, decir que no puedes esperar privacidad en la red, es como decir que si sabes que hay

[92] Andrews, Lori. *Op. Cit.,* p. 14. Traducción propia
[93] *Ibídem,* p. 56. Traducción propia.

voyeristas en el mundo no puedes tener una ventana en tu casa sin que haya alguien que se asome o que si en cierto vecindario las violaciones son algo recurrente, una mujer no puede esperar estar libre de dicho peligro.

Con el fin de ayudarnos a comprender mejor las situaciones que se viven en el día a día en red, que afectan directa o indirectamente a los usuarios, mencionaré dos ejemplos más:

> La Corte de Apelación de París confirmó… que la justicia francesa es competente para juzgar el conflicto que enfrenta a un usuario vs Facebook, empresa que aseveró que sólo debía rendir cuentas a la justicia de Estados Unidos… Facebook se amparó en que así está especificado en una cláusula que los usuarios aceptan para convertirse en miembros de la popular red… El caso se remonta a 2011 cuando el demandante, un ciudadano francés, llevó a la compañía estadounidense a los tribunales galos después de que esta vetara el reportaje - imagen incluida - que había colgado en su cuenta sobre el cuadro "El origen del mundo", que muestra el sexo de una mujer… Stéphane Cottineau, abogado del demandante, se felicitó por el nuevo respaldo de la justicia gala, que en su opinión sienta jurisprudencia de cara a futuras demandas a empresas con sede en Estados Unidos. El letrado confió en que la justicia francesa pueda pronunciarse ahora sobre la confusión de Facebook entre pornografía y obra de arte, a su juicio, y sobre la libertad de expresión en las redes sociales.[94]

A través de esta noticia, nos damos cuenta del alcance global que tiene Facebook y cómo en países fuera de Estados Unidos están demandando a la empresa por falta de criterio y por no respetar la libre expresión de los usuarios, puesto que por amplia y diversa que esta pueda ser, no le corresponde a la empresa ni a otros

[94] Notimex y EFE. "Francia podrá juzgar a Facebook por censura" en *El Universal,* Sección Mundo, 13 de febrero de 2016, p. 30.

usuarios juzgarla, a menos, quizá que sea abiertamente incriminatoria u ofensiva, sin previa advertencia.

Otra noticia que nos ayuda a pintar el panorama de las redes sociales, ahora en la vida política es la siguiente:

> Si algo caracteriza a Jaime Rodríguez Calderón, *El Bronco*, es su presencia en redes sociales. A cuatro meses de gobierno, reitera que es su forma de mantenerse cercano a la gente… Desde su campaña, el gobernador apostó fuerte por Internet y es por ese medio donde da a conocer sus mensajes más importantes y atiende las dudas de los ciudadanos… Sin embargo, la mañana del 11 de febrero, la matanza en el penal *Topo Chico* lo tomó por sorpresa y las reacciones de los internautas vieron primero la luz antes que cualquier publicación o llamada suya… Los tuiteros no perdonaron al gobernador: a las pocas horas surgió la etiqueta #InutilComoElBronco, donde se popularizó la frase "El Bronco no fue bronco ante conflicto en Topo Chico". El hashtag permaneció por más de seis horas en la red social y generó un millón 653,987 impresiones entre tuits y retuits generados por un millón 373,414 usuarios.[95]

Dichos datos duros son representación de lo que ya se comentaba acerca del poder de las redes sociales para hacer denuncias instantáneas y la enorme capacidad que tienen para llegar a millones de personas en cuestión de segundos. Situación que los políticos y su gabinete deben tener muy presente en todo momento pues una simple publicación puede arruinar el trabajo de meses o, incluso, años.

[95] Jiménez, María Fernanda. "Redes, arma de doble filo para El Bronco" en *El Universal*, sección Estados, 14 de febrero de 2016, p. 22.

Como conclusión del apartado, podemos mencionar lo siguiente acerca de lo que una constitución de las Redes Sociales puede hacer por nuestra sociedad: Esta "debe ser flexible y reconocer los principios básicos que nunca deberíamos pasar por alto. Se dirigirían a las acciones de las agencias del gobierno, instituciones sociales y la sociedad, en general. Toda nación democrática tiene principios que la gobiernan acerca de los derechos que los ciudadanos tienen respecto a la privacidad, la vida y la libertad. Los ciudadanos de la Nación Facebook no merecen menos."[96] Algunos de los puntos mencionados por Lori Andrews para dicha Constitución serían:

1. El derecho a conectarse.
2. El derecho al libre discurso y la libertad de expresión.
3. El derecho a la privacidad respecto a la ubicación y la información.
4. El derecho a la privacidad respecto a pensamientos, emociones y sentimientos.
5. El derecho a controlar la imagen de uno mismo.
6. El derecho a un juicio justo.
7. El derecho a un jurado no corrompido.
8. El derecho al debido proceso legal y el derecho de notificación.
9. No discriminación.
10. Libertad de asociación.[97]

Por lo tanto, la discusión acerca de la regulación de las redes sociales ya comenzó y parece que continuará hasta que tanto usuarios como poderes judicial, legislativo y ejecutivo estén satisfechos y bajo común acuerdo al respecto.

[96] Andrews, Lori *Op. Cit.,* p. 15. Traducción propia.
[97] *Ibídem,* pp. 189-191. Traducción propia.

2.3.1.2.3. Hackers.

Para comprender por qué se quiere controlar también la actividad de los hackers alrededor del mundo, se debe uno poner en la posición de los afectados, ya que por seguir una ideología política, hay muchas personas que a través del llamado "Hacktivismo" hacen uso de las herramientas tecnológicas o las crean con fines políticos o sociales, que muchas veces resultan contraproducentes para el Estado.

Por otro lado, habría que diferenciar entre hackers maliciosos y hackers defensores de la cultura libre, la libertad de expresión y del derecho a recibir información oportuna. Esto se puede ver reflejado en lo que Richard Stallman explica como *software* privativo y *software* libre; el primero lo describe como un sistema social no ético y que cobra con tal de recibir sus beneficios, en cambio, del segundo dice que garantiza la libertad de ejecutar el programa de la manera que uno desee, el acceso al código fuente y la libertad de distribuir copias. Concluye describiendo al *software* libre como "un sistema ético, basado en el respeto de las libertades personales y sociales."[98] Un buen ejemplo de los que buscan generar mejores condiciones para el uso libre y colectivo de las herramientas tecnológicas, es el joven George Hotz cuando "a los 17 años descubrió cómo se podía desbloquear su iPhone y después de filmar la operación la colgó en Internet, para que cualquier habitante del mundo pudiera desbloquear el celular de Apple y usarlo con el chip de la compañía telefónica que le plazca. O como…cuando logró desventrar y hackear la Play Station 3, uno de los tres modelos de consolas de videojuegos que controlan el mercado, para que pueda ser utilizada con juegos no exclusivos, piratas o descargados de internet"[99] y ninguna de estas veces, lo hizo George para conseguir retribución económica alguna, simplemente por compartir lo que sabía, lo que había logrado conseguir y quería que más y más gente pudiera hacer uso de ello para disfrutar de la cultura libre.

[98] Op. Cit. Por Peirone, Fernando en *Mundo extenso*: Stallman, Richard. Conferencia. Disponible en http://commons.wikimedia.org/wiki/File:200908251217-Richard_Stallman-Pre_Wikimania.ogg
[99] Peirone, Fernando. *Op. Cit.*, pp. 208 y 209.

De igual manera, tomemos como ejemplo de participación ciudadana a los llamados "hackatones" (palabra formada por hacker y maratón), término que se refiere al "desarrollo de aplicaciones y software libres sobre cierta temática social en un espacio y lapso de tiempo determinados"[100] los cuales son principalmente iniciativas de organizaciones civiles en conjunto con universidades o centros de investigación. Asimismo, ha emergido una nueva tendencia entre la ciudadanía, la cual es el "hacking cívico, mediante el cual se hace uso de las herramientas informáticas en el procesamiento de la información con la finalidad de crear soluciones tecnológicas que atiendan problemas de la ciudadanía."[101] Esto corresponde con lo que ya se mencionaba respecto de la búsqueda de respuestas haciendo uso de la tecnología para resolver problemas políticos, económicos, sociales y de diversos ámbitos que vive la gente a diario en todo el mundo.

Pongamos por caso de este tipo de actividad a México, con la convocatoria realizada por la organización "Codeando México" en la cual se retaba a varios programadores a hacer una aplicación de menor costo a la que ya existía para la Cámara de Diputados, la cual se licitó en marzo de 2013 por 115 millones de pesos. Como resultado de dicha convocatoria, se obtuvieron 130 propuestas que representaban una alternativa de costo mucho menor que la original. El lanzamiento de esta y otra convocatoria por parte del Sistema de Administración Tributaria (SAT) confirmaron que existe talento en nuestro país para desarrollar este tipo de proyectos, por lo que el gobierno debe mostrarse más abierto a los mismos y permitirle a la ciudadanía facilitar muchos procesos que los actores gubernamentales actuales no han podido.

No obstante, resulta conveniente tomar en cuenta que así como esta cultura libre puede hacer que el poder de la gente sea cada vez mayor y sus oportunidades en

[100] Adame Alemán, Juan Pablo. *Op. Cit.,* p. 186.
[101] *Ibídem*, p. 185.

todo ámbito mejoren considerablemente, también presenta un foco rojo para el Estado, ya que con la aparición de grupos hacktivistas como *Anonymous* e incluso WikiLeaks previamente, o derivado de las acciones de Edward Snowden que resultaban poco convenientes para los gobernantes alrededor del mundo, esta puede ser la excusa perfecta para limitar el *software* libre, el acceso a la información y el control general del Internet. Así pues, existen opiniones en contra de WikiLeaks, por ejemplo, que consideran ha rebasado la línea de lo permitido y así ha puesto en peligro la libertad de todos los demás en la red, tal como lo expresa Pablo García-Mexía:

> WikiLeaks le ha hecho un gran perjuicio al Internet al sobrepasar los límites de lo que uno puede y debería razonablemente publicar en línea. Hasta ahora, el Internet ha operado sobre las bases de neutralidad de la red, o extremadamente baja regulación o interferencia externa. La situación de WikiLeaks le permite credibilidad a aquellos que quisieran cambiar eso, y puede ser la excusa que algunos gobiernos han esperado para intervenir y finalmente regular el Internet.[102]

En capítulos siguientes se hará un análisis más profundo de esta situación, no obstante, considero que de entrada no se debe culpar por las medidas restrictivas que buscan los gobiernos imponer, a aquellos que solo buscaban develar la verdad, brindarle información y medios a la gente para actuar en consecuencia y no solo de acuerdo a lo que los altos mandos quieren que sepamos. Sin embargo, es claro que dichas acciones fueron un parteaguas para muchos y hay que estar preparados para la serie de constantes cambios que vendrán en la sociedad internacional y las fuerzas de poder que se mueven en la misma.

[102] García-Mexía, Pablo. "WikiLeaks is an abuse of Internet Freedom" en Tamara Thompson (ed.) *WikiLeaks*, Greenhaven Press, Estados Unidos, 2013, p. 50.

Capítulo 3
La Guerra Cibernética en Estados Unidos

3.1. Ataques cibernéticos

3.1.1. Los cuatro pilares de la guerra cibernética

3.1.2. Los primeros conflictos cibernéticos y los puntos geográficos más álgidos

3.1.3. Ataques dirigidos a Estados Unidos

3.1.3.1. Estados Unidos y sus principales contrincantes en la guerra cibernética.

3.1.3.2. Respuesta del gobierno de Obama a los ataques

3.1.4. Preparación cibernética en distintos gobiernos dentro del panorama actual

3.1. Ataques cibernéticos.

Mientras que en el pasado, el Estado y sus sistemas de inteligencia debían hacerse de caros y sofisticados instrumentos para llevar a cabo las guerras que, a largo plazo, les brindarían más poder sobre los otros países, ahora "la revolución de la información, internet, el ciberespionaje, *Big Data* y tecnologías de escucha e interceptación ya sean sofisticadas o muy asequibles, permiten a muchos países tener sus propias ventajas para competir internacionalmente."[103] El poder ahora se está degradando, es más difícil de conseguir y mucho más fácil de perder; y más ahora que los avances de la tecnología permiten a mucha más gente, grupos extremistas e incluso, a los niveles más altos del gobierno, atacar a otros sin necesidad de medios difíciles de adquirir como en los conflictos de antaño.

[103] Naím, Moisés. *Op. Cit.,* p. 201.

Es por esto que a varios analistas de las relaciones internacionales, se les complica asimilar al mundo cibernético como un nuevo actor a considerar, ya que ahora los oponentes en los conflictos pueden no ser Estados necesariamente, sino grupos étnicos, religiosos, terroristas o de cualquier índole. Por lo tanto, es observando los acontecimientos de cada día y los avances tecnológicos que uno puede llegar a comprender sobre ataques cibernéticos, el avance de las técnicas en los mismos, así como las medidas a tomar en cuenta para hacerles frente.

Ahora bien, cabe mencionar que el crimen cibernético es diferente del espionaje cibernético, ya que mientras el primero toma la información que roba de internet con fines delictivos, el segundo está más enfocado en temas delicados para los actores principales en un conflicto. Si bien, es cierto que las defensas pueden ser las mismas para ambos, las razones que los originan son diferentes.

Así, vemos que "el objetivo del espionaje es información que tiene valor para el atacante. Puede ser inteligencia militar como los movimientos de las tropas, la logística y el despliegue de misiles… Puede ser información diplomática como las intenciones en un Tratado. Puede ser información militar – industrial como diseño de navíos o misiles."[104] Para fines de esta tesis, consideraremos más los ataques cibernéticos encaminados al espionaje cibernético y filtración de información delicada para los gobiernos alrededor del mundo, haciendo énfasis en Estados Unidos.

Con respecto al proceso que siguen los espías actuales, cuyos instrumentos de trabajo ahora son las computadoras, los virus informáticos, los dispositivos de almacenamiento de datos (USB) y todo lo que las nuevas tecnologías de la información nos permiten utilizar, Richard Stiennon explica que:

[104] Stiennon, Richard. *Surviving cyberwar*. The scarecrow press, inc., Estados Unidos de América, 2010, p. 20.

> Como primer paso, el "Sr. Espía" trabaja a partir de una lista de blancos u objetivos. Explora sus sitios web y comienza a sondear sus servidores externos… Cuando encuentra un enrutador (router), servidor de correo electrónico o aplicación que es vulnerable, obtiene acceso e incluso llega a tener los privilegios que tiene… un administrador interno. Roba cualquier información que existe en esa máquina y procede a instalar software de escaneo que le permitirá encontrar blancos adicionales dentro de esa red…Podrían ser comunicaciones militares, transferencias electrónicas del personal, o la laptop del director general. Instala programas de espionaje que graban todo lo que se escribe en el teclado, roba archivos, e incluso enciende el micrófono y la cámara de la laptop. Procede a guardar nombres de usuarios y contraseñas…Todos los documentos, diseños, planes, información financiera, procesos e información termina en manos de una operación de inteligencia ajena.[105]

A manera de ejemplo, se puede mencionar el *phishing*, el cual consiste en el envío de correos electrónicos, que aparentan ser legítimos hacia organizaciones o personas que son el objetivo para la realización de algún fraude o acto malicioso. Una vez que el receptor del correo, abre la página que menciona el mismo o abre algún archivo adjunto, este resulta ser un virus que roba la información del dispositivo y le puede brindar el control al atacante como si fuera el administrador, por lo que puede proceder a hacer un uso malicioso de la información o incluso comenzar a enviar correos electrónicos como si fueran internos o legítimos, pero con mensajes falsos o con más virus, comprometiendo de esta manera a la organización entera.

Por ejemplo, vemos que en el año 2003, los bancos de Estambul notaron un aumento en el robo de las cuentas. Después de las investigaciones, salió a la luz

[105] *Ibídem,* p. 21.

que ladrones cibernéticos estaban instalando software malicioso en los cafés internet para robar esta información.[106] A pesar de que parece un ejemplo un poco antiguo, es algo que continúa ocurriendo, pues hay muchas veces que no es tanto que no protejamos nuestra computadora, sino que el robo de información ocurre por errores humanos, como dejar los dispositivos desbloqueados, compartir contraseñas con gente que no es de confianza, o bien, ignorando todos los ejemplos que se han escuchado de fraudes de todo tipo basándonos en la idea de "a mí no me va a pasar", situación en la que incluso los gobernantes y los sistemas de inteligencia pueden caer y, por lo tanto, deben cuidarse más.

Sin embargo, cabe mencionar la importancia de "educar" a toda la población respecto a la seguridad informática, ya que muchos de estos bienes no están bajo control gubernamental. La preparación cibernética es más difícil de conceptualizar que las cuestiones de defensa o el reconocimiento satelital. Y ¿cómo pueden el gobierno y sus instituciones e infraestructuras estar realmente preparados para un ataque, si no es a través de la educación cibernética?

3.1.1. Los cuatro pilares de la guerra cibernética.

Richard Stiennon explica que dichos pilares deben ser debidamente manejados por las naciones para ocuparse de los conflictos que los ataques cibernéticos puedan traerles. Los divide de la siguiente manera:

INTELIGENCIA.

La efectiva recopilación de información provee a un país ventajas en muchos aspectos respecto a armas (pueden incluso copiar la tecnología ahorrándose el

[106] *Ibídem,* pp 109 y 110.

gasto en investigación), cuestiones económicas o militares, al obtener la información de la gente que trabaja en una organización, cifras sobre despliegues, disposición de recursos y la preparación que tiene el adversario[107]…Son tres los pasos a seguir para una operación de ciberespionaje efectiva:

1. Reconocimiento: De los bienes del objetivo. Este paso requiere actividad continua, ya que los bienes se modifican constantemente, pues los servidores, bases de datos y redes son actualizados a diario.
2. Consecución: Es la ejecución de un ataque contra un objetivo identificado con el propósito de reunir información. Pueden obtener planes militares, correspondencia diplomática, diseño de armas e incluso datos económicos.
3. Análisis: La información muchas veces debe ser traducida, interpretada, evaluada y convertida en una forma útil para finalmente, entregarla al departamento de la organización que puede hacer uso de ella.[108]

TECNOLOGÍA.

Una operación de guerra cibernética efectiva debe incluir un equipo que descubra las vulnerabilidades y desarrolle metodologías de ataque, las cuales deben ser fáciles de ejecutar y difíciles de descubrir. También se debe considerar el uso de diferentes herramientas por muchos operativos, la recolección de datos y el control de los programas, incluso - y quizá con mayor razón - después del ataque. Por otro lado, también se deben desarrollar virus, gusanos, *Trojan horses* y todo tipo de software malicioso, el cual debe ser actualizado constantemente si se desea llevar a cabo una operación exitosa. De igual manera, el análisis forma parte importante del pilar tecnológico.[109]

[107] *Ibídem*, p. 117. Traducción propia
[108] *Ibídem*, pp 120 y 121. Paráfrasis y traducción propia.
[109] *Ibídem*, pp 122-125. Paráfrasis y traducción propia.

LOGISTICA.

Tal como en una guerra convencional, en la cual sin cadenas de suministro y flujo eficiente de armas, comida, reservas, combustible y demás, la posibilidad de continuar sería imposible; por lo que al recibir un ataque informático, la organización debe contar con varias alternativas para continuar su funcionamiento. La logística cibernética lidia con las redes y la capacidad de lanzar un ataque, al mismo tiempo que defiende sus redes, las cuales podrían verse comprometidas en un ataque, ya que el control y defensa de los enrutadores que proveen conectividad de Internet es crítico tanto para las acciones de ofensa y defensa de cualquier nación.[110]

COMANDO Y CONTROL.

Al ser la infraestructura de comunicación uno de los principales blancos en la guerra cibernética, debe ser uno de los aspectos más protegidos por las naciones, así como uno de los objetivos principales de aquellos que quieran atacar a otro. Desarrollar la capacidad de defender los canales de comando y control de algún ataque cibernético debería ser el centro de atención de la preparación cibernética de cualquier nación o, para el caso, cualquier organización que suponga estar bajo un ataque de esta índole.[111]

3.1.2. Los primeros conflictos cibernéticos y los puntos geográficos más álgidos.

Durante las últimas décadas, el concepto tradicional de guerra ha experimentado varios cambios derivados de la inserción de la tecnología en nuestras vidas, por lo

[110] *Ibídem*, pp 127 y 128. Paráfrasis y traducción propia.
[111] *Ibídem*, p. 130. Traducción propia.

que ahora es posible trasladar los enfrentamientos a un nuevo escenario: el ciberespacio. Así, vemos que cada vez más estudiosos de las relaciones internacionales, o bien, gente involucrada en la política de los países, intentan definir a dicho actor y así realizar mejores análisis y pronósticos del porvenir de la sociedad internacional: "De acuerdo con el experto en seguridad Richard A. Clarke, la ciberguerra se define […] como el conjunto de acciones llevadas a cabo por un Estado nación para infiltrarse en las computadoras o redes de otro, con el objetivo de generar un daño."[112] De esta manera, podemos comprender el desarrollo de las primeras guerras cibernéticas desde sus inicios hasta la envergadura que han alcanzado al día de hoy.

En particular, podemos hacer mención de los ataques que Georgia recibió en varias páginas de bancos, ministerios del gobierno y blogs de noticias durante el conflicto con Rusia de 2008 por la independencia de dos regiones al norte de Georgia: Abjasia y Osetia del Sur, las cuales recibían el apoyo de Rusia derivado de las intenciones de Georgia de integrarse a la OTAN. Los ataques cibernéticos comenzaron incluso antes de los daños físicos de agosto puesto que "el 20 de julio de 2008, la *ShadowServer Foundation*, una organización de investigación independiente, documentó un ataque cuidadosamente orquestado contra la página presidencial de Saakashvili. Observaron que un *botnet*[113] nunca antes visto llamado Machbot se estaba comunicando con un servidor de comando y control en Estados Unidos para obtener instrucciones para el ataque de Negación de servicio (DoS: *Denial of service*) […] Los efectos, independientemente de quien ejecutó los ataques, eran inhabilitar los sitios electrónicos que Georgia utilizaba para comunicarse con su pueblo y el mundo."[114] En consecuencia, Saakashvili quien era

[112] Vargas Aguilar, Simón. "Guerra cibernética: la nueva amenaza" en *La Jornada*, México, Sección Opinión, 5 de julio de 2013. Recuperado de: http://www.jornada.unam.mx/2013/07/05/opinion/018a2pol Consultado el 06 de marzo de 2018.
[113] *Botnet*: Es un término que hace referencia a un conjunto o red de "robots informáticos" o "bots", que se ejecutan de manera autónoma y automática. Consultado en: https://www.linguee.es/espanol-ingles/search?source=ingles&query=botnet el 06 de marzo de 2018.
[114] Stiennon, Richard. *Op. Cit.*, pp 96 y 97. Traducción propia.

adepto a usar sus sitios web para presentar su caso al mundo y así recibir apoyo en su lucha contra la hegemonía rusa, se vio imposibilitado de usar dicho recurso y, finalmente, cuando estalló la guerra su voz fue silenciada.

Posteriormente, al hacer el recuento de los daños, vemos que las organizaciones afectadas por estos ataques fueron: "Embajadas de Estados Unidos y el Reino Unido en Tiflis; el Parlamento, la Suprema Corte y el Ministerio de Relaciones Exteriores de Georgia; varias fuentes de periódicos, televisión y otros medios; la Comisión Central de Elecciones; e incluso un blog de noticias."[115] En consecuencia, todas las naciones comenzaron a prepararse en el aspecto tecnológico y de protección de sus redes, ya que a partir de entonces se entendió que cualquier conflicto podría incluir ataques cibernéticos, así que si estas naciones continúan confiando su comercio, la comunicación con sus ciudadanos y la mayoría de los aspectos de la vida política, económica y social interna, se verán de igual manera obligados a implementar defensas cada vez más efectivas para su seguridad cibernética.

Esta última aseveración, la podemos confirmar a través del ataque que sufrió Irán en 2011 con el virus *Stuxnet* del cual informó "el comandante iraní Gholamreza Jalali, director de defensa civil, que la compañía Siemens proporcionó información sobre los códigos de la aplicación SCADA (Control de Supervisión y Adquisición de Datos), utilizada para operar maquinaria industrial"[116] cuestión que efectivamente derivó en problemas para dicho país puesto que "dañó mil centrifugadoras usadas para la purificación de uranio, causó varias explosiones e infectó computadoras del

[115] *Ibídem*, p. 98. Traducción propia.
[116] Reuters. "Irán acusa a Siemens de ataque cibernético" en *La Jornada en línea*, Sección Mundo, 18 de abril de 2011, Recuperado de: http://www.jornada.unam.mx/2011/04/18/mundo/027n1mun Consultado el 21 de febrero de 2018.

reactor nuclear de Bushehr, así como 30 mil computadoras en todo el país."[117] Dicho ataque puede ser considerado como uno de los daños más grandes que se habían visto hasta entonces ocasionados por medios electrónicos, lo cual comenzó a preocupar a muchas naciones en todo el mundo.

Por otra parte, en lo que respecta a las naciones tecnológicamente desarrolladas y que también representan puntos geopolíticos álgidos podemos encontrar en el Medio Oriente a Israel, país avanzado en cuestiones tecnológicas y de redes, que es igualmente el centro de una guerra de ideologías y un área a considerar para los avances en guerra cibernética. Un poco más al este podemos también detenernos en Irán, el cual siempre ha sido foco de atención del mundo debido al desarrollo y refinamiento de sus armas nucleares. Bastante cerca de Irán, también se encuentran Pakistán e India, dos países contendientes que son miembros de los países que cuentan con armas nucleares y que, a su vez, han logrado desarrollar sus redes y liderar en el ámbito de la tecnología. Finalmente, en el lejano oriente, tenemos la constante lucha entre las dos Coreas (Corea del Norte también en pugna con Estados Unidos), así como Rusia y China que no escatiman esfuerzos para competir con la hegemonía estadounidense en todos los ámbitos posibles.

No obstante, no está de más continuar al pendiente de los desarrollos tecnológicos que logren las demás naciones del globo para agregarlos a la lista de posibles contendientes en la guerra cibernética, así como también considerar que un ataque puede parecer provenir de una computadora o algún dispositivo en un punto específico del mundo, sin tratarse por ello de un ataque de dicha nación sino de un individuo que puede ser un extranjero que se encuentra realizando el ataque desde ese país en lugar del suyo. Por lo tanto, aún se necesitan muchas pautas para lograr encontrar a los verdaderos culpables de un ataque de este tipo, lo cual

[117] Vargas Aguilar, Simón. "Guerra cibernética: la nueva amenaza" en *La Jornada*, Mexico, Sección Opinión, 5 de julio de 2013. Recuperado de: http://www.jornada.unam.mx/2013/07/05/opinion/018a2pol Consultado el 06 de marzo de 2018

representa un mayor reto para aquellos que deseamos analizar las consecuencias de los mismos en las relaciones internacionales.

3.1.3. Ataques dirigidos a Estados Unidos.

La seguridad cibernética es un tema no sólo primordial sino estratégico en nuestros días, y aquel país, empresa o individuo que no cumpla con las recomendaciones se atiene a las consecuencias que esto puede traer consigo. Así, vemos que desde el Departamento de Seguridad Interior se informaba que las agresiones cibernéticas contra redes de computadoras del gobierno estadounidense eran algo común e indicaban que en 2008 hubo 5499 ataques, más que los 3928 de 2007. Algunos años después estas cifras aumentaron exponencialmente ya que, a nivel mundial, tan solo en 2015 los delitos informáticos incrementaron un 65 por ciento con relación al año anterior. Dentro de ellos, a Estados Unidos le correspondieron fraudes cibernéticos que representaron pérdidas por 15 mil millones de dólares en el mismo año, derivados del robo de identidad de 13 millones de ciudadanos. [118] Y eso que corresponde únicamente a fraudes cibernéticos, no a toda la gama de ciberataques que en todo el mundo representan pérdidas que se estiman entre 375 mil y 575 mil millones de dólares.[119] Estas son las cifras que han puesto en tela de juicio el verdadero control que tienen sobre su información todos los que poseen artículos electrónicos, sobre todo con conexión a internet, no sólo ciudadanos, empresarios o periodistas, sino también los funcionarios del gobierno e incluso los regentes de un país.

[118] Sánchez Jiménez, Arturo. "Al alza, ataques cibernéticos, alerta académico" en La Jornada en línea, Sección Política, domingo 5 de febrero de 2017, Recuperado de: http://www.jornada.unam.mx/2017/02/05/politica/009n2pol Consultado el 21 de febrero de 2018. (Parafraseo)

[119] Posada García, Miriam. "Se logró contener unos 170 mil ataques cibernéticos contra el Estado: funcionario" en La Jornada en línea, Sección Economía, Jueves 8 de septiembre de 2016, Recuperado de: http://www.jornada.unam.mx/2016/09/08/economia/022n1eco Consultado el 21 de febrero de 2018.

Como ejemplos de este tipo de ataques contra Estados Unidos nos podemos remontar a uno que se dio en 2001-2002, cuando "Gary McKennon logró intervenir más de 100 computadoras en el Pentágono y otros lugares usando simples herramientas para adivinar contraseñas."[120] Él clamaba estar buscando pruebas del ejército de Estados Unidos sobre interacciones con alienígenas y tuvo éxito en su búsqueda, lo cual demuestra los bajos niveles de seguridad que tenían las agencias de inteligencia de dicha nación a principios de este siglo. De igual manera, con el fin de comprender cómo han aumentado y se han diversificado este tipo de ataques con el paso del tiempo, podemos mencionar de manera breve los siguientes casos:

> En febrero de 2005, un ataque a Bank of America que afectó a 1,2 millones de cuentas dio comienzo a la escalada. Desde entonces, bancos, tiendas, universidades, aseguradoras y centros sanitarios se han convertido en el blanco favorito de los atacantes. En junio Citigroup veía cómo accedían a los datos de 3,9 millones de ficheros.
>
> Sony es uno de los objetivos preferidos. En abril de 2011 su plataforma de juego online quedó inutilizada durante varias semanas. En 2013 se dio el mayor ataque hasta entonces contra los supermercados Target. Se desvelaron datos sensibles de sus clientes como tarjetas de crédito, correos, direcciones físicas y contraseñas. En 2014, además de los estudios de Sony, JP Morgan y Home Depot han visto cómo sus datos dejaban de ser secretos. En 2015, la empresa especializada en seguros de salud Blue Cross ostentaba el dudoso honor de contar con el ataque más notable hasta el momento: 11 millones de archivos, muchos relacionados con sus pacientes, quedaron al descubierto.[121]

[120] Stiennon, Richard. *Op. Cit.*, p. 48. Traducción propia.
[121] Jiménez Cano, Rosa. "Los peores ataques cibernéticos en EE UU" en El País, sección Internacional, 4 de junio de 2015, Recuperado de: https://elpais.com/internacional/2015/06/05/actualidad/1433461961_205806.html Consultado el 21 de febrero de 2018.

Para hacer mención de un caso más reciente y de mayor escala, tenemos el que sucedió en octubre de 2016 cuando la idea de un gran ataque que dejara sin internet a un país dejó el plano de la ficción y se hizo realidad, pues millones de estadounidenses se encontraron imposibilitados para ingresar a algunos de los sitios más populares del país y del mundo, tales como "la empresa de streaming de música Spotify, las redes sociales Twitter, Reddit, y Tumblr, las compañías de ventas online Amazon y Shopify, y la de intercambio de archivos de música SoundCloud"[122] También las páginas de periódicos como el *New York Times* y el *Boston Globe* se vieron afectadas. Los ataques parecen haberse realizado contra la empresa *Dyn* que conecta a los usuarios con los servidores de las empresas mencionadas y constó de dos oleadas: una a las 7:30 a.m. aproximadamente cuyos efectos se sintieron en el este del país; la segunda se dio tres horas más tarde y no solo afectó esa zona sino que se extendió hacia "California, Nevada […] Texas, Chicago, Seattle, y el Medio Oeste. Eso supone prácticamente la totalidad de los grandes núcleos urbanos estadounidenses, con la excepción de Miami y Phoenix."[123] También, cabe mencionar que varias de las empresas afectadas, aparte de tener un alto valor e impacto a nivel mundial, son de las más cotizadas en la bolsa de valores de Estados Unidos; no obstante, Wall Street no las penalizó. Sin embargo, el portavoz de Barack Obama no se tomó nada bien dicho ataque y declaró que se encontraban investigando la interrupción, la cual calificaron de "maliciosa".

Ahora, teniendo en consideración el nivel de ciberataques que Estados Unidos recibe constantemente que le afectan en aspectos económicos y sociales más que nada, podemos también trasladar esta situación a los ataques que pueden afectarles más profundamente si se orientan hacia empresas estatales, agencias de inteligencia y seguridad nacional y, al propio gabinete del gobierno.

[122] Pardo, Pablo. "Estados Unidos investiga un ciberataque a gran escala" en El Mundo, sección Tecnología, 21 de octubre de 2016, Recuperado de: http://www.elmundo.es/tecnologia/2016/10/21/580a7bda468aeb94588b4666.html Consultado el 21 de febrero de 2018.
[123] *Idem*.

Por otro lado, a pesar de que resulta más complicado identificar al perpetrador de un ataque cibernético a diferencia de uno físico, existen algunos países o grupos de choque a los que Estados Unidos les atribuye dichos ataques, cuestión que resulta en un interés particular de análisis para la disciplina de las relaciones internacionales, tema en el que profundizaré en el siguiente apartado.

3.1.3.1. Estados Unidos y sus principales contrincantes en la guerra cibernética.

Como ya se había mencionado, en la guerra cibernética resulta más complicado determinar a los culpables de un ataque, a diferencia de en uno que se realice por aire, mar o tierra; no obstante, sabemos que Estados Unidos tiene a varias naciones como rivales en el aspecto político, militar o económico, como lo pueden ser Rusia, Corea del Norte, China, Irán y varios países del medio oriente, por mencionar algunos. Por lo tanto, al gobierno estadounidense poco le importará realizar una investigación exhaustiva detrás de cada ataque, pues tan solo la cantidad exorbitante que recibe de los mismos no se lo permite. Sin embargo, al considerar a la guerra cibernética como un instrumento para debilitar a los países enemigos en nuestros días, el país norteamericano no dudará en culpar a los más aguerridos y constantes que tiene.

De esta manera, por ejemplo, vemos que se culpa a China directamente por los intentos de robar diseños militares debido a la historia y reputación que tiene de replicar tecnología de otros tanto en el ámbito industrial como en el militar. Uno de los incidentes más famosos de esto fue el “desarrollo en China de una pequeña ojiva termonuclear adecuada para ser usada en un misil balístico intercontinental, lo cual coincidía con datos robados de la inversión masiva que Estados Unidos había hecho en dicha tecnología […] La ojiva original de Estados Unidos se llama W-

88"[124] De igual manera, se continúa culpando a China en la actualidad por robos de identidad, tal como nos lo presenta Jaime Hernández en su artículo *Ciberguerra, las batallas del siglo XXI* referente a un ataque que sufrió Estados Unidos en julio de 2015, en el cual se consiguieron los nombres, claves de seguridad y hasta huellas digitales de millones de funcionarios de la administración:

> Cuando los expertos en materia de seguridad y ciberataques confirmaron […] ante un Comité de inteligencia del Congreso estadounidense, la incursión de piratas cibernéticos en la base de datos de la Oficina de Gestión de Personal del gobierno (OPM) y el potencial robo de más de 22 millones de identidades, la señal de alarma se extendió hasta la Casa Blanca y la Agencia de Seguridad Nacional (NSA), que ordenaron una inmediata investigación de esta intrusión sin precedentes.
>
> Tras una serie de pesquisas, el almirante Michael Rogers, comandante del cibercomando y director de la NSA, se resistió a identificar a los responsables del peor ataque en los últimos años. Menos reacio a identificar a los responsables del ataque, el director nacional de inteligencia, James Clapper, se atrevió a dar un paso al frente para identificar a China como "el principal sospechoso" de haber perpetrado ese ataque.[125]

Casi un mes después de dicho ataque, fuentes del Pentágono reportaron un "sofisticado ciberataque" que colapsó el sistema de correos clasificados del jefe del Estado Mayor Conjunto, el general Martin Dempsey, responsable de la estrategia militar de EU en Irak y Afganistán. Ante lo cual, el mismo Pentágono apuntó a Rusia como el principal sospechoso, de igual manera, sin mayor investigación.

---

[124] Stiennon, Richard. *Op. Cit.*, p. 49. Traducción propia.

[125] Hernández, Jaime J. "Ciberguerra, las batallas del siglo XXI" en El Universal, México, Sección Mundo, 16 de agosto de 2015. Recuperado de: http://www.eluniversal.com.mx/articulo/mundo/2015/08/16/ciberguerra-las-batallas-del-siglo-xxi Consultado el 12 de mayo de 2016.

Desde hace varios años, Estados Unidos libra esta guerra con Rusia, China y Corea del Norte, quienes parecen ser sus principales contrincantes, aunque los gobiernos de dichos países aseguran no contar con programas para penetrar las redes del gobierno o de contratistas de las agencias de seguridad e inteligencia estadounidenses. No obstante, ha sido durante la administración de Obama cuando más voces se han levantado para culpar a dichas naciones por estas incursiones.

De hecho, como si no hubiera ya el nivel de pánico suficiente en la gente, en la misma semana de los ataques, "el secretario estadounidense de Estado, John Kerry, sorprendió a millones de telespectadores cuando reconoció, en una entrevista con la cadena CBS, que los chinos y los rusos "muy probablemente" revisan todos los días sus correos electrónicos . "Por eso los tengo que escribir a sabiendas de que los pueden leer…", aseguró Kerry"[126] admitiendo así la capacidad de dichas potencias tecnológicas para penetrar en sus redes sin mayor problema.

Por lo que se refiere a la zona de medio oriente, tenemos a Irán, país al que convenientemente Estados Unidos culpa por ataques no sólo hacia ellos, sino a países europeos, Arabia Saudita y Corea del Sur. Los analistas comenzaron a enfocarse en un grupo llamado APT33, por las siglas en inglés de *Advanced Persistent Threat* (amenaza persistente avanzada), ya que en los últimos años la actividad cibernética de dicho país ha ido en aumento, lo cual los hace blancos perfectos si de buscar culpables se trata, aunque bien puede ser cierto pero difícil de determinar. Los culparon de docenas de ataques informáticos que se dieron entre 2011 y 2013 "hacia instituciones financieras en Europa y Estados Unidos - sobre todo DDos (denegación de servicio) incluido el de una represa cerca de Rye

[126] *Idem*.

Brook, en el Estado de Nueva York, EE.UU."[127] Por su lado, los iraníes aseguran que sí cuentan con el equipo necesario para monitorear mensajes y aplicaciones. Además, existe un grupo que se hace llamar "Ejército Cibernético Iraní" y según expertos, se encuentra relacionado con el gobierno, pero dicha aseveración no es oficial. De igual manera, afirman que dicho grupo reclamó la autoría de varios ataques contra la empresa de internet china Baidu y contra Twitter.

También vincularon a los hackers iraníes con sitios web del Ministerio de Energía de Arabia Saudita y la Universidad Rey Abdulaziz, en Riad.[128] Sin embargo, hay algunos analistas que establecen que dichos ataques por parte de Irán se tratan de una ofensiva cibernética derivada del ataque que ellos recibieron conocido como *Stuxnet*, ya mencionado previamente, el cual tenía la finalidad de sabotear las actividades nucleares de la república islámica provocando fallos en las centrifugadoras de uranio.

Finalmente, podemos hacer mención rápidamente de Corea del Norte, país al que Estados Unidos intentó atribuir el ataque cibernético de escala mundial *WannaCry* de mayo de 2017. Sin embargo, esto se dio después del periodo de Obama, por lo que tendríamos que analizarlo bajo el enfoque de la administración de Donald Trump, quien parece llevará una relación aún menos cordial con dicha nación.

3.1.3.2. Respuesta del gobierno de Obama a los ataques.

Antes que nada, debe quedar claro que al ser el Pentágono el núcleo de las operaciones militares de Estados Unidos, este cuenta con redes diversas, conflictos en la administración y jerarquías, y servidores de computadora para

[127] Redacción. "APT33, el grupo de hackers iraní al que se atribuyen ataques a Estados Unidos, Arabia Saudita y Corea del Sur" en BBC Mundo, sección Tecnología, 16 de octubre de 2017, Recuperado de: http://www.bbc.com/mundo/noticias-41637526 Consultado el 21 de febrero de 2018.
[128] *Idem*.

comando y control, todo esto los hace el blanco perfecto para los ataques cibernéticos cuyo objetivo es la obtención de información. Así, vemos que desde el verano de 2003, "aún después de la experiencia de múltiples virus tales como CodeRed, Nimda y SQL Slammer, el Pentágono tenía todavía muy poca habilidad para detectar y bloquear aquellos gusanos, mucho menos un ataque dirigido. La primera línea de defensa era conseguir un *firewall (software* "cortafuego") con respaldo de tecnología IDS (Sistemas de Detección de Intrusiones)."[129] Sin embargo, esta tecnología no hacía nada para detener los ataques, sólo alertaba a los usuarios sobre ellos.

Es por esto que, en octubre de 2009, la Secretaria del Departamento de Seguridad Interna de Estados Unidos, Janet Napolitano, anunció que se contrataría a 1000 "expertos en seguridad"[130], sin embargo, aún no tenían identificadas las funciones o el perfil que estos deberían cumplir, por lo que comenzaron a solicitar información internamente a su personal de varios departamentos para que proporcionaran los datos con los que contarán al respecto de ese tipo de puestos en la actualidad. En pocas palabras, sabían lo que debían hacer, pero no el cómo, cuestión que no los detuvo pues como ya se ha mencionado, la tecnología avanza a mayor velocidad de la que conocemos o somos capaces de manejar pero solo aquellos que lo intenten tendrán mejor suerte en los años venideros.

En el mismo año, el presidente Barack Obama ordenó la creación del Cibercomando, el cual tiene como misión "la planeación, coordinación, integración, sincronización y dirección de operaciones de defensa de redes específicas del Departamento de Estado en contra de amenazas terroristas, del crimen

[129] Stiennon, Richard. *Op. Cit.*, p. 47. Traducción propia.
[130] *Ibídem*, p. 102. Traducción propia.

organizado, físicas, virtuales y de otros países."[131] Dicho organismo ha reconocido que "el volumen de ataques contra el Pentágono supera los 250 mil por hora, es decir, aproximadamente 6 millones de ataques por día."[132] Cantidad bastante alarmante si el país más poderoso actualmente la considera como una prueba de la pérdida constante de su poder en los escenarios de las guerras actuales.

Por otra parte, cabe mencionar un evento reciente en el cual Estados Unidos vio minado el sistema democrático que tanto defiende. Esto derivado de los supuestos ataques cibernéticos que realizó Rusia en contra de la campaña de Hillary Clinton para robar información que la demeritara y hacerla pública, con tal de favorecer al candidato del partido republicano: Donald Trump.

No fue hasta 2017 que Estados Unidos acusó a Putin de tratar de desestabilizar al sistema electoral estadounidense, sin embargo fue desde agosto de 2016 que "Obama puso a la Casa Blanca en pie de guerra: ordenó a sus servicios de inteligencia y de seguridad obtener la máxima información posible y hacer una lista de represalias posibles, desde sanciones económicas hasta ataques cibernéticos."[133] Por su parte, el *Washington Post* informó de la opción diplomática por la que estaban optando Obama y el director de la CIA a la par de los ataques cibernéticos que estaban considerando en caso de que Putin no hiciera caso: "además de la advertencia directa de Obama a Putin al margen de una cumbre en China en septiembre (de 2016), el director de la CIA, John Brennan, llamó por teléfono el 4 de agosto (de ese año) a su homólogo del servicio de seguridad ruso

[131] Vargas Aguilar, Simón. "Guerra cibernética: la nueva amenaza" en La Jornada, Mexico, Sección Opinión, 5 de julio de 2013. Recuperado de: http://www.jornada.unam.mx/2013/07/05/opinion/018a2pol Consultado el 06 de marzo de 2018.

[132] Hernández, Jaime J. "Ciberguerra, las batallas del siglo XXI" en El Universal, México, Sección Mundo, 16 de agosto de 2015. Recuperado de: http://www.eluniversal.com.mx/articulo/mundo/2015/08/16/ciberguerra-las-batallas-del-siglo-xxi Consultado el 12 de mayo de 2016.

[133] AFP. "Advirtió la CIA a Obama que Rusia quería hackear elecciones" en La Jornada en línea, sección Mundo, viernes 24 de junio de 2017, Recuperado de: http://www.jornada.unam.mx/2017/06/24/mundo/020n1mun Consultado el 21 de febrero de 2018.

FSB, Alexander Bortnikov, para también advertirle. […] Pero Obama se mostró reacio a actuar antes de las elecciones por temor a que Rusia lanzara ataques en la jornada electoral."[134] Al llegar el día de las elecciones - e incluso antes - fue claro que había intervención rusa, por lo que el presidente saliente tomó la decisión de cerrar residencias diplomáticas rusas en Estados Unidos, así como castigos económicos contra los servicios secretos de dicho país. Además de la implementación de una operación secreta en conjunto con la CIA y la NSA (Agencia de Seguridad Nacional) con el cual se implantaría un código malicioso en la infraestructura rusa que podría ser activado en caso de una escalada por su parte. Ahora, nos corresponderá ver qué tan obediente se vuelve la administración de Trump ante el gobierno ruso, a quien Obama en su debido momento le dijo "Tú y yo estamos del mismo lado, Putin no".

3.1.4. Preparación cibernética en distintos gobiernos dentro del panorama actual.

Ante el nuevo panorama que vivimos donde las amenazas derivadas de los avances tecnológicos se le presentan a diario a los gobiernos y a la sociedad en general, vemos que "gobiernos de todo el mundo han comenzado a modificar sus paradigmas de seguridad, y a trabajar en la adquisición de nuevas capacidades para impedir o detectar ataques informáticos, a fin de aislarlos y neutralizarlos mediante técnicas de ingeniería reversa. Entre 2000 y 2013, 25 países publicaron estrategias y políticas nacionales en materia de seguridad cibernética."[135] De esta manera, los gobiernos alrededor del mundo incrementan sus esfuerzos en lo que respecta a la seguridad informática de sus sistemas de inteligencia, por lo que crean Cibercomandos, como el implementado en Estados Unidos en 2009, y también encuentran necesario aumentar la cantidad de personal de "IT" o sea,

[134] *Idem*.
[135] Vargas Aguilar, Simón. "Guerra cibernética: la nueva amenaza" en La Jornada, Mexico, Sección Opinión, 5 de julio de 2013. Recuperado de: http://www.jornada.unam.mx/2013/07/05/opinion/018a2pol Consultado el 06 de marzo de 2018.

expertos en Tecnologías de la Información y la seguridad de las mismas. En el próximo capítulo se analizará cómo estas medidas también trajeron consecuencias contraproducentes para el gobierno de Estados Unidos y por qué, pero por lo mientras veamos algunos ejemplos de la preparación cibernética en varias naciones.

En Estados Unidos, antes de la creación del Cibercomando, se impulsó la CNCI o *Comprehensive National Cybersecurity Initiative* (Stiennon, 2010) a finales de la administración de George W. Bush la cual contaba con los siguientes puntos:

1. Conexiones de Internet Confiables (TIC, por sus siglas en inglés), lo cual está basado en la idea de defender más fácilmente un perímetro pequeño[136], lo cual resulta cada vez más complicado debido al continuo crecimiento de las redes.
2. Sistema de Detección de Intrusiones (*IDS*, por sus siglas en inglés), también llamado Proyecto "Einstein II", el cual se refiere a un equipo encargado de estar listo para los ataques, no sólo para responder sino para prevenirlos a través del monitoreo de las redes.
3. *IPS:* Sistema de Prevención de Intrusiones, proyecto también llamado "Einstein III" el cual se refiere a las acciones a tomar para no solo identificar los ataques, sino realmente bloquearlos.
4. Coordinación *R&D (Research & Development)*: Vela por la investigación y el desarrollo de tecnología para la seguridad cibernética.
5. Conectar a los centros de expertos: Esto para que en una situación de crisis, los responsables de las redes se puedan comunicar más fácilmente.
6. TOP SECRET: Es el único elemento del CNCI que está clasificado.
7. Contraespionaje: Identificar, monitorear y tirar las actividades de los espías

[136] Stiennon, Richard. *Op. Cit.*, p. 133. Traducción propia.

cibernéticos.[137]

8. Educación y entrenamiento de la fuerza de trabajo: La continua capacitación del personal de seguridad cibernética llevará a mejores resultados.
9. Adelantarse en las tecnologías: Invertir en nuevas tecnologías para descubrir vulnerabilidades y posibles defensas de las redes.
10. Disuasión: Es la idea de amenazar a los atacantes potenciales diciendo que Estados Unidos devolverá el ataque.[138] Sin embargo, esto es muy subjetivo, porque no a todos los atacantes les va a preocupar este tipo de amenazas si se saben más calificados que el personal del gobierno.
11. La administración de los riesgos en la cadena de suministro: Esto debido a que, por ejemplo, mucho del equipo nuevo lo proveen empresas chinas, de donde también pueden provenir enemigos potenciales.
12. Protección crítica de la infraestructura: También conocido como "Proyecto 12" e involucra muchas asociaciones y consorcios entre gobierno y empresas privadas. Parece ser la responsabilidad principal del Director de Protección y Conocimiento de la Infraestructura Cibernética Crítica, de la División de Seguridad Nacional Cibernética del Departamento de Seguridad Nacional (*Department of Homeland Security*).[139]

Cabe considerar que a pesar de que no basta con sólo crear leyes y puntos a seguir para protegerse en la guerra cibernética, sino realmente contratar personal capacitado, así como desarrollar constantemente la tecnología necesaria para hacerle frente, no cabe duda que al menos todos estos elementos representan un buen punto de partida para cualquier nación que desee comenzar a proteger sus redes.

[137] *Ibídem,* p. 135. Traducción propia.
[138] *Idem*
[139] *Idem*

Otro país que está preparándose continuamente - y tal vez mucho más que cualquier otro – para la Guerra cibernética es China, quienes desde 2016 crearon "tres nuevos cuerpos militares como parte de las reformas puestas en marcha para modernizar sus fuerzas armadas […] Un comando general para el Ejército de Liberación Popular, un grupo de misiles y una fuerza de apoyo estratégico."[140] De esta última, se hace referencia a que podría centrarse tanto en el desarrollo espacial como en la guerra cibernética, por lo que podemos constatar que en dicho país hasta hace pocos años aún no le dieron la relevancia que debía tener pues la incluyeron dentro de una "fuerza de apoyo estratégico", sin embargo han continuado su trabajo en el desarrollo de tecnología para hacerle frente al futuro:

> Científicos chinos realizaron la primera distribución de una clave cuántica desde un satélite a la Tierra, con lo que sentaron las bases para la construcción de una red global de comunicaciones cuánticas a prueba de ataques cibernéticos. Llamado Micio (Mozi) por un filósofo y científico chino del siglo V a.C. […] el satélite fue enviado el 16 de agosto de 2016 a una órbita sincrónica con el Sol a una altitud de 500 kilómetros.
>
> La tasa de transmisión de la clave cuántica del artefacto a la Tierra es hasta 20 órdenes de magnitud más eficiente que lo esperado con una fibra óptica de la misma longitud.
>
> Cuando el satélite sobrevuela China, ofrece una ventana de experimentación de unos 10 minutos. Durante ese tiempo, puede generar y enviar 300 kilobites de claves seguras, según Pan Jianwei, científico en jefe de Quess y miembro de la Academia de Ciencias de China. Eso, por ejemplo, puede satisfacer la demanda de una conversación telefónica absolutamente segura o la transmisión de una gran cantidad de datos bancarios, puntualizó.
>
> El cifrado tradicional de clave pública se basa en la indescifrabilidad

[140] Agencias AP y EFE. "China moderniza su ejército para ciberguerra y espacio" en *El Universal*, Sección Mundo, p. A22, 3 de enero de 2016.

> computacional percibida de ciertas funciones matemáticas. Con el entrelazamiento cuántico, se utiliza la tecnología de la clave cuántica en las comunicaciones de este tipo (para codificar la información), eliminando la posibilidad de espionaje y asegurando la conexión. Un espía en el canal cuántico tratando de lograr información sobre la clave introducirá inevitablemente interferencias en el sistema y podrá ser detectado por los usuarios, concluyó.

De esta manera, podemos ver cómo China continúa su lucha por entrar dentro de las primeras potencias en todo aspecto, incluyendo el desarrollo de tecnología informática con el fin de "convertirse en una potencia cibernética hacia 2035"[141] tal como lo aseguró Miao Wei, el ministro de Industria y Tecnología Informática del país asiático.

Finalmente, cabe mencionar a tres países que se encuentran también desarrollando tecnología e implementando unidades cibernéticas o cibercomandos dentro de sus fuerzas armadas, pero a los que aún les falta mucho camino por recorrer para alcanzar a las dos naciones mencionadas previamente. Nos referimos a Corea del Sur, a su vecino Corea del Norte y a la Federación Rusa. Corea del Sur anunció en Noviembre de 2009 que crearía un Comando de Defensa Cibernética en las oficinas centrales de inteligencia del Ministerio de Defensa[142], el cual está activo desde 2011-2012.

Por otro lado, Corea del Norte y Rusia mantienen un perfil bajo pero son a los que más se les atribuyen los ataques cibernéticos, por lo que veremos qué respuesta tienen hacia dichas acusaciones y qué avances nos mostrarán en un futuro.

---

[141] Agencias. "China buscará modernización en Internet" en La Jornada en línea, Sección Economía, 26 de diciembre de 2017, Recuperado de: http://www.jornada.unam.mx/2017/12/26/economia/018n3eco Consultado el 21 de febrero de 2018.

[142] Stiennon, Richard. *Op. Cit.*, p. 141. Traducción propia.

Capítulo 4
La filtración de información y sus implicaciones en la Guerra Cibernética de Estados Unidos

4.1. Triada Assange-Manning-Snowden.

Por lo que se refiere a la filtración de información que tanto ha afectado en los últimos años al gobierno estadounidense y sus relaciones tanto internas como externas, hay tres nombres que han resonado más que otros: Julian Assange, fundador de WikiLeaks, página que tiene la finalidad de hacer del dominio público los secretos del gobierno; Bradley (ahora Chelsea) Manning, ex soldado y analista del ejército estadounidense que filtró miles de documentos a WikiLeaks; y Edward Snowden, antiguo empleado de la CIA y la NSA, quien hizo públicos documentos clasificados como "*Top secret*" incluyendo los programas de vigilancia masiva de dichas agencias de inteligencia.

Es por esto que, si una democracia pretende funcionar, la gente y el mismo gobierno debe cuestionar si sus políticas son realmente legítimas o pueden afectarles más de lo que los benefician. Tal como lo expresó un oficial de la Unión Estadounidense por las Libertades Civiles (ACLU, por sus siglas en inglés), Morton Halperin: "La única arma que los oponentes a una política presidencial, dentro o fuera de la rama ejecutiva, tienen es el debate público. Si una política puede ser debatida abiertamente, entonces el Congreso puede ser persuadido a restringir al

Presidente y la presión pública puede forzarle a cambiar una política. Pero si la secrecía es aceptada como norma y legitimada, entonces los controles puestos en operaciones encubiertas pueden ser ignorados fácilmente."[143] Y no sólo pueden pasarse por alto los controles o límites impuestos a los servicios de inteligencia con respecto a su vigilancia a terroristas u otros oponentes al gobierno o a cualquiera que consideren prudente espiar, sino también los límites que se deben conservar en cuanto a la vigilancia a la población misma del país o a civiles inocentes en cualquier otro punto del planeta.

De esta manera, los tres hombres mencionados previamente se unieron a la lista de acusados o perseguidos por el gobierno de Estados Unidos por revelar al público información clasificada, de acuerdo con el Acta de espionaje de 1917, la cual fue "una ley originalmente promulgada para criminalizar y enjuiciar a individuos por ser infiltrados, informantes o espías pero no para encausar a los llamados "soplones" que denuncian lo que consideran que es fraude o abuso de las agencias del gobierno."[144] Es precisamente esto lo que han hecho estos llamados "soplones", nada más que hacer públicos los abusos del gobierno, ya que una cosa es tratar de obtener más información de otros gobiernos y sus funcionarios mediante medios poco ortodoxos, y otra es realizar un espionaje masivo incluyendo a civiles que nada tienen que ver y que sólo ven mermada así su libertad y privacidad.

Tomemos como antecedente el caso de Daniel Ellsberg, quien se hizo famoso durante el gobierno de Richard Nixon por la filtración de los llamados "Papeles del Pentágono" en 1971 a los periódicos *The New York Times* y posteriormente al *Washington Post*, los cuales dañaron enormemente la imagen de Nixon y

[143] Shulsky, Abram N. y Schmitt, Gary J. *Op. Cit.*, p. 146

[144] Márquez, William. "¿Qué pasó con los otros soplones de Estados Unidos?" en BBC Mundo, Reino Unido, Sección Internacional, 27 de junio de 2013. Recuperado de: http://www.bbc.com/mundo/noticias/2013/06/130626_eeuu_otros_soplones_wbm Consultado el 11 de mayo de 2016.

representaron el comienzo del fin para su mandato. Esto lo vemos en palabras de Anthony Lewis, antiguo columnista del *New York Times* quien asevera que: "la revelación pública de los Documentos del Pentágono desafió la base del poder de un presidente: su papel en los asuntos de seguridad extranjeros y nacionales"[145]. De igual manera, conviene señalar que Ellsberg trabajaba para el gobierno - tal como Manning y Snowden - era un "analista militar que le entregó al diario *The New York Times* y a otras publicaciones documentos que revelaban cómo el público había sido engañado con respecto a la guerra de Vietnam. Se trataba de un estudio secreto que Ellsberg había logrado fotocopiar, en el que se indicaba que las autoridades sabían desde muy temprano de la improbabilidad de ganar el conflicto y que continuar con él ocasionaría muchísimas más bajas que las que reconocían."[146] El gobierno de Nixon intentó callar estas voces, sin embargo la Corte Suprema de Justicia reconoció su derecho a publicar los documentos basándose en la Primera Enmienda que defiende el derecho a la libertad de expresión. Pocos años después, en 1974, el *Washington Post* también publicó acerca del escándalo de Watergate, lo cual obligó a Nixon a dimitir a la presidencia.

Ahora bien, considerando que la labor de los tres hombres mencionados afectaron a Estados Unidos en 3 rubros cruciales para ellos como lo son el político-diplomático, el militar y el de la opinión pública, así podemos aseverar que este es un camino que no se puede dejar de lado u olvidarlo y si Estados Unidos no hace todo lo posible por permitir la libertad de expresión y la transparencia, o bien, por defender aún más a sus agencias de inteligencia y la información que manejan de los medios tecnológicos, el declive de su poder en este mundo ahora multipolar será mucho más acelerado de lo que se pensaba.

---

[145] Dargis, Manohla. "Reseña: En 'Los archivos del Pentágono', la democracia sobrevive a la oscuridad" en *The New York Times* en español, Sección Cine, 2 de enero de 2018, Recuperado de: https://www.nytimes.com/es/2018/01/02/resena-en-los-archivos-del-pentagono-la-democracia-sobrevive-a-la-oscuridad/ Consultado el 10 de abril de 2018.

[146] Márquez, William. "¿Qué pasó con los otros soplones de Estados Unidos?" en BBC Mundo, Reino Unido, Sección Internacional, 27 de junio de 2013. Recuperado de: http://www.bbc.com/mundo/noticias/2013/06/130626_eeuu_otros_soplones_wbm Consultado el 11 de mayo de 2016.

4.1.1. Julian Assange y WikiLeaks: La diplomacia al descubierto.

Tal como lo decía Napoleón Bonaparte: "El secreto de las guerras reside en las comunicaciones". De esta manera, podemos comprender por qué los países y cualquier individuo u organización con intenciones políticas defenderán su información a "capa y espada". Esto también nos lo expone Jacqueline Peschard cuando dice que "todos los Estados tienen información secreta que buscan mantener al margen de los ojos no solo de sus opositores, sino de los ciudadanos, pues como dice Elías Canetti, <<el secreto está en la médula del poder>>. Sin embargo, la idea muy arraigada de que los secretos de Estado, y en particular los relativos a la seguridad nacional, son siempre inexpugnables, se ha ido sometiendo a revisión, gracias a los avances que ha tenido la promoción de los derechos humanos y el acceso a la información pública como derecho fundamental de las personas."[147] Es así cómo, Julian Assange creó un parteaguas para aquellos que buscaban transparencia en los asuntos secretos del gobierno, sobre todo los que afectan directamente a la sociedad internacional.

WikiLeaks es una "autodenominada <<organización mediática sin fines de lucro>>, lanzada en 2006 con el propósito de difundir documentos originales provenientes de fuentes anónimas y filtraciones."[148] De igual manera, aclaran que no reciben rumores ni opiniones personales, solo material de corte político, diplomático o histórico. A continuación una breve reseña de los materiales filtrados desde 2006:

Fechas	Sucesos
Diciembre 2006	WikiLeaks publicó su primer documento: la decisión de asesinar a oficiales del gobierno firmada por el Sheikh Hassan Dahir Aweys. […] Publicaron la

[147] Peschard, Jacqueline. "Assange: los secretos a debate" en *El Universal*, sección Opinión, 8 de febrero de 2016, p. 28.
[148] Zittrain, Jonathan y Sauter, Molly. Trad. Francisco Reyes. "Todo lo que necesitas saber sobre Wikileaks" en *MIT Technology Review*, 9 de diciembre de 2010. Recuperado de: https://www.technologyreview.es/s/1647/todo-lo-que-necesitas-saber-sobre-wikileaks Consultado el 10 de abril de 2018.

	decisión con un largo comentario, el cual cuestionaba "¿Se trata de un audaz manifiesto de un extravagante militante islámico con vínculos a Bin Laden? ¿O es una prueba perspicaz de la inteligencia estadounidense, diseñada para desacreditar a la Unión, fracturar las alianzas somalíes y manipular a China?"... La autenticidad del documento nunca pudo determinarse, pero las noticias sobre WikiLeaks superaron rápidamente a la filtración misma.[149]
31/Agosto 2007	El *Guardian* presentó en su primera plana una historia sobre corrupción de la familia del ex líder de Kenia Daniel arap Moi. El periódico dijo que la fuente de la información fue WikiLeaks.[150]
Noviembre 2007	Una copia del "Procedimiento Operativo Estándar para Campo Delta" – el protocolo de la armada de Estados Unidos en el campo de detención en la Bahía de Guantánamo – fechada en marzo de 2003, fue publicada en el sitio de WikiLeaks el 7 de noviembre de 2007. […] Su publicación reveló algunas de las restricciones impuestas a los detenidos en el campamento, incluida la designación de algunos presos como prohibidos para el Comité Internacional de la Cruz Roja, algo que el ejército de los EE.UU. había negado reiteradamente en el pasado.[151]
Febrero 2008	El dominio wikileaks.org fue removido de la red después de que el banco suizo Julius Baer demandó a WikiLeaks y al registrador del dominio wikileaks.org, *Dynadot*, y obtuvo una orden judicial permanente ordenando el cierre. WikiLeaks había publicado denuncias de actividades ilegales de la sucursal del banco en las Islas Caimán. El registrador de WikiLeaks en los Estados Unidos, *Dynadot*, cumplió con la orden eliminando sus entradas de DNS. Sin embargo, el sitio web siguió accesible a través de su dirección IP, y los activistas en línea inmediatamente crearon espejos de WikiLeaks en docenas de sitios web alternativos en todo el mundo.[152]
Enero 2009	Más de 600 reportes internos de las Naciones Unidas (60 de ellos marcados como "estrictamente confidencial") fueron filtrados.[153]

[149] Miller-Jones, Edward R. *WikiLeaks. Removing the "top secret" seal*. Fastbook Publishing, Estados Unidos, 2010, p. 6. Traducción propia.
[150] *Ibidem*. P. 7
[151] *Idem.*
[152] *Idem*.
[153] *Ibidem*. P. 8

Feb. 2009	WikiLeaks publicó 6780 reportes del Servicio de Investigación del Congreso.[154]
Marzo 2009	WikiLeaks publicó una lista de contribuyentes a la campaña senatorial de Norm Coleman y un conjunto de documentos pertenecientes al Banco Barclays que se había ordenado eliminar de la página web del *Guardian*.[155]
25/Nov 2009	WikiLeaks publicó 570,000 interceptaciones de mensajes de *pagers* / *beepers* enviados el día de los ataques del 11 de septiembre.[156]
15/Marzo 2010	WikiLeaks publicó un reporte secreto de análisis de contrainteligencia del Departamento de Defensa de EE.UU. de Marzo de 2008. El documento describía algunos informes prominentes filtrados en el sitio web relacionados con los intereses de seguridad de los EE.UU. y describía posibles métodos de marginación de la organización. El editor de WikiLeaks, Julian Assange dijo que algunos detalles en el informe del Ejército eran inexactos y sus recomendaciones defectuosas, y también que las preocupaciones del Ejército de los EE.UU. planteadas por el informe eran hipotéticas. El informe discutió la posibilidad de disuadir a posibles informantes a través de la terminación del empleo y el enjuiciamiento penal de cualquier actual o antiguo conocedor, infiltrado o delator. Las razones del informe incluyen fugas notables, como el gasto en equipamiento de EE. UU., las violaciones de los derechos humanos en la Bahía de Guantánamo y la batalla por la ciudad iraquí de Fallujah.[157]
5/Abril 2010	WikiLeaks publicó material militar clasificado de una serie de ataques el 12 de julio de 2007 en Bagdad por un helicóptero estadounidense que mató a 12 personas, incluidos dos periodistas de Reuters, Saeed Chmagh y Namir Noor-Eldeen, en un sitio web llamado "Asesinato colateral". La filmación consistió en una versión no editada de 39 minutos y una versión de 8 minutos que había sido editada y anotada. El análisis del video indica que los pilotos pensaron que los hombres portaban armas (que en realidad eran equipos de cámara). Los militares llevaron a cabo una investigación "informal" sobre el incidente, pero aún no han publicado los materiales de investigación (como las declaraciones juradas de los soldados

[154] *Idem*
[155] *Idem*
[156] *Ibidem*. P. 10
[157] *Idem*

	involucrados o la evaluación de daños de batalla) que se utilizaron, lo que provocó que el informe fuera criticado como "descuidado".[158]

Creación propia a partir de Miller-Jones, Edward R.

Así fue que, a "finales de noviembre de 2010, Wikileaks empezó a liberar lentamente un tesoro de, según afirma, 251.287 cables diplomáticos adquiridos de una fuente anónima. Estos documentos surgieron justo después de la publicación del vídeo "Collateral Murder" en abril de 2010, y los documentos de las guerras de Afganistán e Irak en julio de 2010 y octubre de 2010, que ascendieron a 466.743 documentos." Poco después, el entonces soldado estadounidense, Bradley (ahora Chelsea) Manning, "confesó" que él había sido la fuente que proporcionó dicha información a WikiLeaks, por lo que se encuentra ampliamente relacionado con este mismo tema. No obstante profundizaremos más en Manning en el siguiente apartado para tocar el tema de la filtración de documentos del ejército.

Por ahora, enfoquémonos en los problemas político-diplomáticos que las filtraciones de WikiLeaks generaban. Julian Assange expresó a manera de festejo después de las revelaciones que: "Esta publicación de documentos revela las contradicciones entre lo que las figuras públicas estadounidenses informan al público y lo que dicen tras puertas cerradas. […] Los cables mostraban duplicidad y mendacidad en acción, incluido el alcance del espionaje de los Estados Unidos sobre sus aliados y las Naciones Unidas, haciéndose de la vista gorda ante la corrupción y el abuso en los derechos humanos en los "estados clientes"; tratos en el "cuarto trasero" con supuestos países neutrales; cabildeo para corporaciones de los Estados Unidos."[159] Lo cual ofrece un panorama muy claro de las relaciones que lleva dicha nación tanto con aliados como con enemigos y también hizo que las mismas sufrieran ciertas repercusiones o daños, por los cuales tuvo que pedir

[158] *Ibidem*. P. 11

[159] Sanger, David. "How our diplomats think" en: Star, Alexander (ed.). *Open secrets: WikiLeaks, War and American Diplomacy*. Grove Press, Nueva York, 2011, p. 331. Traducción propia.

disculpas, dar aclaraciones y, en pocas palabras, vio mermado su poder y credibilidad en el sistema internacional en tan solo unos días.

Estas filtraciones representaban algo sin precedentes, pues (al menos hasta entonces) había sido el <<mayor conjunto de documentos confidenciales nunca dados a conocer al dominio público>>[160]. Además de que tan solo la gran cantidad de documentos que se filtraron habla del impresionante valor que tuvieron aquellos que los enviaron a WikiLeaks y del mismo Assange para publicarlos, también tiene especial importancia el hecho de que nos permitieron dar un atisbo a la política estadounidense verdadera, muy diferente a la que nos dejan ver sus gobernantes:

> Había 251,287 comunicados internos del Departamento de Estado, escritos por 280 embajadas y consulados de 180 países diferentes. Entre ellos había evaluaciones francas y, con frecuencia, poco halagüeñas de los líderes mundiales; análisis, muchos de ellos de buena calidad; así como comentarios, informes de reuniones, resúmenes y rumores. Había relatos de cenas bañadas en vodka, reuniones con oligarcas, encuentros en restaurantes chinos e incluso aquella fiesta sexual en Arabia Saudita. Algunos cables eran largos ensayos, que ofrecían ideas frescas sobre problemas históricamente espinosos, como el de Chechenia; otros eran […] peticiones a Washington.
>
> Ponían de relieve los intereses y las preocupaciones geopolíticas de la superpotencia estadounidense: la proliferación nuclear; la supuesta amenaza de Irán, la situación militar, difícil de controlar, en Kabul e Islamabad. Los cables de las embajadas estadounidenses procedían de centros de poder establecidos (Londres y París), pero también de lugares lejanos (Asjabat, Ereván y Biskek). […] Ofrecen un mosaico incomparablemente detallado de la vida y la política de principios del siglo XXI.[161]

[160] Leigh, David y Harding, Luke. *WikiLeaks y Assange. Un relato trepidante sobre cómo se fraguó la mayor filtración de la historia*. Ediciones Deusto, México D.F., 2011, p. 234.
[161] *Ibidem*, pp. 234 y 235.

En definitiva, los cables, aunque se publicaban en "pequeñas dosis" nos permitieron darnos una idea de cómo es realmente un país tras correr el telón de la secrecía, se puede decir que incluso "desdibujaba claramente la línea que separa la diplomacia del espionaje"[162] ya que "la directiva de Washington pedía información delicada de las comunicaciones: contraseñas, claves cifradas. Requería que la información biométrica detallada <<sobre agentes clave de Naciones Unidas, incluya subsecretarios, jefes de agencias especializadas y sus principales consejeros, asesores de alto nivel del SYG [Secretario General], dirigentes de operaciones de paz y misiones políticas sobre el terreno, incluyendo comandantes de las fuerzas militares>>, así como información secreta sobre <<el estilo de gestión y toma de decisiones [de Ban] y su influencia en el secretariado>>. Washington también quería números de tarjetas de crédito, direcciones de correo electrónico, números de teléfono, fax, mensáfonos y números de tarjetas de vuelo para cargos de Naciones Unidas."[163] Es por esto que, el gobierno estadounidense temía tanto que sus relaciones diplomáticas se vieran seriamente afectadas derivado del conocimiento por parte de todo el mundo –incluyendo a sus aliados- de estas actividades intrusivas.

En consecuencia, Julian Assange se hizo de muchos más adeptos de los que ya tenía, al grado de que en su "Australia natal y en todas partes, muchos lo consideran un héroe […] alguien cuya batalla contra el secretismo ha creado algo genuinamente nuevo y apasionante."[164] Además, se encargó de crear una organización sin Estado, que no solo era mucho menos vulnerable a las leyes de cualquier nación, sino que al ser internacional, contaba con gente trabajando para WikiLeaks en cualquier punto del planeta, por lo que si en algún momento Julian estuviera indispuesto, había mucha gente atrás de él esperando para responder o actuar en su lugar. En pocas palabras, podemos asegurar que WikiLeaks –y cualquier organización basada en internet- tiene un alto grado de resiliencia.

[162] *Ibídem*, p. 236
[163] *Idem*
[164] *Ibídem*, p. 274

A manera de conclusión de este tema, vemos que WikiLeaks además de abrirle paso a otros defensores de la libertad de expresión y del derecho a la información, aumentó el interés en los temas de política exterior no solo para los estudiosos de la misma, sino para el público en general, dado que los cables proporcionaban cierto matiz que muchos desconocíamos del mundo diplomático.

4.1.2. Chelsea (antes Bradley) Manning: La verdad sobre las guerras estadounidenses desde su propio ejército.

Ahora bien, consideremos a Bradley Manning, quien estuvo ampliamente relacionado con Julian Assange en el caso de los diarios de guerra de Irak y Afganistán, en los cuales el entonces analista de inteligencia del ejército estadounidense envió videos y documentos a la página creada por Assange con información detallada de lo que realmente ocurría en dicha guerra.

En Mayo de 2010 se arrestó a Bradley Manning después de haberle confesado a Adrian Lamo (un periodista en el que confiaba plenamente, pero que lo traicionó informando de la confesión que Manning le hizo) que él había filtrado el video "Collateral Murder", así como cerca de 260,000 cables diplomáticos a WikiLeaks argumentándole lo siguiente:

> Si tuvieras dominio libre sobre redes clasificadas por largos períodos de tiempo ... digamos 8-9 meses ... y vieras cosas increíbles, cosas horribles ... cosas que pertenecían al dominio público, y no en algún servidor almacenado en una habitación oscura en Washington D.C. ... ¿qué harías? ... digamos... ¿una base de datos de medio millón de eventos durante la guerra de Iraq... de 2004 a 2009... con informes, grupos de fecha y hora, ubicaciones de latitud, cifras de víctimas? ¿O 260,000 cables del Departamento de Estado de

> embajadas y consulados de todo el mundo, explicando cómo el primer mundo explota al tercero, en detalle, desde una perspectiva interna?[165]

Tomando en consideración dichas motivaciones, vemos cómo en el video más famoso de dicha filtración, llamado "Collateral Murder" (en español, Asesinato Colateral) en la mañana del 12 de julio de 2017, soldados estadounidenses observaron desde helicópteros del ejército a un grupo de hombres reuniéndose en una zona de Bagdad, el cual incluía a dos periodistas de la agencia de noticias Reuters, Namir Noor-Eldeen y Saeed Chmagh, quienes estaban cargando sus cámaras, pero fueron confundidos con hombres que llevaban AK-47's. En consecuencia, los soldados solicitaron permiso para disparar, el cual se les dio sin mucho preámbulo, a pesar de que era claro que los hombres en tierra estaban tranquilos y no tenían ni las armas ni alguna clase de actitud intimidatoria.

En ese primer ataque murieron varios hombres, incluyendo a Noor-Eldeen. Chmagh resultó herido, pero murió pocos minutos después, en un segundo ataque cuando se acercó una camioneta a ayudarlo. En esta otra parte del video pudimos observar cómo "hombres desarmados intentaron subirlo a la camioneta. El equipo de los helicópteros que los observaban solicitó permiso para disparar, mencionando que <<parecía que los hombres posiblemente estaban recogiendo cuerpos y armas>> de la escena, y tras recibir el permiso, abrieron fuego sobre la camioneta y sus ocupantes. Dos niños sentados al frente resultaron heridos en el ataque pero sobrevivieron. Chmagh murió junto con el padre de los niños."[166] Así, vemos la magnitud que puede alcanzar una simple autorización dada al azar si no toman en consideración que dentro del mismo ejército existen quienes encuentran estas acciones injustas y las pueden sacar a la luz para conocimiento de las masas.

[165] Miller-Jones, Edward R. *Op. Cit.*, p. 59
[166] *Ibídem*, p. 46

Glenn Greenwald llamó a este ataque un “asesinato sin justificación de un grupo de hombres desarmados (con sus hijos) llevando a un hombre desarmado, gravemente herido a un lugar seguro.”[167] Después de que se dio a conocer dicha información, la reacción del ejército fue aún más indignante pues respecto al hecho de que había niños involucrados en la escena, comentaron: “Bueno, es su culpa por llevar niños a la batalla”[168] cuando era más que evidente que el grupo de hombres en tierra no esperaba dicho ataque, no llevaban armas ni estaban fraguando alguna ofensiva.

No obstante, a manera de contraste, tenemos un comentario de Josh Stieber, un objetor que en ese tiempo estaba asignado a la compañía Bravo 2-16, quien dijo en *Democracy Now!* que “aunque es natural juzgar o criticar a los soldados, de hecho así es como fueron entrenados para actuar. Dijo que el debate debería ser reformulado, que es más apropiado hacer preguntas sobre el sistema como tal, que enseña que hacer este tipo de cosas es por el bien de los intereses de mi propio país y que si quieren evitar que cosas como esta pasen, dejen de gritarle a los soldados…y por el contrario, usen su energía exponiendo el entrenamiento que los soldados pasan y demanden a los líderes que re-examinen el sistema que crea la insensibilidad mostrada en el video.”[169] Si bien es cierto que los soldados sólo siguen órdenes de sus superiores y el “Sistema”, como lo denomina Stieber, es el principal responsable en todo conflicto entre países, también a los soldados les haría bien tener un poco más de criterio antes de solicitar permiso para disparar a quien les plazca.

Por otra parte, Daniel Ellsberg –sí, el mismo que filtró los Papeles del Pentágono durante la guerra de Vietnam- quien ahora es un aguerrido defensor del caso de Manning, comentó respecto a los cables diplomáticos filtrados que:

[167] *Ibídem,* p. 47
[168] *Idem*
[169] *Idem*

> Cualquier riesgo serio a la seguridad nacional es extremadamente bajo. […] ¿Pondrá en vergüenza a las relaciones diplomáticas? Seguro, es muy probable – pero todo a favor del funcionamiento de nuestra democracia… WikiLeaks no ha publicado nada que haya podido poner en peligro a la seguridad nacional de nadie.
>
> Habiendo leído muchos de los cables diplomáticos, podría hacer el juicio de que muy pocos, menos del uno por ciento, quizá uno por ciento, puede honestamente decirse que pone en peligro a la seguridad nacional. Eso es distinto del porcentaje que podría causar vergüenza – mucha vergüenza, si la gente se diera cuenta de que estamos al tanto de operaciones altamente sanguinarias y corruptas y que las estamos apoyando. Es en verdad embarazoso…Si la elección está entre no publicar ninguna, como al Departamento de Estado le gustaría, y publicarlas todas, yo definitivamente siento que nuestra seguridad nacional mejoraría si todas fueran publicadas. Entre esas dos opciones, preferiría verlas todas publicadas. Nos ayudaría a comprender nuestra propia política exterior y darnos la oportunidad de mejorarla democráticamente. [170]

Conviene subrayar que cualquier información que el público pueda obtener acerca de lo que se trabaja y comenta en sus representaciones diplomáticas y demás oficinas gubernamentales, el Estado lo considerará como un peligro a la seguridad nacional aunque se trate real y simplemente de que la gente se estaría enterando de todos aquellos negocios o decisiones ocultas –e incluso, a veces perturbadoras- que obviamente no desean que la opinión pública tenga en sus manos. En concreto, el propósito de las revelaciones hechas por WikiLeaks a través de lo filtrado por Manning es, como lo expuso el *Toronto Sun*, la siguiente: “Este material arroja luz sobre la brutalidad cotidiana y la miseria de la guerra... El archivo cambiará la opinión pública y cambiará la opinión de las personas en puestos de

[170] *Ibídem,* p. 61

influencia política y diplomática."[171] Por lo tanto, no tiene razón de ser el hecho de que el gobierno y el ejército de Estados Unidos estuvieran acosando y maltratando a Manning durante su juicio y queriendo que confesara ser culpable de "ayudar al enemigo", cargo por el cual lo habrían condenado a cadena perpetua; más aún cuando él sí aceptó ser culpable de 10 de los 22 cargos que se presentaron en su contra, aceptando tan solo que sí fue responsable por la mayor filtración de secretos del gobierno (hasta ese entonces) lo cual traía consigo una condena de 20 años en prisión.

No obstante, vemos que lo que el gobierno estadounidense intentó dejar en claro, a través de dicho juicio, era que "habrá graves consecuencias ante la distribución no autorizada de información clasificada"[172]. Sin embargo, tal como lo sostiene Lawrence Korb, analista del *Centre for American Progress* y también ex secretario asistente de Defensa, las filtraciones "no pasan de revelar intercambios de comunicación que pueden ser embarazosos y que no son nada que no haya aparecido en los diarios de vez en cuando"[173], así que si no le presentan cargos de tal magnitud a los periodistas comunes y corrientes ni juicios tan complicados que hasta presentan violaciones a sus derechos humanos como el proceso de Manning, habríamos entonces de valorar los verdaderos motivos del gobierno estadounidense para sus acciones con el ex analista del ejército. Realmente, parece que se trata más de una lucha del código militar y la ley de espionaje contra la verdad y la justicia que se le debe a los inocentes que mueren en los conflictos bélicos en los que Estados Unidos se involucra.

---

[171] *Ibídem*, p. 66

[172] PJ Crowley, exsecretario de Estado asistente del presidente Barack Obama. En: Redacción. "Los dilemas del caso del soldado Manning" en BBC Mundo, Reino Unido, Sección Internacional, 03 de junio de 2013. Recuperado de: http://www.bbc.com/mundo/noticias/2013/06/130603_internacional_bradley_manning_eeuu_audiencia_nc_lav Consultado el 11 de mayo de 2016.

[173] Lawrence Korb, analista del Centre for American Progress. En: Márquez, William. "Bradley Manning: ¿Espía, activista o desadaptado?" en BBC Mundo, Reino Unido, Sección Internacional, 03 de junio de 2013. Recuperado de: http://www.bbc.com/mundo/noticias/2013/06/130513_eeuu_manning_juicio_militar_traicion_wbm Consultado el 11 de mayo de 2016.

Por el contrario, lo que han logrado con esta lucha es que los “soplones” como les llaman, tengan cada vez más popularidad entre la gente de todas partes del mundo, periodistas, Organizaciones No Gubernamentales e incluso naciones que, izando la bandera de la libertad de expresión y el derecho a la información y transparencia gubernamental, les han dado asilo ya sea en su territorio o al menos en sus embajadas en el extranjero, como es el caso de Ecuador con Julian Assange y Rusia con Edward Snowden, países que también están viendo modificaciones en sus relaciones diplomáticas con el país norteamericano como consecuencia de dichas acciones.

4.1.3. Edward Snowden: La vigilancia masiva del Estado hacia su población.

A los funcionarios de la seguridad nacional no les gusta la luz.
-Glenn Greenwald

En el mundo de la política internacional, hay veces en que la ética y la necesidad de dar a conocer al público la realidad detrás de los muros de secretismo que los gobiernos tanto protegen, pueden más que la obligación de proteger los mismos solo porque trabajan para las agencias de seguridad e inteligencia. Sobre todo, cuando la verdad que viven día a día no se parece en nada a lo que les prometieron al momento de reclutarlos, pues les venden la idea de proteger a su país y llevar “libertad” o “democracia” a todas las naciones del mundo, ya sea desde un escritorio o en el campo de batalla, pero al final se dan cuenta que rara vez es así.

Tal fue el caso de Edward Snowden, quien era funcionario de la NSA (Agencia de Seguridad Nacional) de Estados Unidos cuando descubrió varios programas de

vigilancia a la población que llevaba a cabo dicho gobierno y decidió sacarlos a la luz con la ayuda del entonces columnista del periódico *The Guardian* estadounidense, Glenn Greenwald, y de Laura Poitras, realizadora de documentales sobre la política estadounidense. Dichos personajes fueron los únicos a los que Snowden les permitió un acceso completo a los archivos sobre la vigilancia masiva para que lo apoyaran con la debida publicación de los mismos a la población mundial, a través de los periódicos *The Guardian* y *The Washington Post*, además de un libro que Greenwald escribió y un documental que Poitras realizó: *Sin un lugar donde esconderse / No place to hide* y *Citizenfour*, respectivamente.

Respecto al propósito y al impacto que Snowden deseaba lograr tras revelar la verdad sobre los programas de vigilancia del gobierno, le comentó a Greenwald y a Poitras lo siguiente:

> Mi único objetivo es informar a la gente de lo que se hace en su nombre y lo que se hace en su contra. El gobierno de EEUU, en complicidad con estados clientes, principalmente los Cinco Ojos –Reino Unido, Canadá, Australia y Nueva Zelanda -, han puesto en el mundo un sistema de vigilancia secreta y omnipresente, de la que no es posible escapar. Protegen sus sistemas internos de la supervisión de los ciudadanos mediante clasificaciones y mentiras, y se blindan contra el escándalo de eventuales filtraciones exagerando protecciones limitadas que deciden conceder a los gobernados…
> Los documentos adjuntos son reales y originales, y se ofrecen para procurar un conocimiento de cómo funciona el sistema de vigilancia pasiva, global, para que se puedan crear protecciones contra el mismo. El día en que escribo esto, todos los registros nuevos de comunicaciones pueden ser ingeridos y catalogados por dicho sistema y se pretende guardarlos durante años; por otro lado, están creándose y desplegándose en todo el mundo <<Almacenes Masivos de Datos>> (o, de manera eufemística, almacenes de datos de <<misiones>>), estando el mayor en Utah. Mientras rezo para que la toma de

> conciencia pública desemboque en la reforma, tengamos presente que las políticas de los hombres cambian con el tiempo, y que incluso la Constitución es subvertida cuando el apetito de poder así lo exige. Son palabras de la historia: No hablemos más de la fe en el hombre; atémoslo con las cadenas de la criptografía para que no haga travesuras.[174]

Respecto a la última frase del mensaje, Greenwald explica que la relacionó con una de Thomas Jefferson que originalmente hace relación a las "cadenas de la Constitución" que en esa época tenían el fin de contener precisamente las "travesuras" de los hombres, pero Snowden decidió adaptar la frase a lo que vivimos hoy día. Fue entonces que Snowden les envió los primeros documentos, los cuales hablaban sobre un programa denominado "PRISM", que le permitía a la NSA "recoger comunicaciones privadas de las empresas de internet más importantes del mundo, como Facebook, Google, Yahoo o Skype."[175] Para ellos fue impresionante saber que los grandes de internet se encontraban coludidos con las agencias del gobierno permitiéndoles acceso total a la información privada que los usuarios confiaban a dichas páginas, redes sociales y servicios de internet en general. Además que no solamente involucraba al gobierno estadounidense, sino que, como mencionaba Snowden previamente, existe el grupo de los Cinco Ojos compuesto por EE.UU., Reino Unido, Canadá, Australia y Nueva Zelanda, quienes se han encargado de crear, perfeccionar y sostener este sistema de vigilancia en todo el mundo (o la mayor parte).

Ante esta situación, Glenn y Laura se cuestionaron cual podría ser la razón que impulsó a Snowden a revelar dicha información poniendo en riesgo su libertad, o algo peor, si la situación llegaba a salirse de control, a lo cual éste respondió:

[174] Edward Snowden en: Greenwald, Glenn. *Op. Cit.,* p. 38.
[175] Greenwald, Glenn. *Op. Cit.,* p. 31.

> "Quiero provocar un debate mundial sobre la privacidad, la libertad en internet y los peligros de la vigilancia estatal. No tengo miedo de lo que pueda pasarme. Tengo asumido que, tras esto, mi vida probablemente cambiará. Estoy conforme. Sé que hago lo correcto."[176]

De igual manera, resulta crucial comprender la importancia del Tribunal FISA y de la Ley Patriota (*Patriot Act*) dentro del sistema de vigilancia gubernamental de EE.UU. y sus aliados. El primero es el "Tribunal de vigilancia de inteligencia extranjera (FISA), instituido por el Congreso en 1978, después de que el Comité Church sacara a la luz décadas de espionaje gubernamental abusivo. La idea subyacente a su creación era que el gobierno podía seguir realizando vigilancia electrónica, pero, para evitar abusos, antes debía conseguir un permiso del Tribunal."[177] Sin embargo, fue gracias a la sección 215 de la *Patriot Act* que los requisitos que se debían cubrir para obtener la autorización del Tribunal disminuyeron.

Ahora, respecto a la Ley Patriota / Patriot Act, se trata de una ley aprobada después de los ataques del 9 de septiembre para combatir al terrorismo, en la cual se pudo observar que "la sección 215 rebajó los estándares que debía cumplir el gobierno para obtener <<documentos comerciales/profesionales>> desde <<causa probable>> a <<pertinencia>>. Lo cual significaba que, para obtener documentos muy delicados o invasivos – como historiales médicos, transacciones bancarias o llamadas telefónicas -, el FBI solo tenía que mostrar que esos documentos eran <<pertinentes>> para una investigación en curso."[178] Por lo tanto, al gobierno estadounidense le resultaba mucho más sencillo realizar sus labores de espionaje a diestra y siniestra, aun cuando no eran realmente necesarias, solo porque resultaban "pertinentes".

[176] Edward Snowden en: Greenwald, Glenn. *Op. Cit.*, p. 32
[177] Greenwald, Glenn. *Op. Cit.*, p. 42
[178] *Ibídem*, p. 43

En particular, tenemos que, derivado de las actividades que esta Ley permitía realizar a las agencias de inteligencia sin muchas restricciones gracias a lo permisivo del Tribunal FISA, una de las primeras resoluciones que llegaron a las manos de Glenn y Laura fue una en la que se "ordenaba a *Verizon Business* que cediera a la NSA todos los <<registros de llamadas>> relativas a <<comunicaciones (I) entre Estados Unidos y el extranjero, y (II) dentro de los Estados Unidos, incluidas las llamadas telefónicas locales>>. Eso significaba que la NSA estaba, de forma secreta e indiscriminada, recopilando registros telefónicos de, como poco, decenas de millones de norteamericanos."[179] Sacando esto a la luz, era como podía verse -aunque fuera un poco- realizado uno de los propósitos de Snowden:

> Si creemos que esta investigación debe interrumpirse, que sus resultados han de clasificarse como <<alto secreto>> en un compartimento especial de <<información excepcionalmente controlada>> denominado STLW (STELLARWIND), que hay que descartar cualquier investigación futura partiendo del principio de que detener a quienes abusan del poder va contra el interés nacional, que debemos <<mirar hacia adelante, no hacia atrás>>, y que en vez de clausurar el programa hemos de expandirlo más, seremos bienvenidos a los salones del poder norteamericano; esto es lo que ha llegado a pasar, y yo estoy haciendo públicos los documentos que lo demuestran.
>
> […] Me sentiré satisfecho si quedan al descubierto, siquiera por un instante, la Federación de la ley secreta, la indulgencia sin igual y los irresistibles poderes ejecutivos que rigen el mundo que amo. […] He estado en los rincones más oscuros del gobierno, y lo que ellos temen es la luz.[180]

Gracias a sus habilidades y al ser tan entendido en su trabajo, fue cómo se ganó un lugar importante dentro de su equipo IT (Tecnologías de la Información) aún sin

[179] *Ibídem,* p. 42
[180] *Ibídem,* pp 47 y 48.

tener los estudios ni diplomas requeridos en muchos lugares. No obstante, durante su trabajo en Ginebra pudo tener acceso a mucha información secreta que le exponía las verdaderas acciones de su gobierno en el mundo, muy diferente a lo que se imaginaba en un inicio. Poco después, intentó que sus superiores le explicaran lo que pasaba realmente, pero le decían que no era asunto suyo y que dejara las cosas como estaban.

En palabras del mismo Snowden, él nos expone lo difícil que es obligar a los más poderosos a rendir cuentas: “Fue entonces cuando comencé a ver claramente lo fácil que es separar el poder de la rendición de cuentas, y que cuanto más altos son los niveles de poder, menor es la supervisión y la obligación de asumir responsabilidades.”[181] En consecuencia, Snowden sintió la necesidad de informar a la gente todo lo que el gobierno estadounidense espiaba, desde cómo veían pueblos enteros - valiéndose de drones - al seguimiento invasivo que realizaban a muchas personas mientras solo tecleaban en su computadora o utilizaban sus teléfonos celulares.

Snowden mencionaba que su objetivo, como tal, no era eliminar la capacidad de espionaje de la NSA ya que no le correspondían ese tipo de decisiones ni acciones, pero sí quería informar a la gente lo que estaba pasando con su privacidad para que ellos decidieran cómo continuar su vida: si estaba bien seguir actuando igual o harían algo al respecto para proteger su información de alguna manera, ya fuera usando los programas para encriptación o algún método de seguridad cibernética que conocieran.

Con relación a esto, Snowden informa que mientras trabajó para la CIA y la NSA, cada vez recibía mayor capacitación para “llegar a ser agente cibernético

[181] *Ibídem*, p. 59

cualificado, alguien capaz de hackear sistemas civiles y militares de otros países para robar información o perpetrar ataques sin dejar huellas."[182] Es por esto que, desde que se contactó con Glenn la primera vez le comentó que tenía información muy valiosa referente a las agencias de inteligencias estadounidenses y sus actividades invasivas, pero que no le podría compartir ninguna hasta que instalara una codificación *PGP* (*Pretty Good Privacy*) para encriptación de la información.

De igual manera, tiempo después Glenn se consiguió una computadora completamente nueva y que nunca había estado conectada a Internet, por lo que no había sido "contaminada" y constituía un perfecto "Muro de aire" como le llamaban. A esto es a lo que se refiere Snowden cuando habla de saber proteger nuestra información en este mundo interconectado y tecnológico donde el nivel de vulnerabilidad de la misma es más alto que nunca.

Finalmente, después de varias dudas en los periodistas acerca de la publicación del primer artículo sobre la información compartida por Snowden y de algunas amenazas gubernamentales al *Washington Post*, las cuales fueron también transmitidas al equipo del *Guardian*, se decidieron a publicarlo. "El titular rezaba así: <<La NSA obtiene a diario registros telefónicos de millones de clientes de *Verizon*>>. Había también un subtítulo: <<Exclusiva: La orden secreta de un tribunal a Verizon para que entregue todos los datos de las llamadas pone de manifiesto el aumento de la vigilancia interna bajo el mandato de Obama>>."[183] El impacto del artículo fue instantáneo y mayor a lo previsto, hubo respuesta por doquier, los noticiarios lo hicieron el tema principal e incluso, un portavoz de *Associated Press* les informó –gracias a un senador no identificado- que "el grueso del programa de recogida de registros de llamadas llevaba años funcionando y estaba dirigido a todas las empresas de telecomunicaciones importantes, no solo a

[182] *Ibídem,* p. 61
[183] *Ibídem,* p. 91

Verizon."[184] Ante este panorama, el gobierno de Obama intentó justificar el programa calificándolo como un arma clave en contra del terrorismo, pero todos los medios de comunicación -incluyendo el *New York Times*, a pesar de ser Pro-Obama- comentaron que el gobierno había perdido toda credibilidad con ese argumento, ya que a esas alturas nadie apoyaba la guerra contra el terrorismo ni les resultaba lógico el nivel de intrusión tan solo por perseguir "terroristas".

Incluso, fue a través de algunas encuestas y entrevistas que se puede observar cómo la opinión pública ha migrado de creer en el gobierno y su lucha contra el terrorismo como algo real que beneficia verdaderamente al país a pensar todo lo contrario y que lejos de beneficiar, perjudica más a la población civil que a los supuestos enemigos de la nación:

> En concreto <<una mayoría de norteamericanos (56%) dice que los Tribunales federales no habían impuesto límites suficientes a los datos telefónicos y de internet que está reuniendo el gobierno como parte de sus esfuerzos antiterroristas>>, y <<un porcentaje todavía mayor (70%) cree que el gobierno utiliza estos datos para fines que nada tienen que ver con las investigaciones sobre terrorismo>>. Además, <<el 63% opina que el gobierno también está recogiendo información sobre el contenido de las comunicaciones>>. Lo más curioso es que actualmente los norteamericanos consideran más preocupante el peligro de la vigilancia que el del terrorismo:
> En términos generales, el 47% dice que su preocupación por las políticas antiterroristas del gobierno es mayor porque estas han ido demasiado lejos en la restricción de las libertades civiles de las personas corrientes, mientras que el 35% afirma estar más preocupado por el hecho de que estas políticas no han sido suficientes para proteger el país. Es la primera vez que, en una encuesta del Centro de Investigación Pew, aparece más gente preocupada por las libertades civiles que por la protección frente al terrorismo desde que

[184] *Ibídem,* p. 93

en 2004 se formulara la pregunta por primera vez.[185]

Con relación al programa entre las empresas de comunicaciones con el gobierno estadounidense, el cual recibía el nombre de PRISM, muchas empresas comenzaron a desmentirlo, después de haber leído el artículo del *Guardian*, y a decir que no sabían nada al respecto. Por lo tanto, decidieron que se debía escribir un segundo artículo en el cual se incluyeran dichas posturas, pero también mostrando la disparidad entre las mismas y los documentos incriminatorios de la NSA.

En cuanto el segundo artículo salió a la luz, obtuvo la respuesta que Snowden tanto esperaba, ya que fue de carácter internacional, puesto que -a diferencia de empresas como *Verizon* que tienen su sede en un solo país- los grandes de Internet como Facebook, Yahoo o Gmail, representan medios de comunicación utilizados por gente de todo el mundo y "enterarse de que esas empresas habían llegado a acuerdos secretos con la NSA en virtud de los cuales esta tenía acceso a las comunicaciones de sus clientes constituía un escándalo a escala mundial."[186] Tan solo después de dos artículos publicados, el debate mundial ya había comenzado y era cuestión de tiempo antes de que el gobierno de Estados Unidos reaccionara, ya fuera por temor a una revuelta o por mero sentido común, ya que su imagen en el mundo como defensor implacable de la libertad se venía abajo poco a poco.

De igual manera, vemos que la inteligencia estadounidense no sólo se conforma con espiar extranjeros en su búsqueda de "terroristas", sino que el propio pueblo de ese país también ve mermada su privacidad con el programa PRISM y también con los que ha venido orquestando con sus aliados angloparlantes de los "Cinco Ojos",

[185] *Ibídem*, p. 245
[186] *Ibídem*, p. 99

grupo compuesto por EE.UU., Gran Bretaña, Canadá, Australia y Nueva Zelanda. Por mencionar algunos de estos programas, tenemos los siguientes:

> El grueso del programa de recopilación telefónica fue uno de los descubrimientos más importantes de un archivo envuelto en toda clase de programas de vigilancia encubiertos, desde el PRISM a gran escala, que conlleva recopilación de datos directamente de los servidores de las principales empresas de internet, y PROJECT BULLRUN, un esfuerzo conjunto entre la NSA y su equivalente británico, GCHQ, para derrotar a las formas más habituales de encriptación usadas en la protección de transacciones online, hasta iniciativas a menor escala con nombres que reflejan el espíritu despectivo y jactancioso que subyace a los mismos: JIRAFA EGOISTA, que capta el navegador TOR, que debe permitir el anonimato en la navegación online; MUSCULAR, un método para invadir redes de Google y Yahoo, y OLYMPIA, el programa de vigilancia que ejerce Canadá sobre el Ministerio de minas y energía de Brasil.[187]

Como lo menciona Glenn Greenwald, la agencia tenía una misión global: "Conseguir que ninguna comunicación electrónica escape de sus garras sistémicas."[188] Y es que muchos de los programas ni siquiera tenían que ver con la seguridad nacional, sino que incluso incluían temas de espionaje económico.

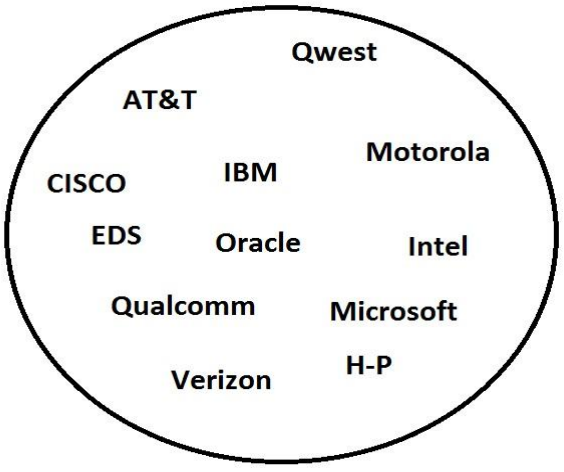
Por otro lado, vemos que toda la actividad intrusiva de la agencia tenía una razón de ser además de la búsqueda de terroristas. El nombre de dicha razón era Keith B. Alexander, general de 4 estrellas que dirigió la NSA desde 2005 hasta marzo de 2014 bajo el lema "Recogerlo todo" a tal magnitud que el reportero James Bamford lo definió como "el jefe de inteligencia más poderoso de la historia de la nación."[189]

[187] *Ibídem*, pp. 117 y 118.
[188] *Ibídem*, p. 118.
[189] *Ibídem*, p. 119.

De esta manera, “empezó a poner su filosofía en práctica en 2005, mientras recopilaba inteligencia de señales relativa a la ocupación de Irak […] Alexander acabó muy descontento con la limitada atención de la inteligencia militar norteamericana, concentrada en insurgentes sospechosos y otras amenazas para las fuerzas de EE.UU. […] <<Lo quería todo: todos los mensajes de texto, las llamadas telefónicas y los emails iraquíes que los poderosos ordenadores de la agencia pudieran captar>>.”[190] Llegaron incluso a captar más información de la que podían analizar o que resultara útil siquiera, pero no importaba porque cumplían con la meta de “Recogerlo todo”.

Otro elemento que Snowden envió en los documentos se refiere a las Operaciones de Fuentes Especiales o SSO (*Special Source Operations*) a las que califica como “La <<joya de la corona>> de la Organización”[191] pues son las empresas que le facilitan a la NSA los sistemas para obtener la información de las llamadas telefónicas y otros servicios de telecomunicaciones. Son las siguientes:

Se trata de empresas en los siguientes giros:
-Telecomunicaciones y proveedores de servicios de internet.
-Infraestructura de redes.
-Plataformas de hardware-Desktops/Servidores.
-Sistemas operativos.
-Software de aplicaciones.
-Hardware y software de seguridad.
-Integradores de sistemas.



Adaptación a partir de Greenwald, Glenn, p. 127.

[190] *Idem*
[191] *Ibídem*, p. 127.

Ahora bien, respecto a los programas revisados por las SSO, tenemos como los más importantes a: BLARNEY, FAIRVIEW, OAKSTAR y STORMBREW. Sobre el primero, el *Wall Street Journal* reveló que: "BLARNEY se basaba en una relación concreta: la que tiene con AT&T. De acuerdo con los propios archivos de la NSA, en 2010 la lista de países seleccionados por BLARNEY incluía Brasil, Francia, Alemania, Grecia, Israel, Italia, Japón, México, Corea del Sur y Venezuela, así como la Unión Europea y las Naciones Unidas."[192] Estos son países que representan objetivos de vigilancia, aunque algunos sean aliados también para EE.UU., solo que el trato que les den va a depender de qué tema se esté llevando.

Por otra parte, tenemos que el segundo programa de las SSO, FAIRVIEW, el cual "opera en Estados Unidos, pero tiene acceso a información que transita por el país y, mediante sus relaciones empresariales, proporciona acceso único a otras telecos y otros ISP (Proveedores de servicios de internet)."[193] Cabe mencionar que este programa se encuentra más regulado por sus socios y proveedores pero, de igual manera, representa un bastión esencial en cuanto a las posibilidades de la NSA de obtener la mayor cantidad de datos posibles.

Así, vemos que resulta crucial para la agencia colaborar no solo con socios estadounidenses, sino con extranjeros y agencias gubernamentales de otros países, por ejemplo, los de Polonia, tal como se opera el tercer programa mencionado: OAKSTAR. Respecto al mismo, podemos mencionar (basándonos en un documento filtrado por Snowden) lo siguiente:

> (TS//SI//NF) ORANGECRUSH, parte del programa OAKSTAR bajo la cartera empresarial de las SSO, comenzó a enviar metadatos desde una página web

[192] *Ibídem,* p. 129.
[193] *Ibídem,* p. 130.

> de un tercero (Polonia) a depósitos de la NSA desde el 3 de marzo, y contenidos desde el 25 de marzo. Esta empresa multigrupal inició su andadura en mayo de 2009 e incorporará el proyecto OAKSTAR de ORANGEBLOSSOM y su capacidad de DNR. El nuevo acceso proporcionará SIGINT desde enlaces comerciales gestionados por el socio corporativo de la NSA, y se prevé que incluya comunicaciones del ejército nacional afgano, oriente medio, parte del continente africano y Europa.
>
> Del mismo modo, el programa OAKSTAR aprovecha el acceso de uno de los <<socios>> corporativos de la agencia (Nombre en clave: STEELKNIGHT) a los sistemas extranjeros de telecomunicaciones, utilizando este acceso para desviar datos a sus propios almacenes.[194]

Finalmente, vemos que el cuarto programa más importante para las SSO de la NSA, el STORMBREW, aprovecha el "cuello de botella" que se genera en Estados Unidos respecto a todas las comunicaciones por internet, privilegio del que gozan por haber creado el mismo: "Entre tanto, el programa STORMBREW, dirigido en <<estrecha asociación con el FBI>>, da a la NSA acceso a internet y al tráfico telefónico que entra en suelo norteamericano por varios <<cuellos de botella>>. Saca partido del hecho de que casi todo el tráfico mundial de internet fluye en algún momento por la infraestructura de comunicaciones de Estados Unidos, un subproducto residual del papel central desempeñado por EE.UU. en la creación de internet."[195] Es gracias a todos estos programas, acuerdos, socios y demás, que el país norteamericano ha podido obtener tanta información de gente de cualquier punto del planeta. Esto lo obtienen por cualquier medio, si no es por las buenas relaciones que mantienen con otros países – no solo con los integrantes de los Cinco Ojos, sino como vemos también con Polonia - se valen igualmente de sus privilegios sobre el Internet para abrirse paso en la comunidad internacional con ayuda de las herramientas tecnológicas.

[194] *Ibídem,* p. 131.
[195] *Ibídem,* p. 132.

Los programas mencionados operan para obtener la información a través de los cables de fibra e infraestructura como tal, pero la NSA también lo ha logrado a través de otro programa llamado PRISM. Se trata del programa principal referente a la recogida masiva de datos por parte de la NSA, pero a través de las empresas que conocemos como "los gigantes de Internet" entre los cuales encontramos a Microsoft, Google, Yahoo o Facebook. Muchas de estas empresas han negado reiteradamente este apoyo a la NSA, pero es gracias a los documentos filtrados por Snowden que nos dimos cuenta de la verdad al respecto. También es probable que estas empresas no estuvieran realmente enteradas, puesto que la agencia, como vemos, tiene la capacidad de obtener la información por infinidad de medios gracias a los socios que apoyan en los programas de las SSO, por lo que los empleados de la NSA pueden obtener los resultados que buscan sin tener interacción alguna con las empresas involucradas.

Para terminar, cabe mencionar también a la División de Operaciones de Acceso a Medida o TAO (*Tailored Access Operations*), la cual constituye a la Unidad de hackers de la agencia, quienes se encargan de infectar a los ordenadores instalando malware para vigilar a los usuarios. Según un documento de la NSA, se nos informa que "la agencia ha conseguido infectar al menos 50 mil ordenadores individuales con un tipo de malware llamado <<Quantum Insertion>>"[196]. De esta manera, llegan a tener acceso a todo lo que los usuarios teclean y a lo que aparece en sus pantallas, consolidando así su poder como el "Gran Hermano" o el "Ojo que todo lo ve" que tan cándidamente nos presentaban escritores de ficción como George Orwell o J.R. Tolkien.

[196] *Ibídem,* p. 146.

4.1.3.1. Las relaciones internacionales en el marco del espionaje de la NSA y respuesta de Estados Unidos

> ¿Qué país no quiere convertir el mundo en un lugar mejor…para él mismo?
>
> - Frase en documento de la NSA, filtrado por Snowden.

Para comenzar este tema, es conveniente mencionar que Estados Unidos divide a los países con los que mantiene relaciones –más allá de las diplomáticas, económicas, o de cooperación – de alianza respecto al espionaje y la vigilancia. Esta división se da en 3 grupos: (I) sus principales aliados; (II) los que se encuentran entre aliados y objetivos de vigilancia; y (III) los que son enemigos o no alcanzan el nivel de aliados y por lo tanto son los objetivos principales para el espionaje.

Dentro de la primera categoría se encuentran los países de los Cinco Ojos, con quienes Estados Unidos hace alianza para espiar a otros, pero casi nunca en ellos, a menos que lo soliciten. El aliado más importante para la NSA dentro de este grupo es el Reino Unido, representado más específicamente por el GCHQ (*Government Communications Headquarters*), uno de sus servicios de inteligencia.

De igual manera, se puede ver que los miembros de los Cinco Ojos – exceptuando a EE.UU. – muchas veces ceden ante los deseos de la NSA o les solicitan apoyo para espiar a su propia población y controlar alguna situación que consideren se está saliendo de control. Por ejemplo, tenemos que “en 2011, el gobierno australiano suplicó explícitamente a la NSA que ampliara su <<sociedad>> y sometiera a sus propios ciudadanos a una mayor vigilancia. El subdirector interino de la Dirección de Señales de Defensa de la Inteligencia Australiana (DSD) escribió

a la Dirección de Inteligencia de Señales de la NSA, que Australia <<actualmente afronta una amenaza siniestra y resuelta procedente de extremistas del "país" activos tanto dentro del territorio nacional como en el extranjero>>. Solicitaba una mayor vigilancia de las comunicaciones de los ciudadanos australianos considerados sospechosos por el gobierno."[197] Así, vemos el poder con el que cuenta el líder del grupo no solo para lograr que sus miembros lo apoyen en sus requerimientos respecto a vigilancia desde sus territorios a posibles "terroristas" o alguna otra necesidad que tengan para salvaguardar su seguridad nacional, sino que estos países le dan la batuta al mismo EE.UU. para que se encargue de sus asuntos internos.

Ahora bien, dentro del segundo grupo, se encuentran "los aliados de <<grado B>> de la NSA: Países que mantienen una colaboración limitada con la NSA y son a la vez seleccionados para vigilancia agresiva no solicitada."[198] Aquí podemos encontrar países que suelen ser aliados de EE.UU. en otros aspectos, pero que en cuestión de vigilancia representan objetivos importantes. También cabe mencionar que a muchos de estos, EE.UU. les paga para que desarrollen tecnologías de vigilancia y así tengan una razón para poder involucrarse en el proceso. A los dos primeros grupos los podemos encontrar divididos como socios en segundo y tercer grado en el cuadro de la siguiente página:

[197] *Ibídem*, p. 152
[198] *Ibídem*, p. 153.

Socios en segundo grado	Socios en tercer grado		
Con quienes se mantiene una relación de cooperación exhaustiva.	Con quienes se mantiene una relación de cooperación específica.		
Australia	Alemania	Finlandia	Países Bajos
Canadá	Arabia Saudita	Francia	Pakistán
Nueva Zelanda	Argelia	Grecia	Polonia
Reino Unido	Austria	Hungría	República Checa
	Bélgica	India	Rumania
Coaliciones / Multilaterales	Corea del Sur	Israel	Singapur
	Croacia	Italia	Suecia
AFSC	Dinamarca	Japón	Tailandia
OTAN	Emiratos Árabes Unidos	Jordania	Taiwan
SSEUR	España	Macedonia	Tunez
SSPAC	Etiopía	Noruega	Turquía

Adaptación a partir de Greenwald, Glenn, pp. 153 y 154.

Para ejemplificar, podemos considerar a un país como Israel que puede ser un gran aliado de EE.UU. en muchos aspectos, incluyendo el de la vigilancia, pero que también puede ser objetivo, derivado de las actividades de espionaje que muchos israelíes realizan en contra del país norteamericano.

Finalmente, en el último grupo encontramos a los "países que suelen ser objetivos pero nunca socios de EE.UU. en los programas de espionaje. Entre ellos se incluyen, como era de esperar, gobiernos considerados adversarios, como los de China, Rusia, Irán, Venezuela y Siria; pero también otros cuya condición oscila entre la de amigo y neutral, como Brasil, México, Argentina, Indonesia, Kenia y Sudáfrica."[199] Ahora bien, resulta natural pensar que las naciones se espíen entre

[199] *Ibídem,* p. 157.

sí, ya que llevan años haciéndolo; sin embargo, respecto a los países que se vieron envueltos en escándalos de espionaje con EE.UU., este les tuvo que responder debido a que no sólo estaban los dirigentes o diplomáticos involucrados, sino sus empresas y su propia población. De manera que, si no establecían una postura condenatoria a las acciones de la NSA, podían quedar mal ante la opinión pública o incluso, podrían causar revueltas por lo mismo, puesto que un pueblo desprotegido cuenta con las razones suficientes para ponerse en contra de su gobierno.

Derivado de todo esto, es que Estados Unidos se está viendo en la necesidad de incluir al Internet y varias tecnologías dentro de su lista de enemigos:

La amenaza actual			
Hackers	Satélites	Inalámbricos	Facsímiles
Personas con acceso a información confidencial	Inteligencia extranjera tradicional	Circuitos de alta velocidad	Buscapersonas (pagers)
Internet	Países en desarrollo	Terroristas	Elementos criminales

Adaptación a partir de Greenwald, Glenn, p. 211.

Gracias a esto, podemos comprender por qué el gobierno de Estados Unidos condenó tan arduamente las acciones de los tres famosos “soplones” mencionados a lo largo de este capítulo. Realmente, no era tanto porque le preocupara la seguridad de su país como tal, pues no se generaría una guerra a causa de las filtraciones, pero sí dañaban su reputación como defensor de las libertades y la justicia en el mundo, le ocasionaron costos pues tuvieron que dar explicaciones a los afectados (directa e indirectamente) así como cancelar varios de sus programas de vigilancia, aunque seguramente llevarán a cabo otros más avanzados, más

difíciles de detectar o quizá desarrollarán técnicas de seguridad interna más fuertes para que aquellos que encuentren algo inhumano o que vaya contra la moral o incluso la seguridad de la gente, no puedan extraer y filtrar la información.

Se trata de un objetivo que parece difícil de alcanzar para el gobierno estadounidense, pero si desea mantener su puesto como “el país más poderoso” o, al menos no bajar muchos peldaños en la carrera internacional, tendrán que llevar a cabo muchas medidas para proteger más sus intereses, sobre todo políticos, pero adentrándose también en lo económico y tecnológico, naturalmente.

Conclusiones.

Como se mencionaba al comienzo del presente escrito, el objetivo era dar a conocer el conflicto de la filtración de información dentro del fenómeno de la guerra cibernética estadounidense considerando la hipótesis de que el poder del internet en las Relaciones Internacionales está poniendo en tela de juicio el control que el Estado y los Servicios de Inteligencia pueden tener en la Política Exterior de un país, así como la pregunta principal de investigación: ¿En qué medida el Internet puede ser una herramienta o un enemigo para los gobiernos y la sociedad internacional?

Por consiguiente, a lo largo del escrito encontramos que los gobiernos continúan tratando de defender sus propios intereses a costa de las libertades civiles, incluyendo la privacidad en línea, cuestión en la que la sociedad se encuentra en constante desacuerdo pues existen los que defienden el lema de que “es el precio que hay que pagar por usar el internet” mientras que otros consideran que merecen el mismo respeto a su privacidad como si se tratara de su casa o cualquier bien que posean en donde las autoridades no tienen derecho a entrar si no es con un permiso previo.

No obstante, es importante mencionar que a la misma población le hace falta informarse más respecto a su seguridad informática, ya que muchos no cuentan con antivirus o programas o aplicaciones de encriptación de la información que comparten, y muchas veces observamos que ni siquiera les interesa, entonces a final de cuentas, es como si no les importara cerrar su casa con llave para impedir que los intrusos entren. Por lo que, para vivir en una sociedad donde se respete verdaderamente la privacidad de la población en todos los medios, necesitamos informarnos dado que resulta mucho más complicado evitar que existan intrusos en el mundo que saber cómo defendernos de ellos.

Dado que en muy pocos países en el mundo, al Estado realmente le importa que su población cuente con los recursos suficientes para subsistir en el mismo, incluyendo los medios electrónicos y la conexión a Internet, lo que debemos hacer es trabajar en conjunto como "pobladores del mundo" – título que la "globalización divergente" mencionada por Fernando Peirone nos permite portar – para que a través de la "inteligencia colectiva" podamos potencializar nuestras habilidades y conocimientos y que así, el poder de la ciudadanía sea explotado a través de los diferentes medios que existen y haya mayor cercanía con sus gobiernos. Esto considerando que hay una correspondencia innegable entre el nivel de compromiso cívico de la población con la calidad de su gobierno, así como entre la ciudadanía digital y el gobierno abierto, que se puede considerar cada vez más como un requisito en lugar de una opción de gobernanza.

Ahora bien, referente a la teoría seleccionada para esta tesis: el Neorrealismo estructural, vemos que se puede aplicar en el tema de la nueva estructuración de la "sociedad red" puesto que existen nuevos actores y poderes de contrapeso a considerar en la estructura de la sociedad internacional. Con esto, no se pretende nulificar el poder institucional que tiene el Estado, el ejército, los diplomáticos y en general todos los actores tradicionales, sino incluir a todos aquellos que están surgiendo en nuestros días tales como las organizaciones no gubernamentales, los grupos activistas con diferentes intereses y propósitos (políticos, sociales, medio ambientales, eclesiásticos, entre otros), asociaciones de inmigrantes (y todo lo que las diásporas traen consigo a los países que los reciben), empresas, inversores y un sinfín de nuevos actores.

Ahora lo que nos queda es ver si el rumbo que tomará la sociedad internacional será hacia una mayor apertura en redes pero manteniendo privado lo que el usuario especifique desea mantener como tal o si los gobiernos continuarán tomando la información útil para sus fines sin importar lo que pensemos al respecto

o las acciones contraproducentes que esto les podría acarrear tanto en el ámbito interno como en su imagen al exterior.

Como lo vimos a lo largo del escrito, dado que muchos estadounidenses, desde el 11 de septiembre de 2001 a la fecha, han cambiado drásticamente su opinión de un apoyo ferviente al gobierno y su guerra contra el terrorismo hacia una baja credibilidad en la misma y, más bien, ha ido al alza la lucha por las libertades en internet y el respeto a los derechos de los usuarios; considero que el gobierno de Donald Trump tendrá que comenzar a respetar más a sus ciudadanos en estos aspectos o saldrán a la luz más temas como el escándalo de *Facebook* y *Cambridge Analytica* respecto al uso de la red social para la obtención de información de los votantes y la influencia que se pretendió generar en sus opiniones desde las redes para las elecciones de 2016.

O bien, el presidente Trump tendrá que aplicar la estrategia de su campaña y de sus primeros años de gobierno y exacerbar de nuevo el odio de los ciudadanos pero ahora para con los terroristas o el enemigo que surja eventualmente, y así poder justificar la vigilancia de nueva cuenta. Aunque a mi parecer esto no podrá resultar muy sencillo puesto que la gente ya no considera que valga la pena darle muchas libertades al gobierno bajo la supuesta finalidad de la salvaguarda de su propia seguridad.

En los últimos años, ha habido incluso experimentos psicológicos en los que se observa que el comportamiento de las personas cambia cuando se saben observados. Por lo que considero que debemos informarnos sobre la seguridad cibernética para evitar que el gobierno o, como ahora podríamos llamarle, “El gran hermano” hablando en términos Orwellianos, nos tenga controlados y que al sabernos vigilados, nos volvamos más fáciles de gobernar.

Considero que esta tesis cumple con la hipótesis, tan solo haciendo referencia a los movimientos que se orquestaron en red a principios de esta década, a través de los cuales se pudo observar cómo el poder de la gente se veía exacerbado gracias a las posibilidades que el Internet les ofrecía. Minimizando de esta manera, el control que sus gobiernos podían ejercer sobre ellos, dado que en cuestión de segundos los “pobladores del mundo” sabíamos lo que estaba pasando, lo cual generó un aumento en la cohesión de la sociedad en varios puntos del planeta, haciendo así realidad lo que Zbigniew Brzezinski decía: “es infinitamente más fácil matar a un millón de personas que controlarlas”.

FUENTES DE CONSULTA

Bibliografía:

Adame Alemán, Juan Pablo. *Ciudadanía digital ¿Oportunidad o amenaza?* Imagia Comunicación, S. de R.L. de C.V. México, 2015.

Andrews, Lori. *I know who you are and I saw what you did. Social networks and the death of privacy.* Free Press, New York, 2011.

Berkowitz, Peter (ed.) *The future of american intelligence*. Hoover Institution Press, California, 2005.

Castells, Manuel. *Redes de indignación y esperanza. Los movimientos sociales en la era de internet*. Alianza Editorial, Madrid, 2012.

García-Mexía, Pablo. "WikiLeaks is an abuse of Internet Freedom" en Tamara Thompson (ed.) *WikiLeaks*, Greenhaven Press, Estados Unidos, 2013.

Greenwald, Glenn. *Snowden. Sin un lugar donde esconderse.* Ediciones B S.A., Barcelona, 2014.

Gutiérrez Pantoja, Gabriel. *Teoría de las Relaciones Internacionales*. Oxford University Press-HARLA México S.A. de C.V., México, D.F., 1997.

Leigh, David y Harding, Luke. *WikiLeaks y Assange. Un relato trepidante sobre cómo se fraguó la mayor filtración de la historia*. Ediciones Deusto, México D.F., 2011.

Miller-Jones, Edward R. *WikiLeaks. Removing the "top secret" seal*. Fastbook Publishing, Estados Unidos, 2010.

Moser, Claus, 1980, p.4. Citado por Webster, Frank en *Theories of the information society*, segunda edición, Routledge, Londres, 2002.

Naím, Moisés. *El fin del poder*. Random House Mondadori, S.A., Barcelona, 2013.

Peirone, Fernando. *Mundo extenso. Ensayo sobre la mutación política global*. Fondo de Cultura Económica, Buenos Aires, 2012.

Perry, David L. *Partly Cloudy. Ethics in war, espionage, covert action, and interrogation*. The Scarecrow Press, Inc., Estados Unidos de América, 2009.

Sanger, David. "How our diplomats think" en: Star, Alexander (ed.). *Open secrets: WikiLeaks, War and American Diplomacy*. Grove Press, Nueva York, 2011.

Shulsky, Abram N. y Schmitt, Gary J. *Silent warfare. Understanding the world of intelligence.* Brasseys, inc. Washington, D.C., 2002

Stiennon, Richard. *Surviving cyberwar*. The scarecrow press, inc., Estados Unidos de América, 2010.

Hemerografía:

AFP. "Advirtió la CIA a Obama que Rusia quería hackear elecciones" en *La Jornada en línea*, sección Mundo, viernes 24 de junio de 2017, Recuperado de: http://www.jornada.unam.mx/2017/06/24/mundo/020n1mun Consultado el 21 de febrero de 2018.

Agencias. "China buscará modernización en Internet" en *La Jornada en línea*, Sección Economía, 26 de diciembre de 2017, Recuperado de: http://www.jornada.unam.mx/2017/12/26/economia/018n3eco Consultado el 21 de febrero de 2018.

Agencias AP y EFE. "China moderniza su ejército para ciberguerra y espacio" en *El Universal*, Sección Mundo, p. A22, 3 de enero de 2016.

Casciari, Hernán. "Más respeto que soy tu crisis" (entrevista) en suplemento *Radar*, 19 de febrero de 2012, p. 12.

Dargis, Manohla. "Reseña: En 'Los archivos del Pentágono', la democracia sobrevive a la oscuridad" en *The New York Times* en español, Sección Cine, 2 de enero de 2018, Recuperado de: https://www.nytimes.com/es/2018/01/02/resena-en-los-archivos-del-pentagono-la-democracia-sobrevive-a-la-oscuridad/ Consultado el 10 de abril de 2018.

Hernández, Jaime J. "Ciberguerra, las batallas del siglo XXI" en *El Universal*, México, Sección Mundo, 16 de agosto de 2015. Recuperado de: http://www.eluniversal.com.mx/articulo/mundo/2015/08/16/ciberguerra-las-batallas-del-siglo-xxi Consultado el 12 de mayo de 2016.

Ibáñez, Josep. "Globalización e Internet: Poder y gobernanza en la sociedad de la información" en *Revista Académica de Relaciones Internacionales*, No. 5, Noviembre de 2006, UAM-AEDRI, p 2. Recuperado de: http://www.relacionesinternacionales.info/ojs/article/view/38.html Consultado el 19 de noviembre de 2014.

Jiménez, María Fernanda. "Redes, arma de doble filo para El Bronco" en *El Universal*, sección Estados, 14 de febrero de 2016, p. 22.

Jiménez Cano, Rosa. "Los peores ataques cibernéticos en EE UU" en *El País*, sección Internacional, 4 de junio de 2015, Recuperado de: https://elpais.com/internacional/2015/06/05/actualidad/1433461961_205806.html Consultado el 21 de febrero de 2018.

Márquez, William. “¿Qué pasó con los otros soplones de Estados Unidos?” en *BBC Mundo*, Reino Unido, Sección Internacional, 27 de junio de 2013. Recuperado de: http://www.bbc.com/mundo/noticias/2013/06/130626_eeuu_otros_soplones_wbm Consultado el 11 de mayo de 2016.

Notimex y EFE. “Francia podrá juzgar a Facebook por censura” en *El Universal,* Sección Mundo, 13 de febrero de 2016, p. 30.

Pardo, Pablo. “Estados Unidos investiga un ciberataque a gran escala” en *El Mundo*, sección Tecnología, 21 de octubre de 2016, Recuperado de: http://www.elmundo.es/tecnologia/2016/10/21/580a7bda468aeb94588b4666.html Consultado el 21 de febrero de 2018.

Peschard, Jacqueline. “Assange: los secretos a debate” en *El Universal*, sección Opinión, 8 de febrero de 2016, p. 28.

PJ Crowley, exsecretario de Estado asistente del presidente Barack Obama. En: Redacción. “Los dilemas del caso del soldado Manning” en *BBC Mundo*, Reino Unido, Sección Internacional, 03 de junio de 2013. Recuperado de: http://www.bbc.com/mundo/noticias/2013/06/130603_internacional_bradley_manning_eeuu_audiencia_nc_lav Consultado el 11 de mayo de 2016.

Posada García, Miriam. “Se logró contener unos 170 mil ataques cibernéticos contra el Estado: funcionario” en *La Jornada en línea*, Sección Economía, Jueves 8 de septiembre de 2016, Recuperado de: http://www.jornada.unam.mx/2016/09/08/economia/022n1eco Consultado el 21 de febrero de 2018.

Redacción. “APT33, el grupo de hackers iraní al que se atribuyen ataques a Estados Unidos, Arabia Saudita y Corea del Sur” en *BBC Mundo*, sección Tecnología, 16 de octubre de 2017, Recuperado de: http://www.bbc.com/mundo/noticias-41637526 Consultado el 21 de febrero de 2018.

Reuters. “Irán acusa a Siemens de ataque cibernético” en *La Jornada en línea*, Sección Mundo, 18 de abril de 2011, Recuperado de: http://www.jornada.unam.mx/2011/04/18/mundo/027n1mun Consultado el 21 de febrero de 2018.

Reuters. “Ponen límites a espionaje a europeos” en *El Universal*, domingo 28 de febrero de 2016, sección Mundo, p. 27.

Sánchez Jiménez, Arturo. “Al alza, ataques cibernéticos, alerta académico” en *La Jornada en línea*, Sección Política, domingo 5 de febrero de 2017, Recuperado de:

http://www.jornada.unam.mx/2017/02/05/politica/009n2pol Consultado el 21 de febrero de 2018.

Vargas Aguilar, Simón. “Guerra cibernética: la nueva amenaza” en *La Jornada*, México, Sección Opinión, 5 de julio de 2013. Recuperado de: http://www.jornada.unam.mx/2013/07/05/opinion/018a2pol Consultado el 06 de marzo de 2018

Vargas Hernández, José Guadalupe. “El Realismo y el Neorrealismo estructural” en *Estudios Políticos*, Novena época, núm. 16, enero-abril, 2009. p 113.

Wegener, Henning. “La Guerra Cibernética” en *Política Exterior,* No. 80, Marzo-abril 2001, p 131. Recuperado de: https://www.unibw.de/infosecur/documents/published_documents/guerra_cibernetica Consultado el 19 de noviembre de 2014.

Zittrain, Jonathan y Sauter, Molly. Trad. Francisco Reyes. “Todo lo que necesitas saber sobre Wikileaks” en *MIT Technology Review*, 9 de diciembre de 2010. Recuperado de: https://www.technologyreview.es/s/1647/todo-lo-que-necesitas-saber-sobre-wikileaks Consultado el 10 de abril de 2018.

Cibergrafía:

(s.a.) Quees.la. *¿Qué es espionaje?* (s.f.) Recuperado de: http://quees.la/espionaje/ Consultado el 10 de septiembre de 2014

(s.a.) *Seguridad Nacional: Definiciones y conceptos*. (s.f.) p 9, recuperado de: http://catarina.udlap.mx/u_dl_a/tales/documentos/lri/munoz_p_ba/capitulo1.pdf Consultado el 11 de septiembre de 2014.

(s.a.) *Botnet*. Consultado en: https://www.linguee.es/espanol-ingles/search?source=ingles&query=botnet el 06 de marzo de 2018.

Casciari, Hernán. *Para ti, Lucía*. 21 de diciembre de 2011. Disponible en línea: http://orsai.bitacoras.com

CISEN. *Amenazas y riesgos*. (s.f.) Recuperado de: http://www.cisen.gob.mx/snAmenazasRiesgos.html Consultado el 11 de septiembre de 2014.

CISEN. *Seguridad Nacional*. (s.f.) Recuperado de: http://www.cisen.gob.mx/snSegNal.html Consultado el 11 de septiembre de 2014.

Gonggrijp, Rop. Discurso de apertura al 27° Congreso de Chaos Computer Club (CCC), Berlín, 27 de diciembre de 2010. Disponible en línea: http://rop.gonggri.jp/?p=438

Uzal, Roberto. *Guerra Cibernética: ¿Un desafío para la Defensa Nacional?* (s.f.) Recuperado de: http://esgcffaa.mil.ar/numero7/40.html Consultado el 19 de noviembre de 2014.

Diccionarios:

Real Academia Española. *Diccionario de la Lengua Española*. Tomo 1. Editorial Espasa Calpe, S.A. España, 2002.