UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

CENTRO DE RELACIONES INTERNACIONALES

LA ERA DE VIGILANCIA DE OBAMA

T E S I S

QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN RELACIONES INTERNACIONALES

P R E S E N T A

ATENEA ROMINA GONZÁLEZ VELA

Director de Tesis:

Dra. Ismene Ithaí Bras Ruíz

Ciudad Universitaria, CDMX 2016

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

ÍNDICE

ÍNDICE DE SIGLAS Y ABREVIATURAS

AFI	Air Force Intelligence
AI	Army Intelligence
CC	Comando Combativo
CGI	Coast Guard Intelligence
CIA	Central Intelligence Agency
CMF	Fuerzas de Misiones Cibernéticas
CNO	Computer Network Operations
CS&C	Office of Cybersecurity and Communications
CSC	Complejo de Seguridad Centrado
DARPA	Defense Advanced Research Projects Agency
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DNS	Domain Name System
DoD	Department of Defense
DOJ	Department of Justice
DT	Department of Treasury
ED	Department of Energy
FBI	Federal Bureau Institute

FISA	Foreign Intelligence Surveillance Act
GCHQ	Government Communications Headquarter
IA	Information Assurance
IC	Comunidad de Inteligencia
IP	Internet Protocol
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISC	International Strategy on Cybersecurity
ISO	International Standard Organisation
ISR	Inteligencia, Vigilancia y Reconocimiento
MCI	Marine Corps Intelligence
MIP	Military Intelligence Program
MSC	Mini Complejos de Seguridad
NCCIC	National Integration Center Cybersecurity and Communications
NECP	Plan Nacional de Comunicaciones de Emergencia
NGA	National Intelligence-Geospatial Agency
NI	Navy Intelligence
NICCS	National Initiative for Cybersecurity Careers and Studies
NIP	National Intelligence Program
NRO	National Reconnaissance Office
NSA	National Security Agency
NVD	National Vulnerability Database
QDRR	Quadrennial Defense Review Report

SD	Department of State
SI	Seguridad de la Información
SIGINT	Signals Intelligence
SOPA	Stop Online Piracy Act
STRATCOM	U.S. Strategic Command
TAO	Tailored Access Operations
TIC	Tecnologías de la Información y Comunicación
UAS	Sistemas de Aeronaves No-tripuladas
UNISDR	United Nations Office for Disaster Risk Reduction
US-CERT	United States Computer Emergency Readiness Team
USAF	Fuerza Aérea
USCYBERCOM	U.S. Cyber Command
USSOCOM	U.S. Special Operations Command

ÍNDICE DE MAPAS, GRÁFICAS, ESQUEMAS Y TABLAS

INTRODUCCIÓN

El orden internacional del siglo XXI ha demostrado que los conceptos de: seguridad nacional, amenaza, riesgo y peligro, contienen una alta complejidad desde su definición hasta su aplicación, ya que los factores, objetivos y contextos que los definen son cambiantes y temporales.

Tras la evolución de las amenazas hacia Estados Unidos, se han vislumbrado peligros emanados fuerzas tradicionales (léase Estados) y emergentes, como lo son aquellas que afectan a la ciberseguridad para la nación estadounidense que, debido a la programación de los sistemas, de las infraestructuras críticas y la conexión de las mismas al Internet, las podemos encontrar incluidas en el *National Security Strategy report 2015*, desarrolladas e identificadas como: aquellos países maliciosos, criminales, actores individuales que tratan de evitar tales atribuciones de dañar la infraestructura de red estadounidense desconociendo sus actos ilegales. [1]

Estados Unidos reconoce que el mundo comparte espacios entre sí; el ciberespacio es uno de ellos, que promueven el libre flujo de personas, servicios, mercancías, ideas y que es un espacio esencial para el desarrollo de los individuos *per se*. Uno de los problemas que enfrentan los gobiernos al momento de construir medidas de protección contra las ciberamenazas es la delimitación del campo de acción de las mismas, el ciberespacio, puesto que es difícil marcar un límite o dimensión del mismo.

Entre las áreas consideradas vulnerables para los Estados Unidos a agresiones por las amenazas del siglo XXI, son: el ciberespacio, el espacio, el aire y el océano; áreas compartidas por la humanidad y que son retomadas por Estados Unidos para realizar un esfuerzo conjunto con programas y acciones

[1] The White House, *National Security Strategy Report 2015* , Disponible en línea: https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf Consultado: Octubre de 2015.

colectivas, mientras que la procuración del ciberespacio será ejecutada y resguardada dentro de lo posible por el *Department of Homeland Security* con las fuerzas armadas de este país en detrimento de los riesgos que las amenazas representan para este ámbito.

Cabe señalar que durante la Guerra Fría y la Post-Guerra se mantiene una vigilancia selectiva con amenazas no tradicionales, que poseen temporalidad y contexto y por ende, no se pueden considerar las mismas durante toda la historia pero lo que se pone en riesgo continúa siendo vigente, la patria.

Es así que Estados Unidos, como el país donde se creó Internet mediante el programa ARPANET, siente la necesidad de proteger la operatividad y la estabilidad de la Red debido a que el desarrollo económico, político y social, entre otros, dependen del gran avance tecnológico y digital del país; donde el gobierno electrónico va en crecimiento y la digitalización de la información crítica para empresas e instituciones se encuentra en un nivel alto, que conlleva ventajas como la fluidez de los datos y la información para realizar actividades, y desventajas como lo es el robo de datos e intrusiones a los sistemas operativos para ocasionar fallas.

Asimismo, el Global Risk Report 2016 muestra que el impacto que tiene un ciberataque actualmente supera el de una escasez de comida, un conflicto entre Estados o el tráfico ilícito y en cuanto a su probabilidad de ocurrencia es mayor que un ataque terrorista; en resumen, un ciberataque cuenta con 4.9 puntos de impacto y 5.1 de probabilidad de ocurrencia en una escala del 1 al 7 utilizada por esta fuente. En el mismo reporte, se presenta un mapa de riesgos por región en el que los principales riesgos para Estados Unidos este 2016 son los ciberataques, el fraude cibernético y el robo de información. Sin embargo, los riesgos dentro del ciberespacio no figuran dentro de la agenda global, por lo que la ciberseguridad, es meramente de interés estadounidense.

Dicho lo anterior, Estados Unidos considera que tiene la obligación de asegurar su infraestructura y asumir la "responsabilidad de liderar el mundo conectado a la red".[2] Por lo que dentro de las políticas de Seguridad Nacional en torno al ciberespacio, durante el periodo de Barack Obama, se han establecido directrices y marcos jurídicos que violan las libertades individuales que responden a ciertas agresiones hacia el Estado norteamericano;[3] como claro ejemplo es el abuso de los mecanismos de vigilancia del país para espiar a sus ciudadanos y a otros Estados, como la privación de la libertad de expresión con el caso emblemático de la ley SOPA (Stop Online Piracy Act) y la persecución de los *whistle-blowers*.

Sin embargo, las metas u objetivos hacia los que las políticas de Barack Obama se han enfocado en la vigilancia en masa fortalecida por los distintos mecanismos del complejo de vigilancia, ciberdefensa y ciberseguridad. La aparición de Wikileaks y Edward Snowden son detonadores de una crisis en el complejo de vigilancia que surge en contra del espionaje y el mantenimiento del poder político de los Estados Unidos basado en el manejo de información confidencial y el chantaje a través de los mecanismos de vigilancia establecidos por la institución más ponderosa en este rubro, la NSA.

Es así que nuestra hipótesis general intentará probar que el gobierno estadounidense ha construido un complejo de vigilancia como parte de una estructura de defensa –que funciona tanto al interior como al exterior-, dotándolo de infraestructura, una normatividad, que le han permitido establecer un *estatus quo* de un vigía permanente. No obstante lo anterior, las consecuencias del ambicioso plan de Estados Unidos por integrar al ciberespacio a su poder nacional, ha tenido severas consecuencias en el escenario internacional, gracias a las filtraciones de información, que le restan legitimidad y dañan su imagen como

[2] *Ídem*
[3] En este trabajo se abordarán pero de una manera general, sin llegar al escrutinio de las características de la ciudadanía y sus libertades aceptadas en la Constitución de los Estados Unidos y sus enmiendas.

el “hegemón” que ha determinado las políticas de seguridad internacional en este siglo; por ende, el motivo de este trabajo es presentar la construcción de tres complejos principales que integran el complejo de seguridad centrada, el complejo de ciberdefensa, el complejo de ciberseguridad y, haciendo un énfasis en el último, el complejo de vigilancia.

Es así que el objetivo general de esta investigación radica en analizar el desarrollo de las políticas internas que fortalecieron la estructura de vigilancia; el marco regulatorio, que violenta la Constitución, así como los mecanismos de ciberdefensa dirigidos por el *Department of Defense* (DoD), que son ejes que han venido dictando las directrices de la política de seguridad nacional estadounidense bajo excusa de fortalecer la ciberseguridad. De esta manera, es menester de esta tesis presentar las actividades que realiza la *National Security Agency* (NSA) que conllevan el incremento de la vigilancia dentro y fuera de Estados Unidos, que sin duda han tenido un alto impacto político (y costo) para la administración de Obama, quien en algún momento de su primer campaña presidencial y aún siendo Senador, negó tener políticas rígidas (y anti-constitucionales) como las de la administración de George Bush con la ley Patriota.

De este modo es preciso hacer una explicación del Complejo de Seguridad Centrada que representa la determinación de las políticas de seguridad del centro a la periferia, en donde el concepto de seguridad nacional aparece como motor principal para la construcción de las mismas y que moldean la visión de la guerra y las amenazas inmersas en el ciberespacio. Sin duda, un factor fundamental para la determinación de dichas estrategias de seguridad nacional es la evaluación de riesgos y la definición de las amenazas.

Bajo este tipo de evaluaciones y diagnósticos de riesgos y amenazas, la ciberseguridad figura como un pretexto gubernamental para desarrollar sus capacidades de vigilancia con el uso del ciberespacio, aunque cabe aclarar que el desglose de la composición del ciberespacio no es el propósito principal de ésta

tesis, sí lo es el analizar la evolución del uso de la tecnología y la cibernética para el poder y el manejo del lenguaje sensacionalista que ha disfrazado éstos objetivos con la finalidad de desarrollar las capacidades gubernamentales de "saberlo todo" y espiar a sus contras.

Un segundo objetivo específico es presentar dos de las estructuras del complejo que tienen gran aporte para la vigilancia como lo son el de la ciberdefensa y ciberseguridad, planteando los antecedentes legales y políticos en donde se empieza a delimitar el rumbo de las estructuras y las fuerzas armadas, que a la llegada de Barack Obama al poder, suman un esfuerzo emblemático por expandir las influencias, la capacidad de imposición y el poder del país a través del quinto espacio. A pesar de hacer un breve recuento de los antecedentes más ejemplares, se excluye de este trabajo hacer un recuento de las estrategias de política exterior de cada uno de los presidentes, considerando que se parte de un conocimiento previo sobre la materia.

Un tercer objetivo específico es mostrar la crisis del complejo de vigilancia que ha puesto en jaque la imagen de la autoridad y el imaginario construido para extensión del control y poder a través de las redes y la obtención de información personal y estratégica de los individuos de interés gubernamental. De esta forma, la NSA figura como la agencia gubernamental más emblemática sobre la vigilancia electrónica y la más dañada públicamente, gracias a la respuesta de ciudadanos y grupos anti-vigilancia, cabe aclarar que no es el propósito de esta tesis describir cada uno de ellos, pero sí presentar dos ejemplos únicos que son pilar de la crisis del complejo de vigilancia, Wikileaks como prensa libre que divulga cables y documentos oficiales obtenidos por funcionarios que trabajan en los mecanismos y corporaciones de vigilancia, y como segundo ejemplo se encuentra Edward Snowden como el enemigo público número uno del complejo al exponer los métodos de proceso y recolección de información personal en masa de ciudadanos estadounidenses y de otros países del mundo.

El enfoque teórico que este trabajo recupera es la escuela neorrealista puesto que el objeto de estudio presenta las características de: estatocentrismo, polaridad del poder entre las superpotencias, la distribución del material de poder que determina la estructura política global y su balance de poder. En este sentido, los catedráticos que retomaremos son Barry Buzan y Ole Weaver, quienes dominan la teoría sobre la construcción de los complejos de seguridad centrado por parte de las superpotencias, cuya perspectiva es neorrealista y presenta la ambición y rivalidad de los Estados por demostrar una nueva forma de poder a través de todos los niveles, y en este caso será aplicada al ciberespacio.

De este modo, el complejo de seguridad centrado se encuentra dominado por un solo nivel global de poder, o en otros términos, una superpotencia cuyas características es poseer capacidades político militares de primera clase y una economía que sustente estas capacidades, deben ser capaces de tener y también de ejercer éstas con alcance global. Asimismo, las superpotencias tienen que verse y ser aceptadas por otros en retórica y comportamiento. Deben ser jugadores activos en los procesos de securitización y desecuritización en todas o casi todas las regiones, ya sea como amenazas, garantes, aliados o interventores; su legitimidad depende sustancialmente de su éxito en establecer la legitimidad de éstos valores.[4]

El método que se utilizó para este trabajo profesional fue el de realizar un análisis explicativo sobre la postura gubernamental en cuestiones de vigilancia, ciberdefensa y ciberseguridad con sus planes y estrategias correspondientes. En donde se hace una valoración sobre la importancia que ha tomado éstos temas para la política exterior y el gobierno estadounidense en las últimas décadas. La aplicación de la teoría neorrealista para este tema fue la más adecuada puesto que el tema estudiado comparte los elementos presentados en dicha teoría.

[4] Barry Buzan y Ole Weaver, *Regions and Powers: The structrure of International Security*, Cambridge University Press, Diciembre de 2003, 564pp.

Asimismo, se hace un análisis para plasmar las metas y objetivos que tiene el gobierno internacional al establecer medidas que fortalezcan su seguridad nacional y aseguren su liderazgo en el orden internacional frente al crecimiento de nuevas superpotencias, conflictos y amenazas no tradicionales. La tesis no se sitúa en el ciberespacio en sí, sino en la vigilancia que es manejada principalmente por medios digitales.

Dentro de los temas adyacentes a este estudio podemos encontrar la revolución de las fuerzas militares en las que ha traído consigo el uso de la cibernética y la robótica con fines bélicos, de bajo costo (en términos de efectivos), pero que termina con el monopolio del hombre en los ámbitos de seguridad y guerra, que ponen en riesgo la sensibilidad de las personas frente a los crímenes de guerra. A pesar de haber hecho mención en este trabajo sobre las capacidades militares dentro del ciberespacio y el aire, no es el principal objetivo, sin embargo, habría que aclarar, que los ciberataques y el uso de herramientas tecnológicas en el combate van en aumento y traen numerosos riesgos consigo.

En el primer capítulo se discutirá la evaluación de las amenazas, riesgos y peligros consensados dentro de Estados Unidos, ya que esto es relevante para cualquier estudio que va más allá de los términos políticos y legales, hacer un análisis sobre éstos tres términos ayuda a comprender el motivo de algunas políticas públicas, ubicándonos en el contexto para generar un análisis imparcial sobre el tema.

El segundo capítulo tiene como propósito explicar la construcción de los complejos de ciberdefensa y ciberseguridad, en el que ambos forman parte de un proyecto mucho más amplio y que por lo mismo cooperan entre sí fortaleciendo el cumplimiento de las capacidades de Estados Unidos, en este sentido, en el capítulo se retoman los antecedentes de las políticas que ayudan a construir el complejo de seguridad centrado, se tocan las políticas y declaraciones realizadas por el presidente Barack Obama, para así dar continuación a los dos subcapítulos

donde se hace un desglose de dos de los complejos que integran el complejo de seguridad centrado, el complejo de ciberdefensa, representado por el *Department of Defense*, y el complejo de ciberseguridad liderado por el *Department of Homeland Security*, que demuestran una vez más la ampliación de las facultades de las instituciones para ejercer el poder a través del ciberespacio.

Éstos dos complejos asisten a un tercero dirigido principalmente por la *National Security Agency*, de este modo, en el tercer capítulo se realiza la descripción del complejo de vigilancia, puesto que durante la administración de Obama, las filtraciones sobre los programas de vigilancia masiva exponen las directrices del presidente por permitir el monitoreo constante de la ciudadanía estadounidense. Es así, que surgen maneras de protesta en contra de esta falta de ética y legalidad de las actividades gubernamentales mostradas en las publicaciones de Wikileaks, que emerge como una plataforma pública de información de primera que atenta contra la inteligencia y la secrecía que la comunidad de inteligencia y vigilancia requieren. Sin embargo, esto conlleva a mencionar los funcionarios que divulgan información clasificada, entendiendo que, la ingeniería social es el pilar principal de la seguridad de la información, de esta forma, es explicable las medidas que Estados Unidos toma después de su mayor fracaso, Edward J. Snowden.

1. EL COMPLEJO DE SEGURIDAD CENTRADA Y LA DETERMINACIÓN DE LAS POLÍTICAS DE SEGURIDAD

En éste capítulo se trabajarán tres temas esenciales para la estructuración de políticas de seguridad para el quinto espacio, el ciberespacio. Sin duda, éste medio es la manera más eficiente de realizar toda actividad humana, ya que las distancias se acortan, y en cuestión de tiempo, es inmediato.

En un primer momento, se trabajará la importancia que tiene el ciberespacio para la delimitación de estrategias de seguridad nacional retomando la teoría neorrealista sobre los complejos de seguridad, en donde la regionalidad del complejo se va vislumbrando en términos globales con Estados Unidos como superpotencia líder. En el segundo subcapítulo, se desglosará el enfoque de cada uno de los conceptos: amenaza, riesgo y peligro, ya que dichos nos ayudan a comprender la concepción de las estrategias de seguridad. En el último subcapítulo, se hablará sobre las características que forman al ciberespacio y el intento por crear regulaciones técnicas y políticas al mismo, lo que es llamado ciberseguridad.

1.1 Seguridad Nacional y el Complejo de Seguridad Centrado

Para discutir el estado de vigilancia durante el periodo de Barack Obama y hablar acerca del concepto de seguridad nacional, hay que mencionar que es un término evolutivo cuyos factores y actores se desarrollan en un contexto político y económico, con mayor o menor incidencia en la toma de decisiones del Estado y su zona de influencia.

El primer vínculo entre el Estado y la seguridad nacional surge desde el nacimiento del primero como ente político ya que una de las necesidades por las que surgen los Estados es la seguridad de los individuos y el dominio de la fuerza. Por este motivo, la configuración de los Estados (en cuanto a seguridad), se fijan

ciertas amenazas de acuerdo a su contexto y planea a través de estrategias cómo contrarrestarlos, lo que se resuelve en un plan de seguridad nacional para su supervivencia y proteger a sus ciudadanos.

Los planes de Seguridad Nacional de los Estados, tienen en menor o mayor medida un carácter preventivo, en el caso estadounidense estos planes tienen una connotación de enemigo-aliado como en un estado de guerra, por lo que en un primer momento se deben ir identificando los problemas que amenazan al ente y que deben de resolverse o evitar, hacer una evaluación de riesgos y en qué calidad y cantidad pueden dañarlo; y, en caso de que sea necesario, responder a dichas amenazas bajo cualquier costo.

A partir del siglo XXI los conceptos de seguridad nacional, amenaza, peligro y riesgo han demostrado contener una alta complejidad desde su definición hasta su materialización, ya que éstas nociones se encuentran incompletas por no percibir aquellos fenómenos que son producto de la globalización y de la apertura comercial, económica y cultural por lo que pocos Estados integran a sus agendas asuntos como la desigualdad, la migración, entre otros.

Desde la Guerra Fría el concepto de seguridad nacional ha venido transformándose para satisfacer la necesidad de explicar las eventualidades y fijar planes, acuerdos y proyectos, para resolverlos o prevenirlos, sin embargo, hoy en día continúa el debate sobre la exacta definición y delimitación del mismo como un concepto altamente personalizado por las necesidades de las naciones.[5]

Dentro de la estructura de gobierno de Estados Unidos y de cualquier otro Estado, podemos encontrar que la seguridad nacional forma parte del interés nacional y un Estado que no procura su seguridad nacional, está condenado a fallar y desaparecer. En este sentido parece importante mencionar que para Allan

[5] Barry Buzan, *The National Security in International Relations, People States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Harvester Wheatsheaf, Londres, 1991. pp. 1 y ss.

Stolberg, siguiendo a Henry Kissinger y Robert Art, como historiadores políticos, deja claro que la identificación de "los intereses [nacionales] son esenciales para el establecimiento de los objetivos o fines que sirven como objetivos para la política y la estrategia",[6] ello nos ayuda a explicar el por qué de la configuración de las políticas de seguridad. Hay que agregar que la delimitación-elección de los intereses nacionales facilitan la determinación de los tipos y cantidades del poder nacional empleados como medio para poner en práctica una política o estrategia designada.

Sin embargo, habría que destacar que "la búsqueda de la libertad de amenazas",[7] como interés nacional de Estados Unidos, cae en el intento de una construcción de una seguridad nacional eficiente y completa; es así que Buzan señala que el gobierno y las sociedades se verán envueltos en una dicotomía para mantener su "independencia y su integridad funcional".[8]

Aunque este binomio no siempre será armonioso, ya que tenderá en ciertas ocasiones a oponerse entre sí debido a que la meta ulterior es la supervivencia[9] de ambas, pero considerando que son vinculantes –un Estado no tiene independencia si no posee integridad funcional y viceversa- la preponderancia en algunos momentos por mantener la independencia del Estado en un nivel suficiente conlleva a retos y obstáculos que acarrean una militarización de las políticas exteriores e incluso públicas.

Buzan hace una acertada aclaración acerca de la seguridad nacional, en el escenario internacional y la sociedad, nos dice que:

> […] la unidad básica de seguridad en el sistema internacional contemporáneo es el Estado territorial soberano. El tipo ideal es el Estado-nación, donde los límites

[6] Allan G. Stolberg, *The International System in the 21st Century* en Bartholomees, Jr., J. Boone (edit.), *The U.S. Army War College Guide to National Security Issues,* volumen II, Strategic Studies Institute, EE.UU. pp. 153-225. Disponible en línea: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1005 Consultado: abril 2016.

[7] Barry Buzan, op.cit.
[8] *Ídem*
[9] *Ídem*

> étnicos y culturales se alinean con las políticas tal es el caso de Japón y Dinamarca. […] Desde que los Estados son las unidades de análisis dominantes, la seguridad nacional es el problema central en el sentido normal y ambiguo y su aplicación directa a unidades étnicas.[10]

Buzan señala que existen "factores en cinco sectores que afectan las colectividades humanas y son: militares, políticos, económicos, sociales y medioambientales",[11] siempre se encuentran vinculados entre sí y son los que definen y moldean la seguridad nacional y se convierten en objetivo y lineamientos.

Un factor determinante -sino es que fundamental- es la construcción histórica de los Estados Unidos para crear su propia noción de seguridad nacional. Podemos resumir que el auge del país coincide con dos circunstancias trascendentes para la historia de la humanidad, como son las revoluciones tecnológica y económica,[12] que sin duda le dan una gran ventaja y aporte al desarrollo del país durante el siglo XX hasta nuestros días.

Tal como establece Arnold Wolfers en su trabajo *Security as an ambiguous symbol*, la seguridad nacional es un concepto cambiante y amplio en donde se combina política con el interés nacional para dar paso a la Estrategia de Seguridad Nacional de Estados Unidos en concreto, que en sentido normativo, dirá lo que una política de seguridad debe ser, para proteger sus "valores medulares mínimos: su independencia de cualquier amenaza colonial o intervencionista y su integridad territorial".[13]

---

[10] *Ídem*
[11] *Ídem*
[12] Walter Russell Mead, *A Hegemon's Coming of Age. A Brief History of U.S. Foreign Relations*", *Foreign Affairs*, July-August 2009. Disponible en línea: http://www.jstor.org/stable/20699628?seq=2#page_scan_tab_contents Consultado: marzo de 2016

[13] Arnold Wolfers, *National Security as an ambiguous symbol*, en *Discord and Collaboration: Essays on International Politics*. The Johns Hopkins University Press, Baltimore, EE.UU.1962. pp. 5-10

Es importante aclarar que Wolfers al mencionar “valores medulares” no está pensando en los de una sociedad como la estadounidense, hace referencia a aquellos que un Estado mantiene para seguir subsistiendo; es decir, la principal preocupación es seguir manteniendo su existencia (como ente independiente e integral) y su influencia, ya que este y ningún otro es el capaz de proveer los servicios a la ciudadanía, y en específico, la seguridad.[14] De acuerdo a Wolfers la estructuración del plan de seguridad y los medios para asegurarla son un aspecto militar, donde la seguridad por sí misma es también un valor. Como el poder (la habilidad de controlar a otros) o la riqueza (cantidad de posesiones materiales, económicas), la seguridad, en palabras de Wolfers, “mide la ausencia de amenazas a valores adquiridos (ideología, cultura) y la ausencia de temor de que los valores (medulares) sean atacados”.[15]

Para Richard Ullman detrás de todos los bienes que un Estado puede y debe proveer ninguno es más importante que la seguridad. A lo largo de su trabajo hace una referencia a la vitalidad que la seguridad representa en relación con las demás libertades pues, “sin la seguridad la libertad es inútil”, [16] pues en los individuos existe una desconfianza ante lo que puede ocurrir, ya que se desconocen las amenazas y no existen medidas preventivas para contrarrestar en caso de que ocurran o para evitar que ocurran.

De acuerdo con Ullman y Wolfers las vulnerabilidades e interés nacional están definidas por los Estados, es decir, que cada miembro del sistema internacional prioriza sus debilidades e intereses para conformar políticas adaptadas y factibles dentro de su territorio y hacia el exterior, ya que a través del tiempo, las amenazas se van haciendo mucho más difíciles de definir y contraatacar, ya que las amenazas concebidas dentro de lo no-militar han ido desarrollándose con efectos como la globalización, mientras que las amenazas

[14] Aunque habría que excluir las nuevas formas de brindar servicios de seguridad como la privatización de las fuerzas armadas y la seguridad privada comercial o personal.
[15] *Ídem.*
[16] Richard Ullman, *Redefining Security*, en *International Security*, EE.UU. vol.8, no.1, 1983. Pp. 129 y ss.

concebidas sobre un marco tradicional son más sencillas de contraatacar puesto que llevan una estrategia y un cuerpo definido de acción.

Sin embargo, lo que varios autores difieren es en la militarización que se crea a partir de la lógica tradicional que proponen Wolfers y Hobbes como principales expositores del poder militar para la defensa de los intereses nacionales.[17] Ullman hace la aclaración que desde la perspectiva militar la realidad es falsa o incompleta y lleva a una seguridad nacional débil, ya que privilegia y discrimina los peligros desconociendo los riesgos que pueden implicar, tales como la migración, los huracanes o los terremotos. También agrega, que la militarización de una Seguridad Nacional conlleva a una inseguridad global,[18] por un sentimiento de desconfianza entre los Estados, podemos tomar como claro ejemplo el cierre de las fronteras o el desarrollo armamentístico.

El obstáculo para conseguir una definición de seguridad nacional universal, subyace en el hecho de que es un concepto que evoluciona dependiendo de los "procesos socio-históricos que atañen a cada uno de sus actores, (que) provienen de valores culturales y necesidades sociales, como también de las aspiraciones nacionales",[19] se puede decir que depende del contexto y del plan de gobierno en el Estado lo que guiarán la configuración de las políticas nacionales.

Al respecto, retomando a Buzan, considera y pone a discusión la visión tradicionalista realista al no considerar los riesgos internos como una falla en las políticas de seguridad nacional, haciendo una aclaración sobre lo que se debería de considerar dentro de la "seguridad de las colectividades humanas que son afectadas por factores en cinco sectores principales: militar, político, económico, social y de medio ambiente",[20] en el que problemas como la segregación racial, el

[17] Arnold Wolfers, op.cit.
[18] Richard Ullman, op.cit.
[19] Sergio Aguayo y Bruce Michael Bangley (coordinadores). *En búsqueda de la Seguridad nacional perdida. Aproximaciones a la seguridad nacional mexicana*, México, Siglo Veintiuno Editores, 1990, p. 27.
[20] Barry Buzan. op.cit.

antisemitismo o las prácticas con repercusiones severas al medio ambiente, tienen repercusiones a largo plazo, pero pueden tener un alto impacto en el país.

La aclaración de Buzan es de lo más oportuna pues hay que tomar en cuenta que el concepto al ser evolutivo y diacrónico, como plantea Martha Bárcena, y que el cambio en su definición se debe a la presencia "de nuevos actores y problemas transnacionales que rebasan las fronteras del Estado".[21]

Dicho esto, se puede afirmar que no existe una definición concreta que pueda ser el definitiva para lo que entendemos como seguridad nacional, ya que a través del tiempo han surgido nuevos retos en donde no sólo se cuestionan los nuevos riesgos aparentes sino también el papel del Estado en el plan de acción y preparación que ofrece.[22]

Hay que tener en cuenta que los Estados Unidos han tenido que cambiar la delimitación de Seguridad Nacional en su historia por diversos sucesos que podemos observar en el periodo presidencial de John Quincy Adams, [23] Franklin Delano Roosevelt (7 diciembre de 1941) y George W. Bush (11 septiembre 2001), ya que estos presidentes respondieron a las amenazas a su Seguridad Nacional "ampliando la esfera de responsabilidad de los Estados Unidos"[24], en lugar de delimitar la seguridad como cualquier otro país lo haría.

No hay que dejar de lado que tras la expansión de la seguridad nacional en otros ámbitos y espacios, se adquiere el peligro de generar nuevas inseguridades y que podemos encontrar que Estados Unidos trata de contrarrestar con al menos

[21] Martha Bárcena Coqui, *La reconceptualización de la seguridad* en Senado de la República. Memoria del Seminario Informativo. Seguridad Internacional en el siglo XXI: los retos para América Latina y el Caribe, Senado de la República, México, 2004, p.19.
[22] *Ídem*.
[23] Creador de la Doctrina Monroe.
[24] John Lewis, Gaddis, *Surprise, Security, and the American Experience*, Cambridge, MA, Harvard University Press, 2004. 160 pp.

tres políticas: las medidas cautelares,[25] alianzas unilaterales y el uso de su hegemonía. Estas políticas mencionadas han venido marcando y definiendo las relaciones exteriores de Estados Unidos con contrarios, también le han proporcionado un carácter agresivo, desconfiado y ambicioso, e incluso se han hecho los comentarios de que las políticas del país son de paranoia.[26]

A pesar de que dichas políticas no necesariamente deben estar vinculadas entre sí, demuestran la capacidad de adaptabilidad (y la falta de escrúpulos) que tiene el gobierno de Estados Unidos que ha sido característica común al momento de ejercer su política exterior. Un ejemplo de ello se puede observar en los ataques terroristas a dos de los centros estratégicos del país en el 2001, desafiando las predicciones de los altos precios de petróleo, el incremento del terrorismo, la resistencia militar en el país de intervención, los costos materiales y humanos, "sólo para evitar que estas cosas pasen".[27]

Esto se ve reflejado en la declaración de guerra que George W. Bush hizo frente al Congreso y que no presentó ninguna oposición, ni el mismo Obama quien señaló durante su campaña que no apoyaba las guerras "inútiles" haciendo referencia a la Guerra en Irak, y que en la administración de Obama lo pudimos observar con los principales filtradores de información estratégica y de inteligencia como Bradley Manning y Edward Snowden de quienes hablaremos en el tercer capítulo de esta investigación.

Retomando los sucesos del 11 de septiembre de 2001 a las Torres Gemelas en Nueva York, y los graves daños ocasionados al Pentágono en Arlington, Virginia, es preciso para Estados Unidos reconfigurar su política

[25] Karl-Heinz Kamp, *Intervenciones militares cautelares (preemptive strikes): ¿una nueva realidad de la política de seguridad?,* Instituto de Investigaciones Jurídicas, UNAM, Disponible en línea: http://www.juridicas.unam.mx/publica/librev/rev/dconstla/cont/2004.2/pr/pr22.pdf Consultado: enero de 2015.
[26] Este término fue empleado en la edición de Noviembre de 1964 de Harper's Magazine, cfr. http://harpers.org/archive/1964/11/the-paranoid-style-in-american-politics/ Consultado: febrero de 2015.
[27] John Lewis Gaddis, op.cit, pp. 81-82.

nacional y exterior respecto a las amenazas internas y externas que percibía el gobierno, creando así el *Department of Homeland Security* (DHS), cuyas responsabilidades son muy extensas[28] y por ésta misma razón es el tercer departamento más grande del país y que junto con la NSA terminarán siendo los encargados de las políticas de ciberseguridad[29] y vigilancia de Estados Unidos, respectivamente.

En este sentido parece oportuno explicar el término *surveillance* o vigilancia que es el tema angular de este trabajo. La palabra tiene orígenes del verbo francés *surveiller* –que retoma Foucault- y a su vez de la locución latina *vigilare*, que tienen el mismo significado de "vigilar" en español; es interesante hacer su comparación con el verbo supervisar, la diferencia radica en que la primera implica una observación sobre alguien con sospecha de cometer algún delito, ambos conceptos muestran un grado de conflicto puesto que al presentarse como políticas públicas y política exterior se sobreponen a las principales libertades civiles reconocidas en las enmiendas. Sin embargo, no hay que olvidar que desde el atentado del 11 de septiembre las políticas de Estados Unidos se han vuelto de prevención y disuasión.[30]

El enfoque que este estudio retomará para explicar las medidas de vigilancia en la administración de Obama es el del neorrealismo, presentado en complejos de seguridad, término empleado por Buzan y Wæver en el 2003. La perspectiva neorrealista de la seguridad es estatocéntrica, donde existe una

[28] Este departamento envuelve actividades como: vínculos con la academia, seguridad fronteriza, servicios de ciudadanía y migración, derechos y libertades civiles, ciberseguridad, seguridad a la infraestructura crítica, desastres, seguridad económica, comunicaciones de emergencia, tráfico humano, políticas de inmigración, compromisos internacionales, coordinación para la aplicación de la ley de acuerdo a los estratos de la jurisprudencia, prevención del terrorismo, seguridad de transportes, resiliencia y políticas de privacidad.

[29] Que veremos en el subcapítulo 1.3

[30] Aquí habría que señalar que Estados Unidos acuñó *deterrence* y *dissuasion* con dos connotaciones totalmente diferentes, a pesar de que la segunda palabra, tiene el mismo significado originalmente; es así que por *dissuasion* se entiende como persuadir a otras potencias de abstenerse de iniciar una "carrera armamentística" o competencia en las capacidades militares con Estados Unidos. Por *deterrence* se entiende: persuadir al enemigo no atacar al país puesto que su ataque será derrotado convincentemente - es decir, que no va a ser capaz de lograr sus objetivos operativos.

polaridad del poder, y donde la distribución de los materiales de poder (militares y políticos) determinan, la política global y su dinámica con el balance de poder.

De esta forma, tenemos a una superpotencia como lo es Estados Unidos en la actualidad, [31] que securitiza a un nivel global, determinando quién o qué es definido como (el origen de) la(s) amenaza(s) y a quién identifica como objetivo en sus contramedidas. También su actividad yace en todos o casi todos lo procesos de securitización y desecuritización en las regiones del sistema. Es importante mencionar que esta categorización del actor como superpotencia requiere de un alto grado de legitimidad internacional, que dependerá sustancialmente de su éxito al establecer (con legitimidad) los valores a proteger, como la guerra con Irak tras las el atentado del 11 de septiembre, la protección de la vida humana mediante el empleo de la guerra y el marco legal establecido en contra de todo sospechoso de terrorismo.

Dicho esto, podemos identificar que en el caso de la vigilancia, se encuentra cómo una estructura más de un Complejo de Seguridad Centrado (CSC)[32], o llamados Mini Complejos de Seguridad (MSC), que lo auxilian. Es decir, tenemos un Estados Unidos líder mundial en cuestiones de ciberdefensa, ciberseguridad y vigilancia dominante en el discurso sobre quién debe proponer los marcos internacionales de acción, al mismo tiempo que resulta imposible establecer una organización internacional que regule éste espacio más allá del ámbito técnico, y también debido al grado de importancia que los sistemas de información representan para la infraestructura crítica de cualquier país, a la vez que ningún país podría ostentar el liderazgo en dicha organización.

[31] Una superpotencia es aquél que posee capacidades político-militares de primera clase y una economía que sustente esas capacidades. Deben ser capaces de tener, y también de ejercer, sus capacidades militares y políticas en un alcance global. Cabe señalar, que en la actualidad EE.UU. es el único que posee tales cualidades. Véase Barry Buzan, Ole Weaver, *Regions and Powers: The Structure of International Securtity*, Cambridge University Press, Diciembre de 2003, pp. 564

[32] Un Complejo de Seguridad Centrado es una estructura de seguridad dominada por un superpotencia o suficientemente integrado por instituciones colectivas para tener una calidad de actor a nivel mundial. Cfr. Barry Buzan, Ole Weaver, op. cit.

Sin embargo, de manera ilustrativa, el siguiente Esquema 1 representa la construcción del Complejo de Seguridad Centrado a través de los distintos mini complejos que lo componen, en el que los tres MSC, ciberdefensa, ciberseguridad y vigilancia, se vinculan y crean una estructura sólida que tiene como fin ulterior la supervivencia del establishment estadounidense.

Esquema 1. Complejo Centrado de Seguridad

Fuente: Elaboración propia con información de Buzan, Weaver, Regions and Powers, 2003.

Sin duda las ideas de Buzan y Wæver defienden los procesos de securitización sobre los objetivos de la (falta de) seguridad en el ciberespacio, de acuerdo a la dinámica de preponderancia de las agendas/estrategias de seguridad de las superpotencias en el nivel global, es así que la estructura de seguridad en temas de vigilancia, se verán totalmente dominados por Estados Unidos y alguna que otra gran potencia.

En resumen y a manera de conclusión, las políticas de seguridad buscan dar respuesta a las amenazas percibidas por los Estados, el fortalecimiento de las estructuras de seguridad tienen como componentes las nociones de amenaza,

riesgo y peligro, que son componentes que los Estados usan para esbozar sus planes y estrategias de seguridad.

A lo largo de este trabajo se estudiarán las amenazas que la administración de Barack Obama trata de contrarrestar como superpotencia, las acciones que lleva a cabo y los resultados de este proceso. Pero en un primer momento es importante discutir los conceptos de amenaza, riesgo y peligro para esclarecer la construcción de sus políticas y el alcance que planea obtener con ellas.

1.2 Amenaza, Riesgo y Peligro

Es menester para toda política de seguridad nacional del siglo XXI considerar los efectos adversos que puede tener para la integridad, soberanía e independencia de un país, el no tener las capacidades y resiliencia necesarias frente a una de las amenazas potenciales de más alto impacto para un Estado, las ciberamenazas. Hoy día los Estados, las empresas privadas y algunos miembros de la ciudadanía, trabajan en conjunto para disminuir los riesgos y vulnerabilidades frente a los nuevos peligros y actores criminales, sin embargo, en primera instancia, el primer obstáculo al que se enfrentan estos esfuerzos, es la delimitación del ciberespacio.

Tomando en consideración la dificultad de delimitación del ciberespacio, la elaboración de las estrategias y programas de seguridad nacional correspondientes a la ciberseguridad, se basan en la determinación de las amenazas y peligros que enfrenta el estado en éste ámbito espacial. Es así que el propósito de este subcapítulo es explicar los tres conceptos fundamentales y esbozar la problemática de la construcción de las políticas de seguridad en el ciberespacio hoy en día, en un primer momento explicar el concepto de “amenaza”, en un momento “riesgo” y en un tercer punto “peligro”.

En la actualidad no existe un consenso sobre el significado de amenaza para un estado en específico o las características que debe de tener un sujeto o

circunstancia para considerarse como tal. Asimismo, las diferencias sobre esta concepción depende de las nociones aportadas por las ciencias exactas y el riesgo (que es mesurable) que implican. Según los diferentes tipos de condiciones y características entrópicas que los estados poseen, se puede llegar a definir lo que resulta una amenaza para éste, tal cual puede ser el ejemplo de una ciudadanía armada, para Estados Unidos el hecho de tener a sus ciudadanos armados no representa una amenaza en sí; caso contrario para El Salvador, ya que representa un serio grado de inestabilidad e inseguridad al interior del país.

Sin embargo, han habido análisis muy nutritivos sobre lo que se puede considerar una amenaza: Richard Ullman hace una definición general sobre lo que podemos considerar como una "amenaza" a la seguridad nacional y hace dos distinciones, la primera a la que se refiere es respecto a "disrupciones o disturbios que van desde guerras en el mundo a rebeliones internas, desde bloqueos y *boycotts* a escasez de materias primas y desastres naturales".[33] En la segunda categoría, aclara que son aquellas que tienen mayor dificultad de delimitación puesto que las amenazas no aparecen de una manera clara y presente, sabemos que existen, pero no sabemos dónde, cuándo y en qué manera van a actuar.[34]

De acuerdo con esta aportación que nos brinda Ullman podemos detectar que existen amenazas tradicionales, provenientes de los sujetos del Derecho Internacional y las amenazas no tradicionales en las que se encuentran las provenientes o efectuadas en o a través del ciberespacio. Sin embargo, es pertinente hacer referencia al atentado del 11 de septiembre de 2001, ya que tras este suceso, se dio una reconfiguración de los conceptos estadounidenses de seguridad nacional y la restructuración de seguridad como tal, en el que toman un papel primordial las amenazas no convencionales y aquellas amenazas

[33] Richard Ullman, *Redefining Security*, en *International Security*, EE.UU. vol.8, Nº.1, 1983. pp. 129 y ss.
[34] *Ídem.*

transnacionales, en las que se cataloga el terrorismo, el narcotráfico, las organizaciones delictivas, y en específico los cibercrímenes[35] o ciberataques.

Retomando la discusión, podemos decir que las amenazas son: "un fenómeno, sustancia, actividad humana o condición peligrosa que pueden ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales",[36] bajo esta concepción, habría que mencionar qué se consideraría como una amenaza en el ciberespacio o las amenazas para los sistemas de información de Estados Unidos.

Una amenaza para la Seguridad de la Información (SI)[37] se traduce en "secuencias de circunstancias o eventos que permiten a un agente causar daño a la información al explotar las vulnerabilidades en un producto de las Tecnologías de la Información (TI)"[38] también implica "[aquél] evento con el potencial de causar daño a un sistema en la forma de destrucción, acceso no autorizado, modificación de datos o negación de servicio",[39] de ésta manera podemos entender de una forma más clara qué se entiende por una amenaza a los sistemas de información.

Estados Unidos como cualquier otro país, siendo líder en estrategias de ciberseguridad, reconoce que los retos que enfrenta toda seguridad nacional

---

[35] Término que engloba un gran ramal de delitos, pero que para efectos prácticos entenderemos que es cualquier delito cometido en el que se haya utilizado un equipo, una red o un dispositivo de hardware, el equipo o el dispositivo pueden ser el agente, el facilitador o la víctima del crimen. Asimismo, el delito puede tener lugar en el equipo únicamente o en otras ubicaciones también. Symantec, http://securityresponse.symantec.com/norton/cybercrime/definition.jsp.

[36] UNISDR, *Terminología sobre reducción de riesgo de desastres*, 2009. Disponible en línea: http://www.unisdr.org/files/7817_UNISDRTerminologySpanish.pdf Consultado: noviembre de 2015

[37] Seguridad de la Información como aquella protección de la información y los sistemas que los contienen para evitar el acceso no autorizado, uso, divulgación, alteración, modificación o destrucción indebida de ésta.

[38] Guillermo Correa, *Ciberseguridad, Seguridad Ampliada: los nuevos temas de seguridad*, Diplomado de Seguridad Internacional, División de Educación Continua y Vinculación, FCPyS, Enero 29 de 2016. Disponible en línea: http://decyvpoliticas-unam.org/pag/temarios/seguridad/Cibert.%20Ponente%202.pdf Consultado: enero de 2016

[39] *Ídem*

pueden provenir en distintas formas y no sólo por actores tradicionales, como son los accidentes, el terrorismo, los sabotajes y los desastres naturales que ocasionan disrupciones en la infraestructura informática dentro y fuera del suelo estadounidense. Los obstáculos técnicos que este país identifica para la persecución del delito toman relevancia en el mismo nivel que la extorsión, fraude, robo de identidad, la pornografía infantil, el impacto que tienen para la confianza de los usuarios y su seguridad en el ciberespacio. Además, Estados Unidos ubica al robo de propiedad intelectual como una amenaza que merma la competitividad y la innovación del país.[40]

Por obvias razones es entendible que cualquier daño a esta vasta infraestructura cibernética-digital, sea parte del contexto de la Seguridad Nacional de Estados Unidos, ya que su independencia e integridad depende en gran medida del "Internet y de los sistemas de datos del ciberespacio en un rango alto para servicios críticos",[41] esta dependencia deja a toda población expuesta y vulnerable a las ciberamenazas, ya que existen "actores estatales y no-estatales que planean ciberataques destructivos y disruptivos en las redes de la infraestructura crítica y robo de propiedad intelectual para minar la ventaja y desarrollo tecnológico y militar".[42]

Bajo ésta lógica, los Estados Unidos se dan a la tarea de tomar el asunto de la ciberseguridad en sus manos y alentar a los usuarios y empresas a seguir los estándares de seguridad de la información propuestos por sus instituciones con la doble intención de tener acceso mediante "puertas traseras" creadas a partir de la

[40] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, Estados Unidos, mayo 2011
[41] United States Defense Department, *The DoD Cyber Stategy 2015*, Disponible en línea: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf Consultado: febrero de 2016
[42] *Ídem*

degradación de algunos estándares como los criptográficos,[43] de esta manera se facilita la realización de la vigilancia del gobierno sobre los usuarios de las distintas plataformas, teniendo acceso a su información bajo la premisa de la búsqueda y defensa de amenazas.

Debido al reconocimiento estadounidense de las amenazas al ciberespacio, por el alto grado de riesgo que representan para la vida cotidiana y en aquellas infraestructuras críticas que dependen de los sistemas informáticos de red, es que se plantea la creación de una política de ciberseguridad internacional que proteja a la ciudadanía y a los gobiernos de todo este tipo de amenazas, para mantener el ciberespacio interoperable y abierto.

No obstante, es importante que nos refiramos al término "riesgo" antes mencionado, es así que debemos plantear en un primer momento la definición que nos brinda la *United Nations Office for Disaster Risk Reduction* (UNISDR) que dice: "[es aquella] probabilidad de que se produzca un evento y sus consecuencias negativas";[44] ésta es muy similar a la guía 73:2009 de la *International Standard Organization* (ISO),[45] referente al *Manejo de Riesgos* que, de una manera más técnica y desglosada, explica que riesgo es:

> "a) Efecto de la incertidumbre en los objetivos,
>
> b) Un efecto es una desviación de lo esperado (positivo y/o negativo),
>
> c) Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, y las metas ambientales) y pueden aplicarse a diferentes niveles (como estratégica, en toda la organización, proyecto, producto y proceso),
>
> d) El riesgo se caracteriza a menudo por referencia a los eventos potenciales y consecuencias, o una combinación de éstos,
>
> e) El riesgo se expresa a menudo en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad asociada de ocurrencia,

[43] Russell Brandom, *How far did the NSA go to weaken cryptography standards?*, The Verge, 11 de septiembre de 2013, Disponible en línea: http://www.theverge.com/2013/9/11/4718694/how-far-did-the-nsa-go-to-weaken-cryptography-standards Consultado: mayo de 2016

[44] UNISDR, *Terminología sobre reducción de riesgo de desastres*, op.cit.

[45] Tomando en cuenta que el ciberespacio está regido por normas técnicas y estándares que optimizan y efectivizan su funcionamiento.

> f) La incertidumbre es el estado, aunque sea parcial, de la carencia de información relacionada con, la comprensión o conocimiento de, un evento, su consecuencia, o probabilidad."[46]

Se puede destacar la incidencia que tiene el término "incertidumbre" que es aquella falta de conocimiento claro y seguro de "algo" sin temor de no acertar o cumplir con lo que se debe, de esto se puede derivar que tanto la definición de la UNISDR como de la ISO cumplen lo básico al definir al riesgo como aquella probabilidad de que ocurra un evento y los factores que conllevan a que tenga consecuencias negativas,[47] y que se debe medir de acuerdo a la relación entre evento, sus causas y sus consecuencias.

De acuerdo a lo anterior, para proceder a un manejo de riesgos adecuado, sea sobre un objeto o circunstancia, varía dependiendo de sus causas y consecuencias, la ISO recomienda realizar con base en tres fases: identificación del riesgo (proceso de encontrar, reconocer y describir los riesgos), análisis de riesgo (proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo) y evaluación del riesgo (proceso de comparación de los resultados de análisis de riesgos con criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable).[48]

El trabajo de la ISO sin duda resulta mucho más práctico y técnico que los textos con fines políticos, puesto que se mira desde una perspectiva objetiva de los riesgos. En el caso de los análisis y discusiones políticas, se tiene a los Estados como actores y dictaminadores de las políticas encargadas del manejo de los riesgos con base en su comprensión/perspectiva política, en mayor o menor cantidad; fijándose la importancia que las repercusiones de un objeto o

---

[46] ISO, *Guide 73:2009*, International Standard Organization, Disponible en línea: https://www.iso.org/obp/ui/es/#iso:std:iso:guide:73:ed-1:v1:en Traducción personal, Consultado: febrero de 2016.
[47] La identificación del riesgo como primer paso a realizar para una valoración de riesgos adecuadas que den como resultado un manejo efectivo de los mismos.
[48] ISO, op.cit.

circunstancia tiene para su integridad, de otra forma, si se brindase la misma atención a todos los eventos esto recaería en una fatalidad[49] o una inefectividad. Asimismo, los intereses estatales dependen de los grupos en el poder o acontecimientos históricos que reformaron totalmente la concepción de los riesgos que dichas amenazas representan, caso ejemplar, el atentado del 11 de septiembre de 2001 en Nueva York.

En resumen, las amenazas se van midiendo de acuerdo al riesgo que representan para el Estado, suena lógico y es lo óptimo a realizar, ya que la reducción de riesgos debería de primar antes que las mismas políticas de solución del conflicto o de ataque a las amenazas. Otra manera de delimitar las amenazas persistentes, es el pleno conocimiento del interés nacional del Estado, debido a que éste define las metas a lograr por parte de una administración nacional y los mecanismos de acción para contrarrestarlas.

Antes de aterrizar con el tercer concepto, peligro, podríamos concluir que, por riesgo entendemos que es "la posibilidad de que ocurra un resultado adverso o no deseado, resultante de un incidente, acontecimiento o suceso, determinado por la probabilidad de que una amenaza particular explote una vulnerabilidad en particular [y tenga] consecuencias asociadas",[50] para expresar el concepto de una manera más práctica y operativa se utilizará la fórmula $R=A\cdot V$, en donde el riesgo se encuentra expresado en la R, amenaza representado por la A, el punto son los "exploits", aquella la manera de romper un sistema de información a través de una vulnerabilidad que está representada por la V.

En este sentido, podemos observar que la fórmula de riesgo es necesaria la explotación de un punto de vulnerabilidad llevada a cabo por una amenaza, caso

[49] Está claro que los diversos eventos de riesgo no tienen la misma calidad, eventualidad ni consecuencias, por lo que se "personalizan" las políticas de seguridad reflejando las características básicas del Estado como sus intereses nacionales.
[50] Guillermo Correa, *Ciberseguridad*, op.cit.

contrario en el concepto de peligro. Podemos iniciar con que algo peligroso es cualquier actor o elemento potencial fuente de daño o efectos adversos sobre algo o alguien, en determinadas condiciones.

Básicamente, un peligro es aquello que puede causar daños o efectos negativos a los individuos, por ejemplo, los efectos sobre la salud, la propiedad o pérdidas equipo industrial, y donde se hace la categorización de los tipos de peligros que pueden haber como biológicos, químicos, físicos, psicosociales y de seguridad. Hay que resaltar que el término peligro para la ciberseguridad no es bajo la concepción de *hazardous*, que implica únicamente un impacto directo a la salud humana, sino en el sentido de *dangerous*, donde se considera todo aquello que puede ser mortal, que puede lastimar o matar personas, dañar propiedades o el medio ambiente. De esta forma, podemos agregar que la complejidad del estudio de la seguridad en el ciberespacio aumentaría considerablemente si se estudian los riesgos de la misma de acuerdo a los países y sus capacidades, puesto que en dicho estudio se hace una evaluación y administración de los mismos, y se adecúan los procedimientos o lineamientos, en lo que a continuación se puede observar en el Esquema 2.

Esquema 2. Administración de Riesgos

Fuente: ”Risk and Fraud Management”, Accourt Payment Specialists, http://www.accourt.com/wp-content/uploads/2014/01/accourt-risk-fraud-management

En este esquema podemos observar el proceso de la administración de riesgos, iniciando por su identificación, seguido por el análisis del mismo, después la articulación de las estrategias adecuadas al objetivo, para posteriormente observar si la respuesta es la deseada, concluyendo con el control del riesgo y su disminución de ocurrencia. Aunque los planes o estrategias de administración de los riesgos varían dependiendo del alcance de la organización y los elementos o medios con los que se cuentan puesto que todo plan de contingencia tiene un costo y una duración, incluso aquellas medidas que sólo son de supervisión del riesgo.

Cabe agregar que, la creación de políticas de ciberseguridad acarrea sus propios obstáculos, conscientes del riesgo que representan las ciberamenazas para una nación, la seguridad cibernética "debe" representar aquella capacidad central integral de esfuerzos coordinados a través de la unidad capacitada o con la función de procurar la infraestructura cibernética, tomando en cuenta las preparaciones y herramientas necesarias para la correcta operación de la unidad. Es así que podemos definir preliminarmente a la ciberseguridad como: "[…] el proceso de protección de la información mediante la prevención, detección y respuesta a los ataques"[51] mediante el uso de la Red. Sobre este aspecto ahondaremos en siguiente subcapítulo para comprender la importancia de la ciberseguridad para la infraestructura crítica de Estados Unidos.

Al haber explicado los términos, amenaza, riesgo y peligro para la ciberseguridad, podemos pasar al siguiente subcapítulo en el que se describe la necesidad expandir y fortalecer el estado de ciberseguridad para Estados Unidos y el mundo, creando una estructura de seguridad y fijando misiones y visiones con el sector gubernamental, el sector privado y la ciudadanía. Estos MSC poseen diferentes fines y metas que evolucionan y se adaptan a este nuevo mundo de la

[51] National Initiative for Cybersecurity Careers and Studies. *Explore Terms: A Glossary of Common Cybersecurity Terminology*. Homeland Security Department. Disponible en línea: https://niccs.us-cert.gov/glossary#letter_c Consultado: octubre de 2015

conectividad llamado “el internet de las cosas”,[52] cuyo rasgo particular es la capacidad adquirida de las cosas, instrumentos, aparatos (sin descartar la infraestructura estratégica o de menor relevancia), a estar conectados entre sí y ser manejados a distancia mediante una conexión inalámbrica o de red, pero que su operación puede ser -y ha sido- interrumpida por terceros, en el que los gobiernos principalmente, fungen como el principal intruso.

1.3 La hipervigilancia a través del ciberespacio como política de ciberseguridad

Para entender el concepto de ciberseguridad, es importante hacer una aclaración sobre el terreno en el que se desempeña, el *ciberespacio*. De acuerdo al *National Initiative for Cybersecurity Careers and Studies* (NICCS),[53] el ciberespacio es una “red interdependiente de infraestructuras de tecnologías de la información, que incluyen el internet, las redes de telecomunicaciones, sistemas computacionales y controles y procesos codificados”.[54] Si bien esta aportación nos da los componentes técnicos que conforman el ciberespacio, la siguiente definición nos da características político-sociales que la complementan y su uso: “ámbito virtual donde usuarios de la red interactúan por medio de un lenguaje expresado por textos, imágenes, gráficos, sonidos, entre otros, entendiendo que en dicha red como un tejido de computadoras interconectadas que guardan bases de datos y fuentes de información, a las cuales los usuarios pueden acceder”.[55]

---

[52] Unión Europea, *Internet of Things,* Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, 2013 Disponible en línea: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf Consultado: abril de 2016.

[53] Dependencia del Homeland Security Department que tiene como propósito promover los estudios sobre la ciberseguridad y opera en colaboración con la Iniciativa Nacional sobre Educación en Ciberseguridad (NICE).

[54] National Initiative for Cybersecurity Careers and Studies. *Explore Terms: A Glossary of Common Cybersecurity Terminology*. Homeland Security Department. Disponible en línea: https://niccs.us-cert.gov/glossary#letter_c Consultado: octubre de 2015.

[55] Alejandra Morán Espinosa, Alejandro Servín Camaño y Oscar Alquicira Gálvez, *TIC (Internet) y Ciberterrorismo*, Revista de Seguridad, No. 23, UNAM. Disponible en: http://revista.seguridad.unam.mx/numero23/tic-internet-y-ciberterrorismo Consultado: octubre de 2015

Otra de las grandes complejidades sobre el tema del ciberespacio, es su influencia en la realidad física, ya que: "genera situaciones de derecho reales a pesar de romper el ámbito espacial, (…) [aunque] no se realicen en un plano tangible",[56] con esto podemos determinar que la distancia física no es obstáculo para realizar actividades hostiles a través del uso del ciberespacio, lo que ciertamente es preocupante para cualquier Estado que utilice este medio para su integridad y función, que hoy en día es indispensable pensar el mantenimiento de un Estado sin controlar su infraestructura cibernética siendo vulnerable por ciberamenazas.

La sola falla de alguna infraestructura cibernética conectada a infraestructuras críticas del gobierno o empresas, implica grandes riesgos y costos que ponen en alerta a los gobiernos, debido a que pueden minar las operaciones en curso o los proyectos a futuro. Por mencionar dos casos emblemáticos en un primer lugar encontramos a los ataques ciberterroristas en Estonia en el 2007, provenientes de Rusia, que impactó significativamente en la funcionalidad del gobierno, ya que el país posee uno de los más altos grados de gobierno electrónico y el resultado de los ciberataques en la guerra de Kosovo, que se retomarán más adelante.

Por estas razones, es entendible que cualquier daño a esta vasta infraestructura cibernética-digital, esté dentro del contexto de la Seguridad Nacional de Estados Unidos, ya que depende en gran medida del "Internet y de los sistemas de datos del ciberespacio en un rango alto para servicios críticos".[57] Esta dependencia deja a toda población expuesta y vulnerable a las ciberamenazas, dado que existen "actores estatales y no-estatales que planean ciberataques destructivos y disruptivos en las redes de la infraestructura crítica y

[56] *Ídem.*
[57] United States Defense Department, *The DoD Stategy 2015*, Disponible en línea: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf Consultado: mayo de 2016

robo de propiedad intelectual para minar la ventaja y desarrollo tecnológico y militar".[58]

El uso de las TIC en conflictos ha ido acompañada de su evolución y que podemos encontrar en tres categorías principales, en un primer lugar están ciberataques, que son aquellos ataques armados con la aplicación de la tecnología; en un segundo lugar se encuentra el ciberespionaje y en último el ciberterrorismo.[59]

La evolución de las TIC también ha propiciado nuevas oportunidades para la realización de "actividades negativas como la existencia de conductas antisociales y de nuevos delitos".[60] Un ejemplo de esto, son los ciberataques, pueden tener consecuencias catastróficas, debido a que explotan el aumento de la complejidad y la conectividad de los sistemas de infraestructura crítica y la ponen en riesgo.[61] La creación de políticas de ciberseguridad, acarrea sus propios obstáculos, además del riesgo que representan las ciberamenazas para una nación. La seguridad cibernética representa la capacidad central integral de los esfuerzos, coordinados a través de toda la unidad capacitada, con la función de gestionar a la infraestructura cibernética; en relación a lo anterior, una definición básica sobre ciberseguridad es que es "el proceso de protección de la información mediante la prevención, detección y respuesta a los ataques",[62] mediante el uso de la red.

Tampoco hay que excluir a las empresas privadas que han sufrido considerables problemas a causa de este tipo de ataques, tal es el caso de *Home Depot, Target* y *Sony* de Estados Unidos, en el que las dos primeras dos tuvieron

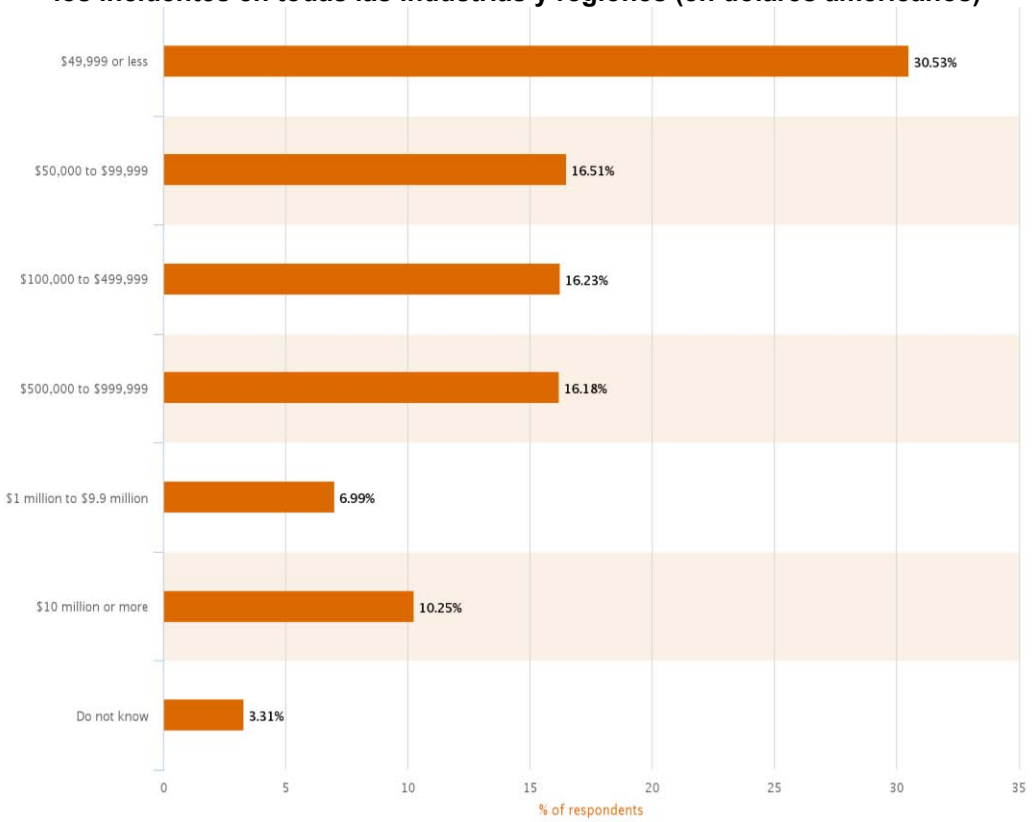
---

[58] *Ídem.*
[59] Alejandra Morán Espinosa, Alejandro Servín Camaño y Oscar Alquicira Gálvez, op.cit.
[60] *Ídem.*
[61] FEMA, National Preparedness Goal 2015, Disponible en línea: http://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf Consultado: mayo de 2016
[62] National Initivative for Cybersecurity Careers and Studies, op.cit.

pérdidas financieras ocasionadas por un *hackeo* a intermediarios de la compra-venta de sus mercancías, mientras que *Sony* sufrió un daño mucho más severo, ya que hubo el uso de un *malware*[63] sofisticado para el robo de información privada de la empresa.[64]

La compañía *Pricewaterhouse Coopers* (PwC) en su trabajo *Global State of Information Security Survey 2016,* elabora una gráfica basada en las encuestas realizadas a las principales compañías mundiales que han sufrido pérdidas económicas significativas y que demuestra el estimado de pérdidas totales en todas las regiones y todas las industrias por incidentes/fallas en el sistema de seguridad de la información y que se muestra en la Gráfica 1.

Gráfica 1. Estimado total de pérdidas financieras como resultado de todos los incidentes en todas las industrias y regiones (en dólares americanos)

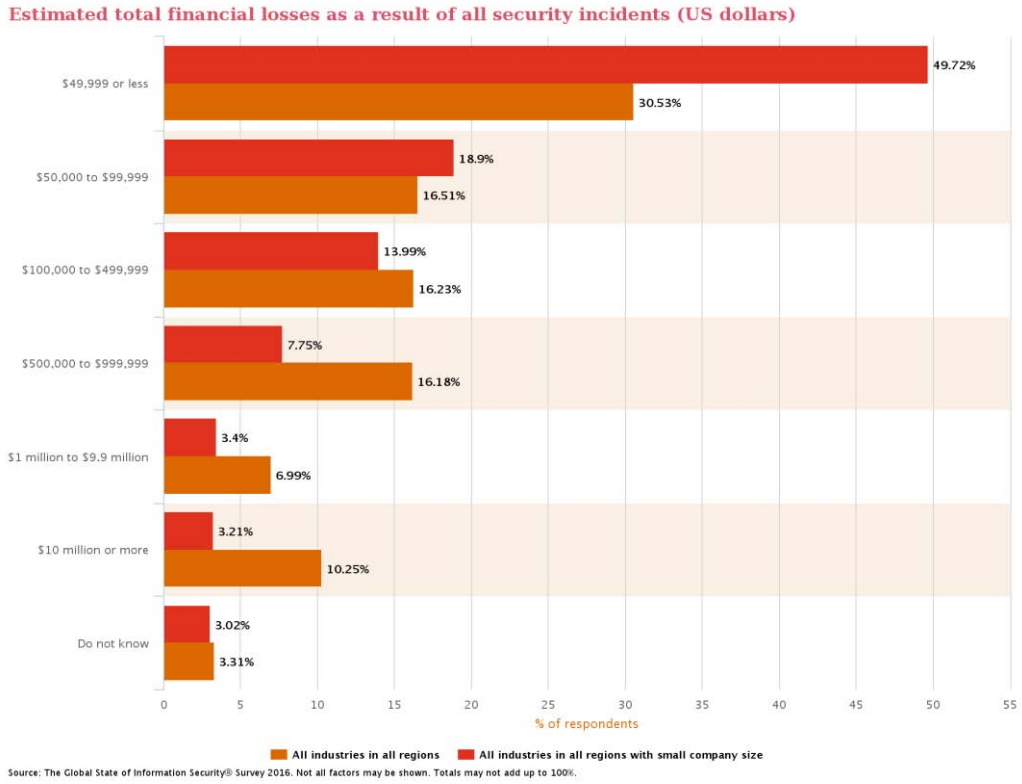


[63] Software que compromete el funcionamiento de un sistema mediante la realización de una función o proceso no autorizado.
[64] ISACA and RSA Conference Survey, State of Cybersecurity: Implications for 2015, Cybersecurity Nexus, Disponible en línea en: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf Consultado: mayo de 2016.

Fuente: The Global State of Information Security Survey 2016, PwC. Disponible en:http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html

Podemos observar que las pérdidas económicas por incidentes en los sistemas de seguridad de la información son altos, es en este sentido que se vuelve comprensible que PwC para el año 2016 pronostique un incremento en el presupuesto de los sistemas de seguridad. Asimismo, podemos hacer un análisis comparando los datos de la gráfica anterior, con el nivel de pérdidas económicas de empresas pequeñas presentada en la siguiente gráfica, mostrando cifras que demuestran que éstas últimas son las que cuentan con una menor infraestructura de seguridad cibernética y por lo tanto, son las más vulnerables a sufrir incidentes delictivos con pérdidas económicas considerables. Es así que la Gráfica 2 señala la cantidad de pérdidas financieras por incidentes de ciberseguridad en empresas chicas en todas las regiones y predominan las pérdidas de un valor menor a los 50 mil dólares pero que representan el 49.72% de sus pérdidas.

Gráfica 2. Estimado total de pérdidas financieras como resultado de todos los incidentes en todas las industrias y regiones en pequeñas y grandes empresas (en dólares americanos)

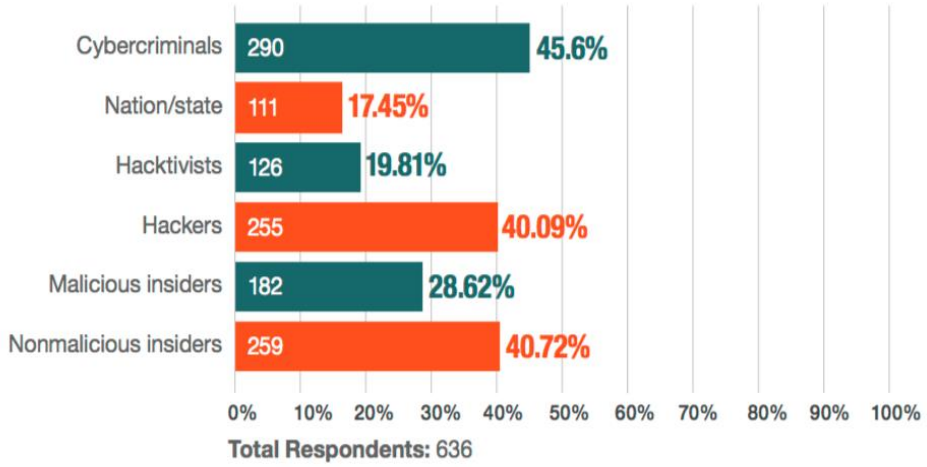


Fuente: The Global State of Information Security Survey 2016, PwC. Disponible en: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html

Es muy destacable el grado de vulnerabilidad a la que están sujetas las pequeñas empresas a los crímenes cibernéticos, lo que demuestra la necesidad de una mejor infraestructura de defensa y protección que va en incremento.

También la evaluación de ISACA en la Conferencia de la RSA[65] en el 2015, una compañía que provee de servicios de evaluación, protección de datos y estandarización de sistemas de información; realiza un resumen anual de referente sobre los perpetradores de los ciberataques haciendo una categorización desde cibercriminales hasta penetradores no-maliciosos como lo muestra la Gráfica 3.

Gráfica 3. Actores Amenaza que explotaron la empresa en 2014

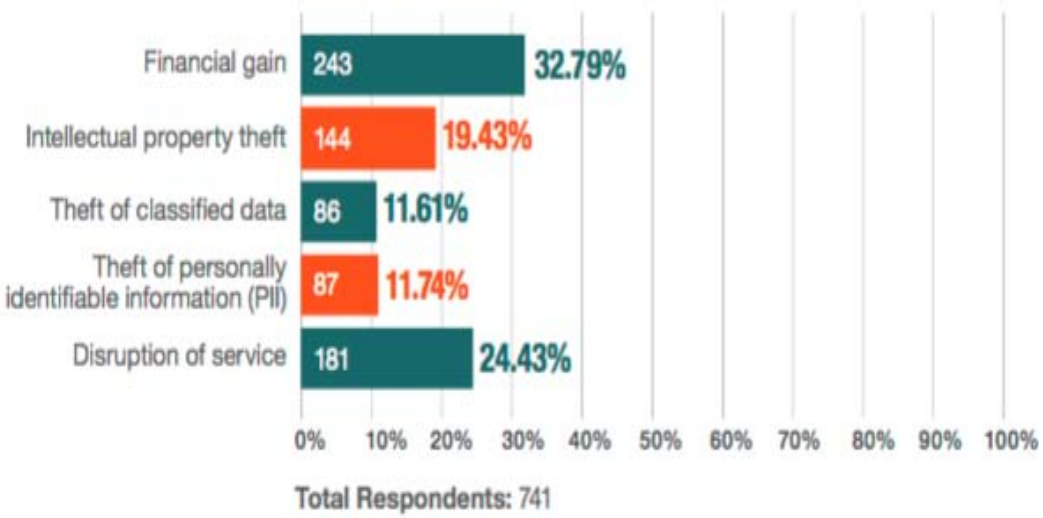


Fuente: ISACA and RSA Conference Survey, State of Cybersecurity: Implications for 2015, Cybersecurity Nexus, Disponible en línea en: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

[65] Una conferencia relacionada con la criptografía y la seguridad de la información, pero que ha sido criticada e incluso boicoteada por sus nexos con la Agencia de Seguridad Nacional de Estados Unidos.

En la gráfica se puede observar que los cibercriminales conforman casi la mitad de los intrusos al sistema[66] de información de las empresas, cuyas actividades *per se*, dañan a la compañía y terminan ocasionando daños que varían en su estimación. Es interesante observar que los porcentajes de actividad de los *hacktivistas* van en incremento, un ejemplo de esto, lo podemos ver en Latinoamérica con los ciberataques de *Anonymous* contra *Telefónica*. ISACA también arroja cifras interesantes sobre el motivo/ganancia de tal ciberataque en el que prevalece la necesidad de obtener una ganancia económica, interrumpir el servicio, robo de propiedad intelectual, robo de identidades y al último, robo de información confidencial tal como lo muestra la gráfica 4.

Gráfica 4. Motivaciones de los ataques



Fuente: ISACA and RSA Conference Survey, State of Cybersecurity: Implications for 2015, Cybersecurity Nexus, Disponible en línea: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

[66] Por cibercriminal es quien realiza actividades criminales utilizando los ordenadores e Internet, a menudo con fines económicos. *Hacktivista* es aquel que realiza explotación de los ordenadores y redes informáticas como medio de protesta para promover fines políticos. *Hacker* es quien usa sus habilidades para tener acceso a una computadora o red sin autorización. Malicious insider es aquel funcionario o empleado que tiene acceso a información clave de la empresa o institución y la explota con diversos fines. Un *nonmalicious insider* es un empleado, contratista o socio de negocios actual o anterior que tiene o ha tenido el acceso a la red o del sistema de datos de una organización y que, a través de su acción/inacción sin intención maliciosa, afecta negativamente a la confidencialidad, la integridad, o la disponibilidad de los sistemas de información o la información de la organización. Información obtenida en: Software Engineering Institute, https://www.cert.org/.

Yendo más a fondo de estas investigaciones, al revisar las cifras correspondientes a la industria gubernamental y militar podemos encontrar que la principal motivación detrás de estos ciberataques es la interrupción de los servicios/operación con un 42.31% y en un segundo lugar se encuentra el robo de información confidencial o crítica o estratégica con un 19.23%,[67] ambos suman el 61.54% del total de incidentes con un impacto crítico para la función del Estado, por lo que Estados Unidos fija los ciberataques como una prioridad a su seguridad nacional.

Aunado a las pérdidas económicas que los ciberataques pueden representar, le sigue la procedencia de éstos, en los que el principal autor y ladrón de propiedad intelectual de Estados Unidos es China, por lo que la respuesta estadounidense ha sido de engrosar sus capacidades de protección a sus sistemas de información mediante el uso de una seguridad de la información eficiente y resiliente.

Lo que integra la Seguridad de la Información (SI), es la protección de la información y los sistemas que los contienen para evitar todo acceso no autorizado, uso, divulgación, alteración, modificación o destrucción indebida de ésta. Los principios de confidencialidad, integridad, disponibilidad y no repudio; son propios de la SI, y se encuentran plasmados y definidos por la norma internacional ISO/IEC 27001, cabe agregar que este estándar internacional es el más importante para cualquier proceso de elaboración de estrategias de ciberseguridad.

En cuanto a la ciberdefensa y la ciberguerra, temas que ahondaremos en el capítulo 2 de éste trabajo, por lo pronto habría que señalar que la institución encargada es el *Department of Defense* (DoD), lo que incluye la protección de los intereses de Estados Unidos y su territorio. Esta instancia debe asegurar la estabilidad del ciberespacio, desarrollando las ciberfuerzas (personal de

[67] ISACA and RSA Conference Survey, op.cit.

operación, organización y las capacidades) necesarias para su protección, a la vez que se fortalece la ciberdefensa (operaciones de defensa) y la capacidad de disuasión en el ciberespacio.[68]

En los esfuerzos de coordinación de Estados Unidos para la implementación de una mayor ciberseguridad, se encuentra el *Department of Defense*, el *Homeland Security Department* con sus organismos de Análisis de Información y Protección de Infraestructura y la División de Ciberseguridad Nacional, también cuenta con la participación del *Department of Justice*.[69] Las agencias gubernamentales para la protección del ciberespacio son los Departamentos de *Energy*, *Commerce*, *Homeland Security*, *State*, *Transports*, Tesoro; cuenta con la participación de la Comunidad de Inteligencia, el Instituto Nacional de Estándares y Tecnología y la Oficina de la Administración y Presupuesto, [70] ya que hay que recordar que Estados Unidos considera el ciberespacio como un espacio sobre el que ejerce su soberanía y por lo tanto debe estar protegido.

Es así que tras la digitalización de las operaciones y la información de las compañías y departamentos de Estados Unidos, ha surgido la necesidad de cubrir las vulnerabilidades que sufren los sistemas digitales de dichas, creando ciberoperaciones y marcos legales que tienen una connotación anticonstitucional que muchos expertos en informática y en derecho han señalado y que la administración de Estados Unidos reconoce como un medio para lograr un fin ulterior, el de la defensa y protección de la seguridad nacional, bajo la instrumentación de complejos de seguridad.

En conclusión, la ciberseguridad es aquella habilidad de proteger o defender el uso del ciberespacio de ciberataques,[71] asimismo, entendemos que el

[68] The DoD Cyber Strategy, op.cit.
[69] FEMA, op.cit.
[70] *Ídem*
[71] National Counterintelligence and Security Center, Glossary, NCSC, Disponible en línea:

ciberespacio es un dominio global en el entorno de la información que consta de una red interdependiente de sistemas de información, incluido internet, las redes de telecomunicaciones, sistemas de cómputo y dispositivos con controladores y procesadores integrados.[72]

Dicho esto, podemos comprender que por el considerable número de infraestructuras críticas conectadas al ciberespacio que por formar parte del interés nacional, la estructuración y complejidad de la protección del ciberespacio, requieren de un alto grado de eficiencia en su defensa, pero que actualmente se han visto rebasadas las capacidades de Estados Unidos para afianzar la seguridad cibernética, de tal manera que sus respuestas han sido restrictivas y agresivas; un ejemplo de ello se ven reflejadas en su legislación sobre la propiedad intelectual y la privacidad, tal como lo fueron las leyes FISA y SOPA, que forman parte importante de las políticas de Barack Obama sobre ciberseguridad (y que le restaron mucha credibilidad a su gobierno) y los proyectos de defensa en el ciberespacio del *Department of Defense* con las ciberoperaciones que se describirán en el siguiente capítulo.

---

http://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf

[72] *Idem*

2. ESTRUCTURACIÓN DEL COMPLEJO DE CIBERDEFENSA Y CIBERSEGURIDAD PARA EL COMPLEJO DE SEGURIDAD CENTRADO

Esta sección de la investigación retoma las estructuras jurídicas y políticas en torno a la construcción del Complejo de Seguridad Centrado, analizando en un primer momento dos mini-complejos que fortalecen esta estructura y un tercero que será retomado hasta el tercer capítulo. Es decir, queremos presentar el marco normativo que se ha constituido para que el complejo de vigilancia pueda operar legalmente.

En este sentido, se hablará de los antecedentes políticos y jurídicos al primer periodo presidencial de Obama que servirán de eje para la continuidad de la creación de este Complejo de Seguridad Centrado. Se discutirá la perspectiva operacional del *Department of Defense* en torno a las misiones de ciberdefensa realizadas a través del uso del USCYBERCOM, que sostienen el complejo de ciberdefensa y la aportación que tienen los drones al complejo de vigilancia.

En el último subcapítulo se comentará la perspectiva del *Department of Homeland Security* sobre el ciberespacio formando parte del complejo de ciberseguridad con el uso del US-CERT en casos de emergencia y detección de amenazas generando reportes que darán aviso a las diferentes dependencias que componen los complejos de vigilancia y ciberdefensa, cabe aclarar, que en este capítulo no se ahondará en el complejo de vigilancia sino hasta el último capítulo de este trabajo.

2.1 Antecedentes de las políticas de ciberseguridad en Estados Unidos

Para entender la actual situación del complejo de vigilancia, debemos analizar primer antecedente de políticas de seguridad retomaremos a la propuesta realizada por el ex presidente William Clinton de invertir 1,460 millones de dólares. para fortalecer las capacidades de seguridad informática del gobierno y proteger la

infraestructura crítica del país en contra de los ciberterroristas,[73] misma en la que se proponía una alianza estratégica con el sector privado para compartir información sobre mecanismos de seguridad. Aunque ésta sería plasmada concretamente en su decreto presidencial del 16 de febrero de 2000, a la vez que se proponía el incremento del presupuesto de 9 millones de dólares en los programas clave de ciberseguridad y 2,000 millones de dólares para la protección de los sistemas de infraestructura crítica[74].

Sin embargo, el verdadero cambio de las políticas de seguridad nacional en torno a la ciberseguridad y vigilancia surgen tras los atentados del 11 de septiembre de 2001 en Estados Unidos bajo el primer periodo de George W. Bush como presidente, en el que el temor a sufrir otra agresión tan catastrófica como la caída de las Torres Gemelas o el ataque al Pentágono dirigió la opinión pública hacia el discurso de la supresión de las libertades civiles cuando fuese necesario para garantizar la seguridad nacional.

Por este motivo, el proceso que Estados Unidos llevará a cabo para cumplir con la obligación de proveer seguridad es en la construcción de marcos legales que fortalezcan las capacidades de vigilancia de las instituciones estadounidenses para la lucha contra el terrorismo. De esta manera, se logra la aprobación de la ley Patriota con apoyo de ambas Cámaras y fijando así el principio del articulamiento del complejo de vigilancia a lo largo y ancho de la federación.

La ley Patriota o USA PATRIOT Act (*Uniting and Strengthening America by Providing Appropiate Tools Required to Intercept and Obstruct Terrorism*) surge tras esta gran conmoción nacional y que tiene 9 objetivos principales, mejorar la seguridad interior contra el terrorismo; mejorar los procedimientos de vigilancia; la reducción internacional de lavado de dinero y contra la financiación del terrorismo;

[73] Matt Hamblen, *Clinton commits 1.46 B to fight cyberterrorism*, CNN, enero 1999, Disponible en línea: http://edition.cnn.com/TECH/computing/9901/26/clinton.idg/ Consultado: junio 2016
[74] The White House, *President Clinton: Working to Strengthen Cybersecurity*, White House at work, 16 febrero de 2000, Disponible en línea: https://clinton4.nara.gov/WH/Work/021600.html Consultado: junio de 2016

protección de la frontera; eliminación de los obstáculos a la investigación de terrorismo; proporcionar ayuda económica a las víctimas del terrorismo, oficiales de seguridad pública y sus familias; incrementar el intercambio de información para la protección de infraestructuras críticas; fortalecer las leyes penales en contra del terrorismo y mejorar la inteligencia.[75] Dentro de los aspectos relativos al tema estudiado, los podemos encontrar en 2 objetivos:

- Mejorar la seguridad interior: en la sección 105 de la ley se propone expandir el grupo de trabajo nacional contra delitos electrónicos o cibercrímenes que atenten contra la nación y sus infraestructuras críticas, asimismo se incluye el ciberterrorismo;[76]
- Mejorar los procedimientos de vigilancia: provee autoridad para interceptar comunicaciones por cables, orales y electrónicas relacionadas al terrorismo, al abuso y fraude cibernético; brinda autoridad para compartir información sobre la investigación criminal, fortalece el empleo de la ley FISA, facilita la incautación de mensajes de voz bajo órdenes judiciales, el acceso a registros telefónicos, el acceso a determinados registros del negocio para investigaciones de inteligencia extranjera y terrorismo internacional.[77]

La ley permite usar cualquier medio necesario para investigar a cualquier sospechoso de terrorismo y luchar contra el mismo, el medio más usado actualmente es a través de la vigilancia electrónica, regida bajo la ley FISA, sin embargo, dentro de la misión de la ley Patriota no se excluye la lucha contra el crimen organizado y todo aquél que tiene como propósito ejecutar ataques y financiar células terroristas o criminales mediante actividades ilícitas en el ciberespacio, que es un alcance muy novedoso que integra lo ya propuesto en su momento por Bill Clinton.

---

[75] United States Government Publishing Office, *USA PATRIOT Act*, 107th Congress of the United States of America, Disponible en línea:https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf Consultado: junio 2016
[76] *Idem.*
[77] *Idem.*

Asimismo, la ley Patriota les facilita a las instituciones gubernamentales de Estados Unidos vigilar dentro del país[78] y dar seguimiento a aquellos sujetos bajo sospecha de ser partícipes en actividades terroristas; aunque cabe resaltar que esta ley rescata los procedimientos legales y judiciales utilizados con el narcotráfico y otros crímenes de la delincuencia organizada por lo que demuestra la ambición de la ley por fortalecer los mecanismos de seguridad dentro y fuera del país.

Cabe destacar que durante el cabildeo de la Ley Patriota, el actual viceperesidente de Estados Unidos, Joe Biden -que durante la administración de George W. Bush fungía como Senador-, apoyó ésta ley bajo la efectividad obtenida para la procuración de la justicia. Barack Obama por su parte, fue co-patrocinador de una propuesta de ley que limitaría el uso de la ley Patriota por las instituciones gubernamentales, pero no logró ser aprobada. Al ver Obama su derrota y no poder abstenerse, votó a favor de la reautorización de la ley Patriota y a pesar de esa derrota mantuvo su postura en contra de los programas de intervención de las líneas telefónicas y en pro de las libertades civiles,[79] ejemplo de esto lo podemos encontrar en su discurso del 1 de agosto de 2007:

> [La actual administración] propone una elección falsa entre las libertades que apreciamos y la seguridad que requerimos. Le proveeré a nuestras agencias de inteligencia y aplicación de la ley las herramientas necesarias para rastrear y sacar a los terroristas sin socavar nuestra Constitución y nuestra libertad.[80]

Obama mantuvo esta misma postura durante su campaña electoral. No obstante, fue muy criticado por la falta de congruencia con las actividades de su gobierno,

---

[78] Ya que apoya a las autoridades y dependencias a solicitar cualquier tipo de información sobre un sujeto en específico bajo una orden judicial.

[79] Se puede encontrar en su voto en contra la nominación de Bush para el nuevo director de la CIA cuyo candidato era Hayden, que había sido el anterior director de la NSA que había puesto en marcha el programa de intervención telefónica sin orden judicial.

[80] Barack Obama, *Woodrow Wilson Center Speech*, Council on Foreign Relations, Estados Unidos, 1 de agosto de 2007, Disponible en línea: http://www.cfr.org/elections/obamas-speech-woodrow-wilson-center/p13974 Consultado: marzo de 2016 .
Ver también: Bob Parks, *Obama's 2007 Promise 'No more illegal wiretapping of American Citizens',* Disponible en línea: http://www.cnsnews.com/blog/bob-parks/obamas-2007-promise-no-more-illegal-wiretapping-american-citizens Consultado: abril de 2016.

un caso ejemplar fue la revelación[81] de la recolección de archivos[82] en masa por la NSA, y a lo que él aclaró que dicha actividad no es específica, sino que tiene que ver con la filtración o proceso de los datos a través de los llamados metadatos[83]. Pero este caso nos da un ejemplo de que Barack Obama no a modificado el curso de la estructura del complejo de vigilancia, la perspectiva de un estado en alerta, como lo establece la ley Patriota, continúa; en este sentido, para el presidente debe "reconocer(se) que no se puede tener cien por ciento de seguridad, cien por ciento de privacidad y cero inconveniencia".[84] De acuerdo con lo anterior podemos identificar que unas de las críticas más fuertes hacia Barack Obama serán respecto a las acciones de vigilancia de su administración.

Otro problema que hay que tocar como antecedente del marco de programas de vigilancia es el conflicto interinstitucional entre la *Central Intelligence Agency* (CIA) y el *Federal Bureau Investigation* (FBI) tienen desde su concepción. La creación de la CIA es después los años más álgidos de tensión entre la Unión Soviética y Estados Unidos en 1964 y trajo consigo la idea de concentrar o centralizar toda la información de inteligencia[85] que consiste en:

> [Todo aquél] conocimiento adquirido a partir de la recolección, sistematización y análisis de información relativa a actores o situaciones que presenten un riesgo o amenaza a la seguridad nacional y que se utiliza en la toma de decisiones para anticipar acciones y neutralizar amenazas.[86]

---

[81] Registros telefónicos en específico

[82] Obama, oportunamente, aclaró que la recolección de *e-mails* y vigilancia de Internet no está siendo aplicada dentro de territorio estadounidense y a ciudadanos estadounidenses, por lo que no se descartan otras nacionalidades.

[83] Que son datos que están inyectados de forma relativamente oculta como parte de una información añadida a cualquier archivo que se genere en un equipo informático bajo cualquier software que edite o escriba ese archivo.

[84] Barack Obama, *Statement by the President*, The White House, Fairmont Hotel, San José California, junio de 2013, Disponible en línea: https://www.whitehouse.gov/the-press-office/2013/06/07/statement-president Consultado: marzo de 2016

[85] Que podemos identificar en tres tipos, Información clasificada: información sensible cuyo acceso está regulado por el Estado a través de leyes y procedimientos específicos, y su nivel de protección está basada en el daño potencial que puede provocar la posesión de esta en manos enemigas. Información confidencial: datos que requieran el consentimiento de los individuos para su difusión, distribución o comercialización. Información estratégica: toda información generada por los Estados o las entidades privadas que sirve de base para la formulación de políticas y programas en un horizonte de mediano y largo plazo.

[86] Glosario de Términos de inteligencia y Seguridad Nacional, Serie Manuales y Guías Núm. 3, México, Noviembre de 2011

Bajo el precepto de “conocimiento es poder”, una de las instituciones más fortalecidas con la ley Patriota será la CIA, ya que el respaldo legal de las actividades que realiza en secreto quedan cubiertas bajo lo establecido en dicha ley,[87] en este sentido, la inteligencia creada a partir de esta agencia ayuda a reducir la incertidumbre en una situación de conflicto y otorga al poseedor, una ventaja sobre la interacción con el actor o la situación que representa un riesgo o amenaza.[88]

Por su parte, la creación del FBI como dependencia del *Department of Justice* (DOJ) bajo la dirección de Edgar Hoover, tuvo como propósito armar los casos legales con pruebas criminales tangibles; es decir, llevar a los criminales ante el sistema judicial de Estados Unidos y que cumplieran su sentencia. Sin embargo, la causa principal por la que Hoover se mostraba reticente a aceptar la creación de la CIA, es porque en principio esta agencia estaba por encima de la ley (por su carácter independiente) y no seguía los esquemas de la legalidad con el uso extremo de la secrecía, la tortura y la autonomía con la que se desenvolvía la agencia dentro de la toma de decisiones del gobierno, lo cual era motivo suficiente para reprobar las actividades que realizaría y realiza en nuestros días.

También es importante resaltar la competencia entre agencias por el presupuesto asignado anualmente a la Comunidad de Inteligencia (IC), [89]creada tras los ataques del 11 de septiembre bajo la recomendación de reforma conjunta del Congreso y la Comisión Nacional sobre los Ataques Terroristas contra Estados Unidos (conocida como Comisión 9/11)[90] y que está conformada por las siguientes instituciones gubernamentales presentadas en la Tabla 1.

---

[87] Of-course-they-do, *FBI And CIA Use Patriot Act's Bulk Data Collection To Get Money Transfer Data*, TechDirt, noviembre 2013, Disponible en línea:https://www.techdirt.com/articles/20131115/02480125256/ Consultado: junio 2016

[88] *Ídem*

[89] Encargada de la recopilación y análisis de inteligencia necesaria para el manejo de las relaciones exteriores y la seguridad nacional.

[90] Comisión independiente, bipartidista creada por la legislación del Congreso y el presidente George W. Bush a finales del año 2002. Su propósito, rendir cuentas sobre las circunstancias y los daños ocasionados por los ataques y la preparación y respuesta inmediata para los ataques, asimismo, está articulada para emitir recomendaciones para la protección ante futuros ataques.

Tabla 1. Comunidad de Inteligencia

Drug Enforcement Administration (DEA)	Department of State (SD)
Central Intelligence Agency (CIA)	Department of Treasury (DT)
Defense Intelligence Agency (DIA)	Department of Homeland Security (DHS)
National Security Agency (NSA)	Navy Intelligence (NI)
National Intelligence-Geospatial Agency (NGA)	Army Intelligence (AI)
Federal Bureau Investigation (FBI)	Air Force Intelligence (AFI)
Marine Corps Intelligence (MCI)	Coast Guard Intelligence (CGI)
Department of Energy(ED)	National Reconnaissance Office (NRO)[91]
Director of National Intelligence (DNI)	

Fuente: Elaboración propia, información obtenida en: https://www.dni.gov/index.php/intelligence-community/members-of-the-ic

La IC está dirigida por la oficina del Director de Inteligencia Nacional (DNI), quien electo bajo la potestad del Presidente y con aprobación del Senado es una de las personas más poderosas e importantes de Estados Unidos, el puesto surgió con el propósito de fortalecer el papel del Presidente y ser su refuerzo durante las decisiones políticas más importantes del país relacionadas con la seguridad nacional; el DNI es el encargado de proveer toda aquella información de inteligencia, "al Presidente y a su gabinete, al Jefe del Estado Mayor Conjunto de los Estados Unidos, al Senado y la Casa de los Representativos y a cualquier persona que el DNI considere apropiado".[92]

La Oficina del DNI, como una agencia independiente (a la par de la CIA), según su acta constitutiva, *Intelligence Reform and Terrorism Prevention Act* del 2004 (IRTPA), esta dependencia no se encuentra dentro de la Oficina Ejecutiva del Presidente, por lo que goza de la independencia pero también funciona como un contrapeso al poder que tiene la CIA en el manejo de información clasificada y

[91] La diferencia entre la NRO y la NGA radica en que la primera es de carácter militar, su información es clasificada y compartida entre las agencias y oficinas del gobierno relativas al monitoreo, operación y auxilio de operaciones militares en los diferentes escenarios del mundo, mientras que la NGA puede ser de acceso a civiles y militares con fines pacíficos o de investigación así como la prevención de desastres naturales.

[92] 108º Congreso de los Estados Unidos de América, Reforma de Inteligencia y Acta de prevención terrorista del 2004, Ley Pública 108-458, Estados Unidos, Diciembre 17 2004, Disponible en línea: https://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf Consultado: abril de 2016

confidencial, ya que, como se mencionó anteriormente, el DNI puede tener acceso a cualquier información siguiendo los protocolos normativos previstos, que la dotan de enormes facultades y manejo de información dentro del ámbito de la inteligencia y la seguridad nacional con el fin de mantener el equilibrio de la IC .

No podemos pasar por alto un elemento muy importante sobre la creación de DNI como un nodo para compartir información: los atentados terroristas demostraron que las agencias e instituciones de inteligencia estaban encaminadas únicamente a "evaluar las capacidades e intenciones de los extranjeros", [93] mientras que las instituciones encargadas de la procuración de la ley, recolectaban información sobre asuntos y cuestiones domésticas;[94] de este modo fue clara la necesidad de compartir información en un alto nivel, dada la incapacidad de la Cuarta Enmienda de la Constitución para compartir información de la inteligencia extranjera con fines nacionales es ilegal.

Por otra parte, la asignación de los presupuestos para los 17 miembros de la IC es canalizado mediante el *National Intelligence Program* (NIP), asignado anualmente y hecho público gracias a que el *Comité 9/11* emitió una propuesta en el año 2007 para desclasificar el presupuesto asignado al NIP y al *Military Intelligence Program* (MIP); dicha proposición fue aprobada bajo la sección 601 de las Recomendaciones de la Aplicación de la ley de la Comisión 9/11 en el 2012, de acuerdo con los lineamientos de gobierno abierto y transparencia se hicieron públicos las solicitudes de asignación de presupuesto globales; sin embargo, cabe rescatar que el presupuesto para estos dos programas es totalmente público pero no las asignaciones a cada una de las actividades y de las agencias relacionadas en el NIP; el MIP al ser coordinado por el DoD, es de carácter confidencial por razones de seguridad nacional.

---

[93] AFCEA Intelligence Committee, *The Need to Share: The US. Intelligence Committee and Law Enforcement,* White Paper, Estados Unidos, Abril de 2007, Disponible en línea:http://www.afcea.org/mission/intel/documents/SpringIntel07whitepaper_000.pdf Consultado: mayo de 2016

[94] *Ídem.*

El presupuesto asignado para el NIP en el año 2007 fue de 43, 500 millones de dólares y para el 2015 fue de 50, 300 millones de dólares con un aumento de un 11.5%. Mientras que el MIP en el año 2007 tuvo asignados 20 mil millones de dólares y 16, 500 millones de dólares en el año 2015, lo cual refleja una baja del 8.25%. Para el año fiscal 2016 se solicitó un presupuesto de 53, 900 millones de dólares y 17, 900 millones de dólares para el NIP y el MIP respectivamente, pero para el 2017 se hizo la propuesta de 53, 500 millones de dólares y 16, 800 millones de dólares para el NIP y el MIP respectivamente[95].

Es interesante ver una baja en los presupuestos, si bien las guerras en el exterior continúan y se ve poco probable que finalicen en el año 2017, no existen diferencias contundentes en los *National Intelligence Program* entre el año 2016[96] y 2017.[97] Lo que hay que observar es la concentración de los recursos reubicados hacia nuevas tecnologías y cómo la asignación de presupuestos para la Comunidad de Inteligencia va en aumento mientras que el presupuesto para el MIP va decreciendo, y que demuestra una vez más que las estructuras que se fortalecen son las del complejo de vigilancia.

Esto puede ser comprobado al observar el reportaje del Washington Post de 2013 sobre el "Black Budget" que suma cerca de 52.6 mil millones de dólares (mmdd) clandestinos destinados a éstos programas, en donde la CIA, la NSA y la NRO que unidos suman el 68% de éste fondo, cuya distribución se encuentra en cuatro áreas principales: colección de datos, análisis de datos, administración e instalaciones y apoyo[98]. También podemos encontrar que financian cinco misiones principales: advertir a los líderes estadounidenses sobre eventos críticos con un

---

[95] *Ídem*.
[96] ODNI, *Requested Budget Figure for FY 2016 Appropiations for the National Intelligence Program*, ODNI, Estados Unidos, febrero 2 2015, Disponible en línea: http://www.dni.gov/files/documents/FY%202016%20NIP%20Fact%20Sheet.pdf Consultado: abril de 2016
[97] ODNI, *Requested Budget Figure for FY 2017 Appropiations for the National Intelligence Program*, ODNI, Estados Unidos, febrero 9 del 2016, Disponible en línea:http://www.dni.gov/files/documents/Newsroom/Press%20Releases/FY2017NIPRequestedfactsheet.pdf Consultado: mayo de 2016
[98] Washington Post, *The Black Budget*, abril 29 de 2013, Disponible en línea: http://www.washingtonpost.com/wp-srv/special/national/black-budget/ Consultado: junio de 2016

gasto de 20,1 mmdd, combatir el terrorismo con 17,2 mmdd, detener el tráfico ilícito de armas con 6,7 mmdd, conducir ciberoperaciones con 4,3 mmdd y defensas contra el espionaje con 3,8 mmdd[99].

En el siguiente subcapítulo se hablará de la estructura jurídica que Obama adoptó para disfrazar la necesidad de su gobierno de ser intrusivo bajo esquemas de ciberseguridad, estrategias que si bien plasman una urgencia por contar con datos acerca de los peligros provenientes del ciberespacio, busca fortalecer los mecanismos gubernamentales y obtener control sobre el flujo de información.

2.2 Las políticas de ciberseguridad de la administración de Obama

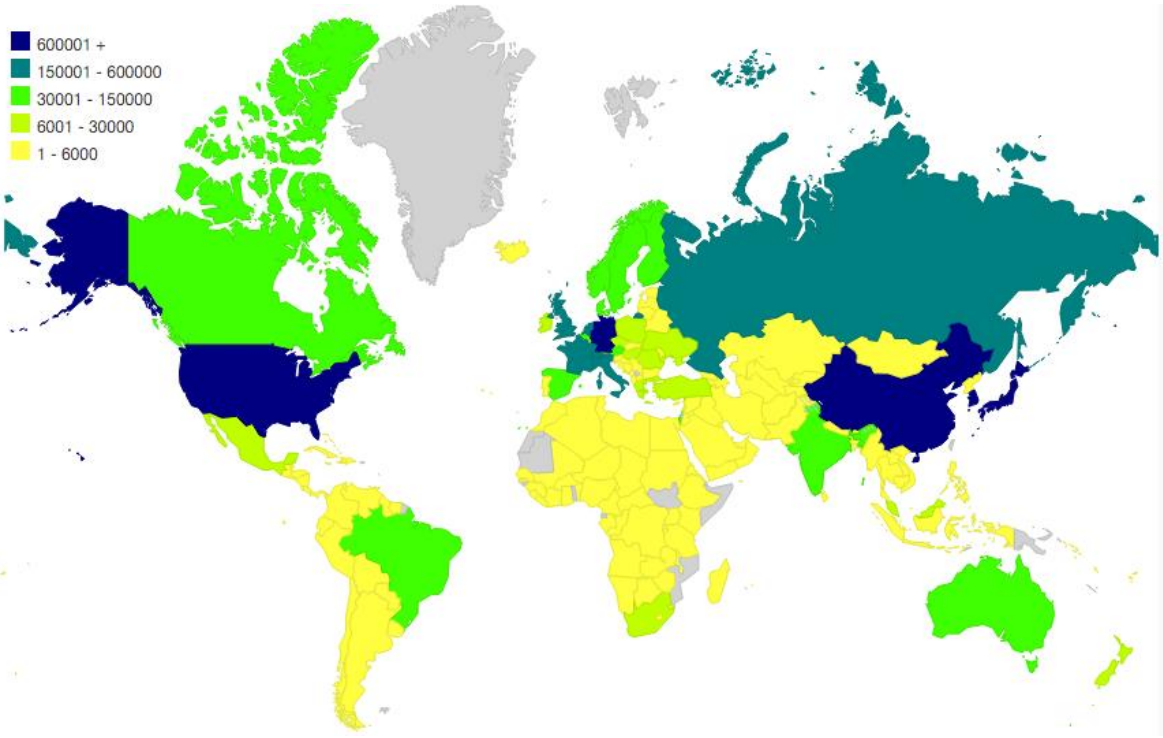
La administración de Barack Obama inició con la intención de ser diferente a su predecesor republicano George W. Bush en cuanto al respeto de las "libertades civiles, [los derechos humanos] y [el derecho a] la privacidad en concordancia con las leyes y principios de Estados Unidos".[100] Como creemos haber demostrado en el subcapítulo anterior, a lo largo de su primer periodo presidencial se fue modificando esta situación y por contrario continuó con el fortalecimiento de las políticas de su predecesor, bajo el pretexto de que todo beneficio en materia de seguridad tiene un precio, éste es la supresión de las libertades civiles.

Barack Obama no tuvo un inicio fácil en su primer periodo, esto se explica con su iniciativa de ley SOPA y las implicaciones que tuvo sobre éste con la comunidad cibernética y diversos defensores de la libertad de expresión en el Internet. La *Stop Online Piracy Act* surgió como una de las respuestas del gobierno de Obama a todas aquellas violaciones de derechos de autor o de propiedad intelectual,[101] y que figura como uno de los principales objetivos de su "Estrategia Internacional de Ciberseguridad", que abordaremos más adelante. El

[99] *Idem.*
[100] Charlie Savage, *Power Wars: Inside Obama's post-9/11 presidency*, Little brown and Company, Estados Unidos, noviembre de 2015, pp. 769.
[101] Dentro de los cuales figurará Aaron Swartz, un hacktivista en pro de la libertad del conocimiento y una gran figura pública opositora de dicha ley, sobre la cual se hablará en el capítulo 3.

supuesto que se advierte en este documento es que debido a la necesidad que requiere la protección de la propiedad intelectual e industrial para los Estados Unidos (véase el Mapa 1), es motivo suficiente para robustecer el complejo de vigilancia a lo largo y ancho del país, con intrumentos legales que faciliten y legitimen el ejercicio de estos programas; es por ello que es pertinente hacer un paréntesis y mostrar el nivel de importancia que este rubro ha tenido para la administración de Obama.

Mapa 1. Número de patentes registradas al año por país



Fuente: WIPO, disponible en: http://ipstats.wipo.int/ipstatv2/ipsMapchart

Como se puede observar en el mapa el número de patentes por origen ~~de~~ entre los años 2009 a 2014 por sector de tecnología,[102] en el que el gradiente de color indica un menor número de publicaciones de patentes, Japón tuvo 2,768,878

[102] Hacemos hincapié en este rubro pues es el más importante a nivel mundial. Sin embargo, Estados Unidos en todos los demás tipos de patentes se ubica entre los primeros cinco lugares mundialmente.

registros, seguido de Estados Unidos con 2,408, 717, y en número descendiente: China con 2,329,111; Alemania 1,074,301; República de Corea 1,028,135 y Suiza 227, 905, -podemos agregar que México tuvo un número de 9,860 resgistros-.

Estas cifras explican por qué es tan relevante la protección de sus planes y secretos comerciales, sin excluir aquellos desarrollos tecnológicos que están en proceso y que pueden ser plagiados por compañías o agencias pagadas por países. Asimismo, indica que el avance en las políticas de propiedad intelectual van en auge y han formado parte de las prioridades de la política exterior de Estados Unidos, ya que cada vez es indispensable la legalidad de las cosas frente a la competencia del exterior, debido a que la tecnología día a día permea las esferas de la cotidianeidad de los individuos y con esto su conectividad a la red mundial de comunicaciones.

Parece oportuno retomar lo anteriormente representado en la gráfica para así poder referirnos a la *International Strategy on Cybersecurity* (ISC) de la Casa Blanca en el año 2011, este documento se enfatiza en sus 4 secciones la creación de marcos normativos y asociaciones internacionales, para la protección de la seguridad nacional y de los intereses nacionales de Estados Unidos.

El primer capítulo es introductorio donde se plasman los principios y valores fundamentales de la cultura estadounidense. En el segundo capítulo, “El futuro del ciberespacio”, está compuesto por dos subcapítulos a su vez: “El futuro que perseguimos” cuyo objetivo es construir un ambiente de normas de conducta para guiar las conductas de los Estados, mantener las asociaciones y apoyar el imperio de la ley. Este ambiente de normas incluyen los principios de sostener las libertades fundamentales, el respeto a la propiedad, valuar la privacidad, la protección del crimen y el derecho a la autodefensa. En el segundo subcapítulo, “Nuestro papel en el futuro del ciberespacio” son los medios por los que se defenderán dichas normas, como la utilización de la diplomacia, la milicia y las

asociaciones internacionales de seguridad cibernética en el que los tres medios son indispensables para la estabilidad del ciberespacio.

En el tercer capítulo menciona las prioridades de la políticas de ciberseguridad para Estados Unidos las cuales son las siguientes:

- Economía: en este rubro se habla sobre hacer certero la capacidad de responder a las necesidades de la economía y el desarrollo tecnológico innovador, en este punto se busca fortalecer el libre mercado para los innovadores, los altos estándares de calidad y la libre competencia, en resumen, se busca abrir y asegurar la participación de los productos estadounidenses en el comercio electrónico. Asimismo, en un segundo punto se busca proteger la propiedad intelectual, incluyendo aquellos secretos comerciales[103]. En un último lugar se coloca la necesidad de crear estándares de ciberseguridad y la implementación de productos creados bajo estos estándares que representan la confianza entre partes.[104]
- Protección de red para la seguridad económica: Este punto promueve la estabilidad del ciberespacio mediante normas y estándares con aquellos países que comparten objetivos para establecer reglas para el comportamiento entre Estados. En un segundo lugar está la reducción de intrusiones o disrupciones de las redes estadounidenses. En un tercero, el manejo de incidentes, advertencias y resiliencia en el que se realiza el intercambio de información con aquellas redes formadas con socios internacionales.

[103] Un secreto comercial tiene un nivel de confidencialidad y diferentes tipos, puede ser una práctica, proceso, fórmula, diseño, método o la generación de conocimiento a través del desarrollo de procesos que de ser conocidos por alguna empresa se obtiene una ventaja considerable frente a la que se le roba la información, Estados Unidos protege dichos secretos bajo la Ley 18 U.S.C. § 1839. Véase Legal Information Institute, 18 U.S.C. § 1839-Definitions, Cornell University Law School, Disponible en línea: https://www.law.cornell.edu/uscode/text/18/1839 Consultado: mayo de 2016

[104] White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, White House, Mayo 2011, Disponible en línea: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf Consultado: mayo de 2016

En un último lugar, mejorar la seguridad en la cadena de suministros de alta tecnología trabajando vis-a-vis con la industria y socios internacionales para desarrollar “mejores prácticas” para la protección de los sistemas de información e infraestructura crítica.[105]

- Cumplimiento de la ley: Este punto habla en un primer momento sobre la pro-activa participación de los Estados Unidos para la persecución de los cibercrímenes como la Conferencia de Budapest ligada al objetivo del segundo punto, el armonizar las leyes referentes a la cibercriminalidad, que faciliten compartir evidencia, extradición y otros tipos de coordinación. En un tercer lugar, la creación de leyes que luchen contra las actividades ilícitas en el ciberespacio sin limitar el nivel de actividad de los usuarios en internet. En último lugar, está el negarle a los criminales y terroristas la capacidad de expandir sus actividades en el ciberespacio, ya sea para planeación, financiamiento o ataques.[106]
- Militar: este apartado consta de mantener íntegra la capacidad de la milicia para defender la seguridad nacional y los bienes nacionales, en primer lugar mantener constante la adaptación de la milicia para obtener redes seguras y confiables, en un segundo lugar está el mejoramiento de la construcción de alianzas militares que buscan confrontar amenazas potenciales en el ciberespacio, en un último lugar, la seguridad colectiva mediante nuevas formas de trabajo y cooperación como análisis forense digital, desarrollo de fuerza laboral, pruebas de penetración de la red y resiliencia.[107]
- Gobernanza: en este rubro se habla en un primer lugar, de priorizar la apertura e innovación del internet a pesar de aquellos Estados que restringen el acceso a la información para no tener disidencia u oposición, asimismo, el cumplimiento de las leyes no debe acomodarse a decisiones que violen las libertades fundamentales o

[105] *Ídem.* p.18-19.
[106] *Ídem*. p.19-20.
[107] *Ídem*. p. 20-21.

que minen la innovación. En un segundo lugar, está el preservar la operatividad del internet, mediante la protección del DNS (Domain Name System)[108]. En un último lugar, promover la discusión de la gobernanza del internet a un nivel internacional con la inclusión de las partes interesadas, gubernamentales o no gubernamentales para contribuir a la discusión en un nivel equitativo entre las partes.[109]

- Desarrollo Internacional: en un primer momento se menciona la ayuda a otros países interesados en aumentar y/o mejorar sus capacidades de ciberseguridad, en las que Estados Unidos brindará apoyo tecnológico, conocimientos o entrenamiento. En un segundo momento, continuar con el desarrollo y contribución de las mejores prácticas en ciberseguridad. En un tercer momento, está el mejorar las capacidades de los Estados para luchar el cibercrimen mediante el cumplimiento de la ley y la asistencia técnica e investigativa. En último lugar está el desarrollar relaciones con los políticos para mejorara la capacidad técnica con apoyo de expertos o contrapartes estadounidenses como sucedió durante la Conferencia del Meridiano.[110]
- Libertad del Internet: este es el último rubro del capítulo y el más controversial de todos, ya que en el primer punto se propone apoyar a la sociedad a lograr plataformas de expresión y asociación confiables, seguras y a salvo, asimismo se busca fomentar a las personas alrededor del mundo a “expresar su opinión, compartir

[108] Es una base de datos distribuida, con información que se usa para traducir los nombres de dominio, fáciles de recordar y usar por las personas, en números de protocolo de Internet (IP) que es la forma en la que las máquinas pueden encontrarse en Internet. Cfr. ¿Qué es el domain name system? http://www.desarrolloweb.com/faq/50.php Consultado: mayo de 2016

[109] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,* op.cit. p. 22-23

[110] Tiene como objetivo el intercambio de ideas e iniciar acciones de cooperación de gobierno a gobierno sobre cuestiones de protección de infraestructuras críticas de información a nivel mundial. Es una conferencia anual y actividades provisionales se llevan a cabo cada año para ayudar a construir la confianza y establecer relaciones entre los miembros para facilitar el intercambio de experiencias y buenas prácticas en materia de protección de infraestructuras críticas de información de todo el mundo. Cfr. Meridian Conference Process, IT Wiki Law Disponible en: http://itlaw.wikia.com/wiki/Meridian_Conference_and_Process Consultado: mayo de 2016

información, monitorear elecciones, exponer la corrupción y organizar movimientos sociales y políticos, también denunciar acosos, arrestos injustos, amenazas o los actos violentos que son perpetrados a las personas que usan las nuevas tecnologías"[111], en sencillas palabras se busca alentar la denuncia, la organización y el intercambio de ideas. En este mismo punto se busca proteger a los Proveedores de Servicio de Internet y otros relacionados con la conectividad, de aquellos regímenes legales que prohíben la publicación de cierta información, ya que uno de los principios fundamentales de Estados Unidos es la libertad de expresión, a lo que conlleva empoderar a la sociedad civil, los abogados de derechos humanos y los periodistas en su uso de medios digitales. En un segundo lugar está colaborar con la sociedad civil y organismos no gubernamentales a protegerse a si mismos de las intrusiones. En un tercer lugar está fomentar la cooperación internacional para la protección de la privacidad de los datos individuales así como de las demás partes interesadas, endureciendo el marco de privacidad comercial estadounidense aplicando principios basados en contexto pero flexibles para la innovación. En un cuarto y último lugar, está la interoperabilidad, de fin-a-fin sin importar el origen nacional o el destino, ya que asegurando el flujo de información íntegro mantiene el internet como una plataforma confiable.[112]

Analizando la conceptualización de las amenazas en el ciberespacio y la ciberseguridad mediante el uso de la palabra *cyber* dentro del documento y es intrigante ver el número de menciones que podemos observar en la Gráfica 5.

[111] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,* op.cit. p.23
[112] *Ídem*. p.23-24

Gráfica 5. Distribución del uso del término "ciber" en la ISC (2011)

Fuente: Tripwire, Distribution of Usage- "cyber" U.S. International Strategy for Cyberspace (2011), http://www.tripwire.com/state-of-security/government/understanding-u-s-nss-2015-using-the-international-strategy-for-cyberspace/

En la gráfica presentada vemos como la palabra *ciberespacio* ocupa el 62% del documento, mientras que *ciberseguridad* representa un 26% y el binomio *cibercrimen/criminal* un 14%; pero el documento a pesar de ser sobre ciberseguridad no menciona dos términos muy populares hoy en día, *ciberataque* y *ciberguerra*, que son dos términos que retomaremos para el siguiente subcapítulo de esta tesis.

En la ISC se mencionan los principios medulares de Estados Unidos, las libertades fundamentales, la privacidad y el libre flujo de la información, también se habla de la protección de la seguridad nacional y la defensa del bien nacional por medios militares, sin embargo, al ojo público la realidad es otra. Regresando a la ley SOPA, podemos identificar que dicha ley es acorde con la ISC, en el sentido de la protección de los derechos de propiedad intelectual pero infringe otros considerados dentro de dicha estrategia como el uso de las redes para la libertad de asociación, la libertad de expresión y la privacidad.

Debido al exponencial crecimiento de las actividades a través, en y por el ciberespacio, Barack Obama asumió un rol protagónico sobre el ciberespacio que estuvo relegado años atrás y que era dominio jurisdicción independiente por parte de los departamentos y agencias; a través de la elaboración de esta estrategia, mucho más ambiciosa, persigue la unión entre instituciones gubernamentales que hoy en día se encuentra débil y delicada por cuestiones de recelo por presupuesto y la creciente demanda por usar artefactos no tripulados y otros medios, para obtener información o realizar operaciones.

Sin embargo, estos marcos legales de acción dan fundamento para nuevos sistemas evolutivos de vigilancia e inteligencia, que posibilitan el cumplimiento de la ley y que son motivo de discusión y controversia, como los programas de la NSA, el DoD y el FBI.

Como último evento respecto a la legislación en ciberseguridad, está la iniciativa de ley *Cybersecurity Information Sharing Act* (CISA) propuesta por el Senador republicano Richard Burr, aprobada por el Senado, que en resumen surge como una protección a las empresas privadas sobre la recopilación de información y el tipo de información confidencial que se maneja, es decir, si existe una amenaza que sea de interés, ésta ley exige que se haga de su conocimiento a las partes interesadas[113]. Cabe destacar, que no es sorpresa que pase el Senado y posteriormente la Casa de Representativos, puesto que la mayoría de ambos está compuesto por el partido Republicano, sin embargo, aún no es ley.

En el siguiente subcapítulo se hablará de los instrumentos de vigilancia y ciberseguridad de la administración de Obama, que son los responsables de los programas que restan de legitimidad al discurso del presidente y que sus "intentos" por crear políticas de seguridad en el ciberespacio minan el desarrollo de los individuos y atentan contra sus libertades fundamentales, en específico, el

[113] 114th Congress, Cybersecurity Information Sharing Act of 2015, marzo 17 de 2015, Disponible en línea: https://www.congress.gov/bill/114th-congress/senate-bill/754 Consultado: julio 29 de 2016

derecho a la privacidad; en el que el ciberespacio es un medio más para realizar actividades hostiles no sólo contra Estados enemigos sino también contra su población. Es por este motivo, que el siguiente subcapítulo se mostrará la visión del *Department of Defense* sobre este quinto espacio y las operaciones y estructuras que este departamento implementa para beneficio del complejo de ciberdefensa y vigilancia.

2.3 Complejo de ciberdefensa

En el proceso de securitización de los problemas del ciberespacio, una estructura muy importante de este complejo de vigilancia de Estados Unidos es el *Department of Defense* (DoD), que más que vigilar realiza operaciones hostiles bajo el argumento de una ciberdefensa preparada y disponible en cualquier momento para proteger las infraestructuras críticas del gobierno y del país.

Durante la Guerra Fría, Estados Unidos requería la creación de tecnologías militares que pusieran al país en una situación de igualdad tecnológica con la Unión Soviética. Es así que en respuesta al lanzamiento del satélite *Sputnik*, en 1958 fue establecido la dependencia del DoD llamado *Defense Advanced Research Projects Agency* (DARPA) [114].

Dentro de los proyectos ambiciosos que se consideraban en el DARPA, era la creación de un sistema de comunicación a distancia que fuera capaz de ser usado en caso que un ataque nuclear destruyera los sistemas de comunicación comunes, sin ser intervenido o vulnerado, dicho sistema de comunicación sería conocido como ARPANET (*Advanced Research Projects Agency Network*), una red de computadoras interconectadas creada a petición del DoD. A pesar que ARPANET fue creada con la intención de crear una comunicación directa más segura, comenzó en cuatro universidades de Estados Unidos y no sería mucho el tiempo antes que se viera en dicha red un uso militar bastante eficiente.

[114] Cambió en el 1972 de ARPA a DARPA ya que se incluye como un programa de Defensa.

Desde este momento, se hace notar la necesidad de Estados Unidos de crear sistemas de comunicación directos que no puedan ser intervenidos o interferidos, situación que se mantendría con la creación de internet y la expansión de el gobierno estadounidense en el ciberespacio, como parte de la expansión del complejo de seguridad al ciberespacio.

Para 1980, el avance tecnológico se hacía notar, sin embargo, para marcar un momento impactante para los gobiernos fue durante el primer conflicto en el ciberespacio, que después sería denominado "Ciberguerra", se da en 1999, durante la Guerra de Kosovo, conflicto en el cual un grupo de *hackers*[115] se infiltró en tres sistemas distintos de seguridad e inteligencia de guerra: el equipo estratégico de la OTAN, de la Casa Blanca y del portaaviones Nimitz de Estados Unidos.

Posteriormente, en el año 2000 se han suscitado otras cinco ciberguerras en las cuales se han visto involucrados los tres Estados con mayor incidencia en el ámbito de los ciberataques y la ciberseguridad en el mundo, ya sea como víctima o victimario, y que son Estados Unidos, China y Rusia.

La dependencia de las infraestructuras críticas de los Estados Unidos en el Internet y los sistemas de datos del ciberespacio es tal, que el DoD es el indicado para defender Estados Unidos y sus intereses de cualquier amenaza incluyendo aquellas provenientes del ciberespacio, conformando cuerpos de misiones y estrategias.

En el *Quadriennial Defense Review Report* 2010 (QDRR) del DoD se establece que hoy en día los ejércitos modernos no pueden operar sin sus redes

[115] En la actualidad existen distintas controversias acerca del término, sin embargo para efecto del presente trabajo se tomará en cuenta al "hacker" como una persona con amplios conocimientos en temas de informática y redes de información quien, a diferencia de un cracker que sólo viola sistemas de seguridad y pasar por los filtros de seguridad de un computador o red de comunicaciones; altera, controla o destruye el sistema de información desde una ubicación remota.

de comunicación y de información en un estado confiable y resilente, sin que se asegure el acceso al ciberespacio.[116]

El fortalecimiento y desarrollo de las fuerzas del DoD en el ciberespacio tiene razón de ser, en un primer lugar, hacer frente a las nuevas formas de ataque hacia la milicia estadounidense que se enfocan en el uso de recursos no tradicionales para dañar o entorpecer las actividades o funciones del poder militar de Estados Unidos; en un segundo lugar, para fortalecer las posturas de ciberdefensa y ciberdisuasión para aquellos que pretenden minar el desarrollo estadounidense. El DoD tiene tres cibermisiones: "defender las redes, sistemas e información del DoD; defender la patria y los intereses nacionales de cualquier ciberataque con relevantes consecuencias; y, apoyar a los planes operacionales y de contingencia".[117] Debido a que la violencia se ha traspasado a este medio, actores estatales y no-estatales buscan ejercer acciones hostiles a través del ciberespacio, a lo que podríamos referirnos como ciberataques o *cyberexploits*, en los que se aprovechan las vulnerabilidades de las víctimas para ocasionar algún daño o pérdida.

En concreto, los ciberataques consisten en "[aquellos] ataques armados con la aplicación de la tecnología"[118] que son ejemplo de la "incorporación del ciberespacio a distintas áreas del Derecho Internacional que evidencian el uso de la fuerza por medio de herramientas tecnológicas a través del ciberespacio"[119] de Estados y actores no-Estatales que buscan minar el progreso y supervivencia de un gobierno en específico.

---

[116] Department of Defense, *Quadrennial Review Report 2010*, DoD, Estados Unidos, Enero 29 de 2010, p.ix, Disponible en línea: http://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf Consultado: mayo de 2016

[117] The Secretary of Defense, *The DoD Cyber Strategy*, The Department of Defense, Abril 2015, Disponible en línea: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf Consultado: mayo de 2016

[118] Moran E. Alejandra, Servin C. Abraham A. y Alquicira G. Oscar, TIC (internet) y ciberterrorismo, seguridad prevención para ti, UNAM, numero 23, 5 marzo 2015: http://revista.seguridad.unam.mx/numero23/tic-internet-y-ciberterrorismo Consultado: mayo de 2016

[119] *Idem*

Para clasificar un ciberataque hay que ver su alcance, intensidad y la duración que tiene, sin embargo, ha habido serias discusiones sobre si un ciberataque es considerado un ataque armado, por lo que Carr Feffrey realizó una clasificación para identificar si un ciberataque califica como uno:

1. "El primer modelo es un instrumento basado en el enfoque, que comprueba si el daño casado por un nuevo método de ataque anteriormente podría haber sido logrado sólo con un ataque cinético.
2. El segundo es un enfoque basado en los efectos, a veces llamado enfoque basado en consecuencia, en la que la similitud del ataque a un ataque cinético es irrelevante y la atención se centra en el efecto general del ataque, estos tienen como víctima al Estado.
3. El tercero es un enfoque de responsabilidad estricta, en la que los ciberataques contra infraestructuras críticas son tratados automáticamente como ataques armados, debido a las graves consecuencias que pueden derivarse de la desactivación de los sistemas".[120]

Algunos de principales problemas que las ciberoperaciones enfrentan es la delgada línea entre un conflicto armado internacional y un ciberataque por el nivel del uso de la fuerza; el Derecho Humanitario Internacional señala que un conflicto armado es todo aquél en el que dos o más Estados utilizan las armas y causan algún daño.[121] Sin embargo, esta definición queda rebasada en el sentido que las ciberoperaciones no siempre utilizan armas convencionales para completar sus misiones pero que llegan a tener alcances catastróficos. Asimismo, el DoD realiza operaciones en conjunto con las demás dependencias gubernamentales y tienen la autorización requerida para desmantelar las instalaciones militares enemigas dentro de un conflicto para ayudar las operaciones del sector militar.

---

[120] Carr, Feffrey, *Inside Cyber Warfare*, United States of America, O'reilly Media, Inc, second edition. 2012, p.59

[121] Comité Internacional de la Cruz Roja, Cuál es la definición de "conflicto armado" según el derecho internacional humanitario?, Dictamen de Marzo de 2008, Disponible en línea: https://www.icrc.org/spa/assets/files/other/opinion-paper-armed-conflict-es.pdf Consultado: mayo de 2016

Respecto a lo anterior, el DoD identifica cinco metas principales para las misiones en el ciberespacio y que son las siguientes:

1. Construir y mantener fuerzas y capacidades listas para conducir operaciones en el ciberespacio;
2. Defender la red de información del DoD, asegurar los datos del DoD, y mitigar los riesgos de las misiones del DoD;
3. Estar preparados para defender la patria de los Estados Unidos y los intereses vitales de ciberataques destructivos o disruptivos de consecuencias considerables;
4. Construir y mantener ciber opciones viables y planear usar esas opciones para controlar el ascenso del conflicto y dar forma al ambiente del conflicto en todas sus etapas;
5. Construir y mantener alianzas internacionales robustas y asociaciones para disuadir amenazas en común e incrementar la estabilidad y seguridad internacional.

Para llevar a cabo estos objetivos el DoD establece Fuerzas de Misiones Cibernéticas (CMF) bajo el mando del *U.S. Cyber Command* (USCYBERCOM o CYBERCOM) en 2010, compuesto de las unidades cibernéticas defensivas y ofensivas para centralizar el mando de operación en el ciberespacio. Este nuevo comando fue establecido para sincronizar y coordinar los efectos de guerra cibernética en todo el entorno de seguridad global[122] y que funge como una estructura medular para el complejo de ciberdefensa.

El USCYBERCOM debe mantener el control centralizado de todos los esfuerzos de guerra cibernética del DoD y sincronizar sus esfuerzos a través de las células de coordinación integrados con cada Comando Combativo (CC). A su vez, debido a la creciente urgencia de un estado colectivo de defensa de ciberguerra permanente y en cualquier área, se hace una diferencia entre las

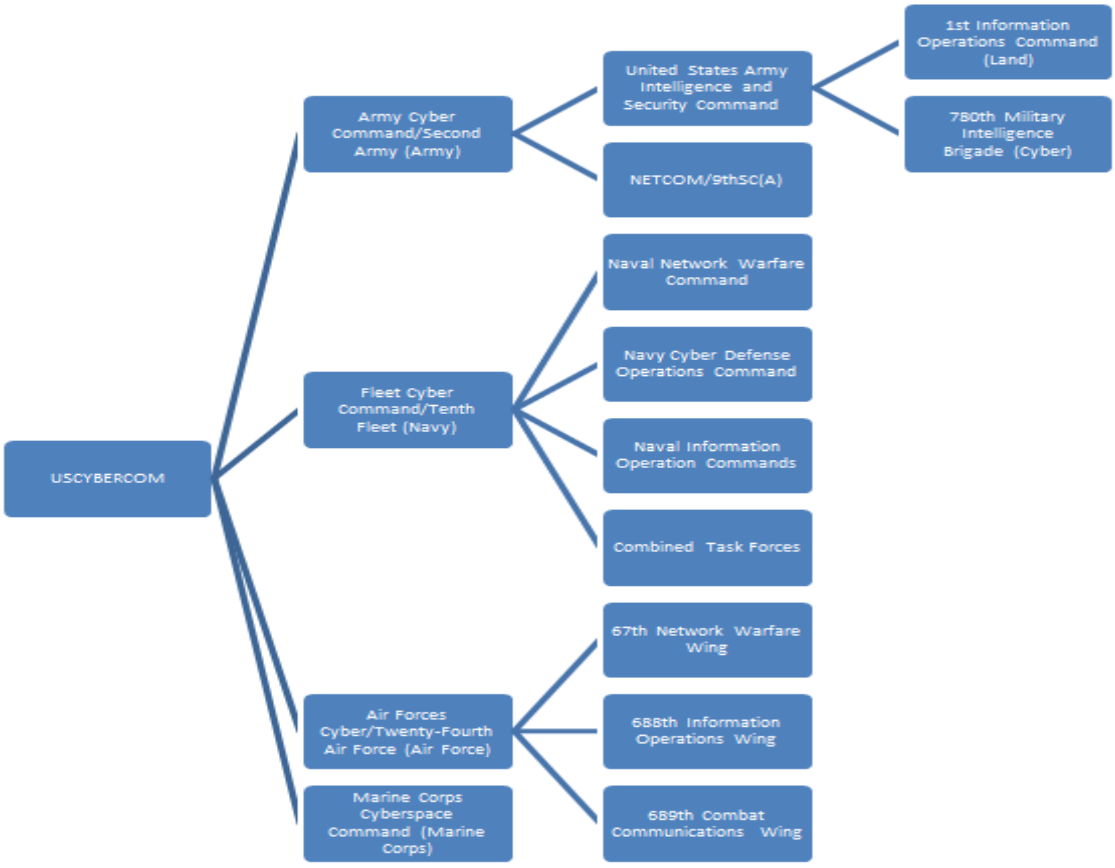
[122] *DoD Cyber Strategy*, op. cit.

unidades ofensivas es que están dirigidos típicamente dentro de un "área de responsabilidad" (AOR), de corta duración, y distinta en cada situación.[123]

Asimismo, la centralización del control y mando de todas las operaciones bélicas también tiene motivo de ser por las características fundamentales del ciberespacio, la falta de delimitación del ciberespacio dificulta la coordinación entre misiones y así se puede actuar con prontitud, efectividad y exactitud, a la vez que la concentración de esfuerzos hace más fuerte la defensa o la ofensa.

Para entender un poco más una de las partes más importantes de la estructura del complejo de ciberdefensa de Estados Unidos, el USCYBERCOM, ponemos a continuación el Esquema 3.

Esquema 3. Estructura del USCYBERCOM



[123] Stephen M. Rodriguez, *USCYBERCOM: A Centralized Command of Cyberspace*, Joint Military Operations Department and the Naval War College, Mayo 31 de 2011, archivo en PDF.

Fuente: INFOSEC, *China vs. US cyber superpowers compared*, http://resources.infosecinstitute.com/china-vs-us-cyber-superpowers-compared/

Su organización resulta un tanto sencilla, pero hay que recordar que USCYBERCOM actúa de manera dinámica, pragmática y muy completa[124]. Sin embargo, una de las recomendaciones que se le hacen a la administración y delimitación del USCYBERCOM, es que adquiera una autoridad similar a la de *U.S. Special Operations Command* (USSOCOM), ya que esto le daría la fortaleza de responder y ocuparse plenamente de los asuntos de ciberguerra puesto que el USCYBERCOM está subordinado al *U.S. Strategic Command* (STRATCOM).

Cabe destacar que el USCYBERCOM recopila todas las capacidades y esfuerzos de guerra en el ciberespacio. Por este motivo, es pertinente resaltar las capacidades indumentarias que el DoD posee para actuar dentro del ciberespacio, en resumen, este departamento:

> […] opera más de 15,000 redes informáticas diferentes a través de 4,000 instalaciones militares en todo el mundo. En un día cualquiera, hay hasta siete millones de computadoras del DoD y herramientas de telecomunicaciones de uso en 88 países que utilizan miles de aplicaciones bélicas y de apoyo. El número de vulnerabilidades potenciales, por lo tanto, es asombroso. Por otra parte, la velocidad de los ataques cibernéticos y el anonimato del ciberespacio favorecen en gran medida el delito. Esta ventaja está creciendo conforme las herramientas de hackers se vuelven más baratos y más fáciles emplear por los adversarios cuyas habilidades están creciendo en sofisticación".[125]

Aunque el USCYBERCOM esté ocupado de la defensa y ataque de Estados Unidos en el ciberespacio, hay que hacer un breve paréntesis para la dependencia más importante en términos del uso de las redes de información, y, el primero en encargarse en los asuntos del ciberespacio, la Fuerza Aérea (USAF).

Como consecuencia de la reducción de fuerzas por parte de Estados Unidos en Irak y Afganistán, y a la luz de los retos crecientes de adversarios estatales, el DoD redirige las inversiones hacia los sistemas que serán efectivos en el espacio aéreo y áreas denegadas. Ya que la capacidad de adaptación debe

[124]Hay que destacar que la composición del USCYBERCOM contiene a todas las unidades cibernéticas de los distintos cuerpos de guerra.
[125] *Quadrennial Review Report 2010*, op.cit. p.37

ser constante, de tal manera que permita a las demás estructuras del complejo operar de manera efectiva y fortalecer el poder nacional. Las capacidades de la USAF han ido en crecimiento gracias los recortes presupuestales para soldados y su reubicación en los Sistemas de Aeronaves No-tripuladas (UAS) como lo son el *Predator o el Reaper*[126], para fortalecer los mecanismos y operaciones de inteligencia, la vigilancia y el reconocimiento desde el 2010 a nuestros días. Este tipo de tecnologías de vanguardia son disputadas por todos los países y han sido (y serán) las que han facilitado el camino y éxito de las operaciones bélicas y de inteligencia como tal, ya que el costo que reduce en cualquier operación es proporcional al impacto que tiene en el resultado de ésta, de esta forma, es indispensable mencionar las capacidades de los UAS *Predator* y *Reaper* en la Tabla 2.

Tabla 2. Características de *Predator* y *Reaper*

Características	MQ-1B Predator	MQ-9 Reaper
Función principal	reconocimiento armado, vigilancia aérea, y la adquisición de blanco	encontrar, arreglar y terminar objetivos.
Contratista	General Atomics Aeronautical Systems Inc.	General Atomics Aeronautical Systems Inc.
Planta de energía	motor de cuatro cilindros Rotax 914F	motor turbohélice Honeywell TPE331-10GD
Empuje	115 caballos de fuerza	900 caballos de fuerza
Envergadura	55 pies (16,8 metros)	66 pies (20,1 metros)
Longitud	27 pies (8,22 metros)	36 pies (11 metros)
Altura	7 pies (2,1 metros)	12,5 pies (3,8 metros)
Peso	1.130 libras (512 kilogramos) vacío	4.900 libras (2.223 kilogramos) vacío
Peso máximo de despegue	2.250 libras (1.020 kilogramos)	10.500 libras (4.760 kilogramos)
Cap. de combustible	665 libras (100 galones)	4.000 libras (602 galones)
Carga útil (explosiva)	450 libras (204 kilogramos)	3.750 libras (1.701 kilogramos)
Velocidad	velocidad de crucero alrededor del 84 millas por hora (70 nudos), hasta 135 mph	la velocidad de crucero aproximadamente 230 millas por hora (200 nudos)
Rango	770 millas (675 millas náuticas)	1.150 millas (1.000 millas náuticas)
Techo	25.000 pies (7.620 metros)	Hasta 50.000 pies (15.240 metros)
Armamento	dos misiles AGM-114 Hellfire guiados por láser	combinación de misiles AGM-114 Hellfire, GBU-12 Paveway II y GBU-38 Municiones de Ataque Directo Conjunto
Sensores Visuales	integra un sensor de infrarrojos,	MTS-B: integra un sensor de

[126] Anteriormente nombrado Predator B

	cámara color/monocromo TV, cámara de televisión de imagen intensificada, láser buscador/designador e iluminador láser. El vídeo de movimiento completo de cada uno de los sensores de imagen puede ser visto en flujos de vídeo independientes o fusionados.	infrarrojos, cámara color/monocromo TV, cámara de televisión de imagen intensificada, láser buscador/designador e iluminador láser. El vídeo de movimiento completo de cada uno de los sensores de imagen puede ser visto en flujos de vídeo independientes o fusionados.
Tripulación (a distancia)	dos (piloto y operador de sensores)	dos (piloto y operador de sensores)
Costo Unitario	20 millones (incluye cuatro aviones con sensores, estación de control terrestre y Predator Primary satellite link) (FY 2009)	64,2 millones (Incluye cuatro aviones, sensores, GCS y Comm) (FY 2006)
Capacidad Op. Inicial	Marzo 2005	Octubre 2007
Inventario	150	93

Fuente: Elaboración propia, información de:
http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104470/mq-9-reaper.aspx

Al comparar estos dos tipos de drones, el *Reaper* es casi 4 ½ veces más pesado, el doble de rápido y con 8.4 veces más capacidad de carga explosiva que el *Predator*. Sin embargo, la capacidad del *Predator* radica en su capacidad de observar y vigilar gracias a sus imágenes aéreas en tiempo real, que han revolucionado la guerra, pero que en conjunto, ambas UAS van a continuar siendo un gran pilar del desarrollo tecnológico militar del departamento.

El DoD ha aclarado que la Fuerza Conjunta[127] estará preparada para luchar contra adversarios cada vez más sofisticados que podrían emplear las capacidades de combate avanzados y al mismo tiempo tratar de negarle a EE.UU. las ventajas que disfrutan actualmente en el espacio y el ciberespacio.[128] Por lo que no hay que excluir que este desarrollo tecnológico continúe y cada día tenga un mayor alcance para el complejo de seguridad que requiere Estados Unidos.

[127] Integrada por las dependencias del ejército, fuerzas aéreas y la armada, encargadas de: la defensa antimisiles, nuclear, cibernética, aire/tierra/mar y de apoyo a las autoridades civiles.
[128] Department of Defense, *Quadrennial Defense Review Report 2014*,Estados Unidos, p.vii Disponible en línea:http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf Consultado: mayo de 2016

Un aspecto importante es el tema de la Inteligencia, Vigilancia y Reconocimiento (ISR) que consiste en "información oportuna y precisa sobre situaciones operacionales y tácticos [ya que] es esencial para la consecución efectiva de cualquier misión militar".[129] En el que en resumidas palabras, el DoD:

> [va] a reequilibrar las inversiones hacia los sistemas que son de capacidad de respuesta operativa y eficaz en entornos altamente controvertidos /comprometidos, manteniendo al mismo tiempo las capacidades adecuadas para ambientes más permisivos con el fin de apoyar la conciencia global de la situación, la lucha contra el terrorismo, y otras operaciones".[130]

Es obvio que la obtención de información oportuna y precisa sobre situaciones operacionales y tácticos es esencial para la consecución efectiva de cualquier misión militar. Para esto, las fuerzas de Estados Unidos operan una amplia gama de sistemas para proporcionar tal información en tiempo de paz, crisis y conflictos por lo que se puede considerar como un estado permanente de alerta y de ISR.

En este sentido, el DoD se asegura de que los sistemas críticos basados en el ciberespacio sean más resistentes al ampliar el acceso a los sistemas espaciales de ISR comerciales y aliados. A medida que el departamento hace dichas inversiones, mantienen las capacidades adecuadas para ambientes más permisivos con el fin de apoyar la conciencia global, lucha contra el terrorismo, y otras operaciones. También el DoD se propone a ampliar el alcance de sus plataformas de ISR en el aire contra el terrorismo y continuamente dotándolas de nuevos y mejores sensores,[131] es así que los Estados Unidos continuarán sus inversiones en UAS para su aplicación en ISR. De tal manera, se puede observar que el rumbo que están tomando las inversiones del DoD para el futuro son en sistemas más sofisticados y que no requieren de tantos recursos humanos, pues el impacto que pueden tener se ven reflejado en el armamento que pueden cargar y el tipo de sensores y cámaras que posibilitan hasta la detección de matrículas o reconocimiento facial, y que en consecuencia, fortalecen el complejo de vigilancia.

---

[129] *Ídem*, p.38
[130] *Ídem*, p.xi
[131] Quadrennial Defense Review Report, op.cit. p.38

En el siguiente subcapítulo se hablará sobre los mecanismos y programas que el DHS posee e implementa para la ciberseguridad y vigilancia dentro y fuera de Estados Unidos como parte de este complejo de seguridad.

2.4 Complejo de ciberseguridad

La concepción del *Department of Homeland Security* (DHS) sobre el ciberespacio es que está integrado por sus diversos y complejos componentes, desde los sistemas operativos que lo conforman hasta los cibernautas. Cabe aclarar que la perspectiva del DHS es de ciberseguridad, por lo que ofrece varios documentos y reportes, generando sus estrategias y acciones que se convierten en un "monitoreo continuo" que serán ejecutadas por una de sus agencias dependientes, la *National Security Agency* (NSA) y que representa la culminación de las estructuras del complejo de vigilancia[132].

En resumen, el monitoreo consiste y está manejado por administradores que supervisan los sistemas informáticos encontrando vulnerabilidades y formulando reportes para su mejora y protección. Esto es considerado como un sistema "sano", que también requiere un grado de sofisticación debido al grado de complejidad que este sistema posee para ejecutar su control y protección; recordando lo planteado por el DoD en el subcapítulo anterior.

El DHS reconoce que en un Estado tan dependiente de las redes de la información, como Estados Unidos, es indispensable que existan alianzas entre departamentos y agencias para mantener la interoperabilidad e integridad compuestas de acuerdo a su noción de seguridad informática. Por lo que destacan tres conceptos que son interdependientes y construyen este ambiente cibernético "saludable", la automatización, la interoperabilidad y la autenticación.

La automatización es aplicada a dos partes de un sistema, la parte operativa, que es llevada a cabo directamente en la máquina para obtener la

[132] Que explicaremos con más detalle en el capítulo 3.

operación deseada, y la parte de mando, que se compone de un autómata programable. De este modo, la automatización puede "aumentar la velocidad de acción, optimizar la toma de decisiones, y la facilidad adopción de nuevas soluciones de seguridad. De esta manera será posible utilizar una estrategia de automatización de las defensas locales fijas, apoyados por las defensas móviles y globales en múltiples niveles".[133] Esto le permitiría al complejo de ciberseguridad resistir ataques y mantenerse operable.

La interoperabilidad consiste en ampliar la colaboración y cooperación, formando nueva información de inteligencia, compartiendo conocimiento y extenderlo. Sin embargo, este concepto tiene tres puntos de vista, semántico, técnico y político. En el sentido *semántico*, es "la capacidad de cada parte de enviar datos/información para comunicar y tener partes que reciban y entiendan el mensaje en el sentido pretendido por la parte que envía".[134] En el sentido técnico, es aquella capacidad de diferentes tecnologías para comunicarse e intercambiar datos sobre la bases bien definidas y estándares de interfaz ampliamente adoptados.[135] Y en el sentido *político*, son aquellos procesos comunes de negocio relacionadas con la transmisión, recepción y aceptación de los datos entre los *stakeholders*.

La autenticación, permite tomar decisiones confiables en línea; casi toda decisión tomada a distancia implica un riesgo, por lo que este proceso provee la seguridad necesaria al verificar que la identidad de los participantes/actores sea verdadera, de esta manera, se elimina el riesgo del uso inapropiado de la identidad de terceros y se protege la privacidad, a la vez que se le permite continuar con todas sus transacciones y operaciones a través de la red.[136] Uno de

---

[133] Department of Homeland Security, *Enabling Distributed Security in Cyberspace, DHS*, 23 de marzo de 2011, p. 2 Disponible en línea: https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf Consultado: mayo de 2016

[134] *Idem*. p. 3

[135] *Ibidem*

[136] A manera que las protecciones de autenticidad de los sistemas crecen, sus actividades expandidas a lo largo de la red, mail, blogs, perfiles de las redes sociales y recientemente, el comercio electrónico, se mantienen de manera segura y confiable para el usuario.

los principales objetivos de esta misión, es contrarrestar la sofisticación de los métodos de robo de identidad, ya que es progresiva y más agresiva con el paso del tiempo, por lo que el desarrollo de los recursos tecnológicos utilizados para éste tipo de crímenes afectan a los ciudadanos.

Sin embargo, la autenticación sería ideal si no solo incluyera los individuos sino también los aparatos cibernéticos, ya que también existe el mal uso de las direcciones IP[137] y que dificultan los análisis forenses en el ciberespacio. Hay que mencionar que esta misión también es fundamental para la defensa cibernética ya que las comunicaciones y la atribución del contenido son factores esenciales en las decisiones de seguridad, por lo que el DoD trabaja lado a lado en este aspecto con el DHS.

Asimismo, la autenticación de identidad figura entre los principales problemas para la construcción del complejo de ciberseguridad, ya que dentro del ciberespacio es posible actuar en anonimidad permitiendo a aquellos que planean cometer un ilícito estar protegidos, tal es el caso de la *Deep Web*.

La *Deep Web*[138] se compone de todos aquellos sitios que no se encuentran indexados[139] y de recursos de bases de datos que no son accesibles[140] mediante los metabuscadores,[141] a los que sólo se les puede accesar conociendo la dirección y utilizando protocolos o software específico para navegar en esta parte. De esta manera, la *Deep Web* representa una de las más grandes amenazas para cualquier mecanismo gubernamental de vigilancia y ciencias forenses en el ciberespacio, esto es a causa de varios factores que lo componen y que restringen el ingreso de cualquier usuario no familiarizado con el funcionamiento de este tipo

[137] Consiste en un número único e irrepetible, que identifica una interfaz de red conectada a un dispositivo.
[138] Lo contrario al internet superficial.
[139] Darle una categorización a una serie de datos o informaciones de acuerdo a un criterio común a todos ellos, para facilitar su consulta y análisis.
[140] Normalmente son indexados por *web crawlers* o arañas que capturan todos los enlaces menos aquellos que niegan el acceso o son innacesibles
[141] Como Google y Yahoo.

de recurso, puesto que al accesar a esta red lo que se busca es el anonimato y las personas que realizan actividades a través de este medio utilizan recursos sofisticados que evitan la identificación del autor por parte de las instancias gubernamentales de procuración de justicia y vigilancia.

Existe una parte de la *Deep Web* llamada *Dark Web*, que es toda aquella red de bienes y servicios ilícitos que se mantienen en compra-venta dentro de este oscuro tejido del crimen organizado que opera de una manera eficiente y anónima, en el que se pueden contratar mercenarios, vender/comprar drogas, obtener pornografía infantil, arte robada, entre otros bienes digitales y físicos que llegan a ser inimaginables y grotescos. Uno de los casos más conocidos por la ciudadanía estadounidense es *Silk Road*, cuyo creador Ross Ulbricht, obtuvo cadena perpetua por haber creado esta página de circulación de narcóticos internacional.[142] Sin embargo, hay que destacar que surgen dudas sobre la manera en que obtuvieron las pruebas que vinculaban a Ross Ulbricht con su actividad anónima a través de la *Deep Web*, lo cual da índices de haber sido obtenidas con ilegalidad a través de la NSA o el propio FBI y que recaería en una inconstitucionalidad; por lo que se alegó durante el juicio que se violó su derecho establecido en la Cuarta Enmienda.[143]

Asimismo, hay que resaltar que la sentencia de Ulbricht suena un tanto exagerada en comparación con las penas que obtienen los mismísimos líderes de crimen organizado, se entiende, dentro de la comunidad cibernética, que este tipo de penas son para dar un ejemplo a todos aquellos que se atreven a utilizar los medios anónimos y privados y disuadirlos. Por lo que el tema sobre la *Deep Web*

[142] Sam Thielman, Silk Road Operator Ross Ulbricht Sentenced to Life in Prison, The Guardian, Nueva York, Estados Unidos, 29 de mayo de 2015, Disponible en línea: https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced Consultado: mayo de 2016

[143] Kate Vinton, Alleged Silk Road Creator Ross Ulbricht Fourth Amendment Rights Were Violated, Lawyers Say, Forbes, 4 de agosto de 2014, Disponible en línea: http://www.forbes.com/sites/katevinton/2014/08/04/alleged-silk-road-creator-ross-ulbrichts-fourth-amendment-rights-were-violated-lawyers-say/#6af0036d11a5 Consultado: mayo de 2016

es que es una amenaza común para todas las divisiones de ciberseguridad y las agencias encargadas a la persecución del crimen como el FBI.

Sin duda, las acciones bajo el anonimato no son el único problema existente para la ciberseguridad y ciberdefensa, existen múltiples y diversas amenazas provenientes del ciberespacio y que son recopiladas específicamente por el *National Vulnerability Database* (NVD) y que apoyan la construcción de lineamientos y operaciones a través del ciberespacio.

En esta parte, la dependencia responsable de analizar y reducir las amenazas informáticas, las vulnerabilidades, la difusión de información de alerta de amenazas cibernéticas, y la coordinación de las actividades de respuesta a incidentes, es el *United States Computer Emergency Readiness Team* (US-CERT). El US-CERT es una rama de la *Office of Cybersecurity and Communications* (CS&C) y *National Cybersecurity and Communications Integration Center* (NCCIC), ambas dependencias del DHS. Esta división tiene tecnologías de red muy avanzadas y medios digitales en materia de análisis para influir en las actividades maliciosas que atacan a las redes dentro de los Estados Unidos y en el extranjero[144] que garanticen una pronta alerta de amenaza[145], un ejemplo de esto es el programa EINSTEIN[146].

Por su parte, el programa EINSTEIN 2 es de un espectro mucho más amplio que su predecesor, y ha generado controversias por violaciones a la privacidad, asimismo, posee un sistema avanzado que genera alertas de intrusión al momento y esto permite la acción inmediata de los equipos de seguridad. Éste programa tiene permitido compartir la información obtenida con agencias

[144] Departmento of Homeland Security, *US-CERT Infosheet*, DHS Cybersecurity, septiembre de 2013, Disponible en línea en: https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf Consultado: mayo de 2016

[145] Proceso automatizado para recopilar, correlacionar, analizar, y compartir información de seguridad de la información en todo el gobierno federal para mejorar el conocimiento de la situación cibernética del país.

[146] Fue originalmente un sistema de detección de intrusos que monitorea las pasarelas de red de los departamentos y agencias del gobierno de los Estados Unidos para el tráfico no autorizado, sin embargo este programa avanzó y hoy en día es mucho más que eso.

ejecutivas federales de acuerdo con "procedimientos operativos estándar" y solamente "en una forma resumida".[147] Por lo que EINSTEIN 2 le permite al US-CERT correlacionar la actividad en toda la federación.

El US-CERT tiene como responsabilidad notificar a las fuerzas de la aplicación de la ley o las entidades de inteligencia sobre un evento y les proporcionará la información de contacto para que puedan coordinarse directamente con la agencia federal afectada. De esta manera, la dependencia no se centra en las identidades de los individuos específicos, los datos obtenidos de los proveedores de datos estará limitada a la información relevante para la protección de las redes informáticas,[148] por lo que éste mecanismo funciona dentro del complejo de vigilancia de manera en que monitorea las actividades maliciosas y su proveniencia.

En este sentido, bajo la visión simple de la protección de los individuos y las libertades civiles, el DHS tiene una percepción del “deber ser” del internet que se necesita para lograr un ecosistema cibernético saludable y según esto es que debe de poseer las siguientes características:

- Inclusivo: capacidades que se incrusten en una red cada vez más amplia más allá de las nociones tradicionales, en donde se incorporen la red inteligente (Smart grid)[149], la próxima generación del Sistema Nacional del Espacio Aéreo, que aprovecha las capacidades de satélite, el gran número de dispositivos heredados y los sistemas de control que deben interoperar con las nuevas tecnologías.
- Efectivo: que sea capaz de defenderse contra todo tipo de amenazas informáticas, incluyendo ataques de la cadena de suministro; ataques remotos o basados en la red, incluidos los lanzados por los atacantes sofisticados y con buenos recursos que utilizan métodos persistentes; ataques inmediatos o físicos o eventos adversos; y la información privilegiada o de los ataques de los empleados descontentos.

[147] US-CERT EINSTEIN 2, *Privacy Impact Assessment*, DHS, 19 de mayo de 2008, Disponible en línea: https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf Consultado: mayo de 2016

[148] *Ibidem*. p.12

[149] Al igual que Internet, la red inteligente consiste en controles, computadoras, la aplicación de la automatización y nuevas tecnologías y equipos que trabajan conjuntamente, pero en este caso, estas tecnologías trabajarán con la red eléctrica para responder digitalmente a nuestro rápidamente cambiante de demanda eléctrica, salvar energía, trabajar eficientemente y ofrecer una mejora en la seguridad.

- Inteligente: capaz de percibir el entorno, reconocer patrones, y compartir información en tiempo casi real en todos los sectores y comunidades, tanto a nivel humano y máquina con el fin de asegurar las transacciones autorizadas, prevenir las violaciones de seguridad más graves y aumentar la eficacia de la respuesta al incumplimiento u otros eventos adversos que se produzcan.
- Sin barreras: que tenga opciones de seguridad instanciadas en las políticas digitales configurables en lugar de ser "hardwired" [150] (integrado) en la red o diseños del sistema o impuestas por las limitaciones tecnológicas o los déficit. Los diseñadores diseñarían con la suposición de que todo va a ser compartido con todo el mundo, y las únicas barreras a la colaboración sería las impuestas por la política.
- Optimizado: que tienen las capacidades y la toma de decisiones repartida entre humanos y máquinas con el fin de aprovechar mejor los puntos fuertes y los tiempos de ciclo de cada uno, en consonancia con el mantenimiento de la agilidad. Además, después de tener una ciberdefensa organizada de tal manera que las máquinas se defiendan contra las máquinas y las personas se defiendan contra las personas.
- Comprensible: tener la seguridad expresada en términos de usuarios o grupos de interés en lugar de en la "jerga" de seguridad especializada y reconociendo que todos estamos interesados en la ciberseguridad. Por ejemplo, las partes interesadas podrían querer visibilidad global en el medio cibernético, la capacidad de consultarlo y tener la capacidad de racionalizar los costos de seguridad.
- Asegurado: capaz de mantener la confianza del consumidor en el tiempo. Esto podría significar ir más allá de las nociones tradicionales de seguridad de "prevenir transacciones no deseadas" para "garantizar que ocurran las transacciones correctas", lo que podría contribuir de manera más amplia a una sensación de seguridad de los consumidores y la confianza en las operaciones del sector para el transporte, la energía, la salud, etc.
- Usable: que tiene propiedades de montaje, configuración, funcionamiento y rendimiento que son directos y sencillos y comportándose adecuadamente, en lugar de forma complicada y abrumadora, frágil y propenso a errores.[151]

Sin embargo, podemos observar que todas éstas características no tienen un impacto directo en la seguridad de los individuos, sino busca en un primer momento la protección de los sistemas gubernamentales y la defensa del gobierno frente a cualquier amenaza, asimismo, delimita o amplia las capacidades que este complejo de ciberseguridad posee o desea poseer.

El DHS no sólo se da a la tarea de detectar las amenazas cibernéticas en el exterior o el interior, sino también es el encargado del manejo de la seguridad de la información y las comunicaciones durante un desastre, por lo que existe el Plan

[150] Que reúne en una sola pieza otros aparatos que podrían existir independientemente
[151] *Enabling Distributed Security in Cyberspace, DHS*, op.cit. p.23

Nacional de Comunicaciones de Emergencia (NECP), el cual funciona como primer plan estratégico de Estados Unidos para la orientación de comunicaciones de emergencia en situación de desastre. El NECP para el 2013 cubre el 75% de todas las jurisdicciones, demostrando que es capaz de dar un nivel de respuesta dentro de tres horas con todas las comunicaciones de emergencia.

También, el DHS busca lograr un ecosistema sano equilibrado, en donde las amenazas se ven percibidas en términos del usuario promedio y no en términos belicistas o predominantemente estatales, como es el caso del DoD y como es visto por la NSA, aunque hay que aclarar que a pesar de que esta sea su visión, no deja de apoyar a estos dos cuerpos gubernamentales. No obstante, cabe destacar que el órgano más fuerte en términos cibernéticos del DHS, es el US-CERT, el cual no posee ninguna facultad de perseguir crímenes ni tener información de inteligencia o generarla, el análisis va en un aspecto mucho más de impacto y vulnerabilidades, y que se trató de modificar al crear el programa EINSTEIN 3 en el 2013, ya que analiza datos no sólo de las páginas gubernamentales sino también de las privadas;[152] y que ha generado un poco de reticencia entre los funcionarios del DHS sobre la violación de los derechos de la privacidad de los individuos y la "Incertidumbre acerca de si los datos privados pueden quedar excluidas de un examen no autorizado",[153] también hay dudas respecto a la elección de los blancos o amenazas, ya que cualquier individuo que frecuente mucho las páginas gubernamentales puede ser considerado como una amenaza.

Este tipo de programas es una prueba de que Obama intenta continuar con las operaciones llevadas a cabo en la era de Bush, usando la asistencia de las agencias de seguridad e inteligencia en la detección de tráfico de información, de

[152] Department of Homeland Security, "Privacy Impact Assessment for EINSTEIN 3 Accelerated (E3A)", U.S. Department of Homeland Security, 19 de abril de 2013, Disponible en línea: https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf Consultado: mayo de 2016

[153] Ellen Nakashima, *DHS Cybersecurity Plan Will Involve NSA, Telecoms*, The Washington Post, 3 de julio de 2009 Disponible en línea: http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771.html Consultado: mayo de 2016

computadoras del gobierno y dentro de las redes del sector privado. A pesar de lo mucho que el DHS se apegue a la seguridad humana esto no se vislumbra en sus políticas y estrategias, ya que el discurso puede ser en relación a la protección de los ciudadanos, pero en la operación, este departamento funciona como un mecanismo más del complejo de seguridad y que ha demostrado apoyar operaciones de vigilancia dirigidas por la NSA, la agencia que posee papel más emblemático del complejo de vigilancia de Estados Unidos.

3. CRISIS DEL COMPLEJO DE VIGILANCIA

La *National Security Agency* como agencia encargada de la recopilación de inteligencia extranjera, es el ejemplo más emblemático de esta estructura del complejo de vigilancia. Sus mecanismos y herramientas poseen un alcance global, efectivo y resiliente que demuestran el poder nacional estadounidense a través de los distintos medios de comunicación y en específico, el ciberespacio.

Las capacidades de vigilar de este país son de una dimensión extraordinaria gracias a la recurrente inversión económica en nuevas y creativas tecnologías que tienen como fin el completar el complejo de seguridad de la nación aportando información estratégica o de inteligencia a las distintas dependencias del gobierno, sin embargo, todo gobierno está compuesto por personas que poseen los valores estadounidenses de los derechos civiles y la democracia, pero cuando éstos últimos no son respetados conforme a la ley, los funcionarios, en papel de ciudadanos, divulgan los errores y la falta de ética ejercida dentro de la institución convirtiéndose así en un *whistle-blower*.

Éste tipo de filtraciones o divulgaciones, encuentran su refugio en una plataforma con servidor en Islandia llamada Wikileaks, cuyo propósito es el de funcionar como una prensa pública sin censura. Mientras muchos *whistle-blowers* han sido privados de su libertad, el nombre Edward J. Snowden representa el acto heroico realizado por éstos y exhibe los mecanismos de vigilancia usados por el gobierno de Estados Unidos para asegurar su poder en el globo terráqueo.

3.1 La NSA y los mecanismos de vigilancia masiva.

El mecanismo más representativo del complejo de vigilancia del periodo de Barack Obama es la *National Security Agency* (NSA). Es una dependencia del *Department of Defense* que se creó el 4 de noviembre de 1952, por orden del presidente Harry Truman, y ésta decisión se produjo tras el importante trabajo de Estados Unidos al romper los códigos alemanes y japoneses durante la Segunda

Guerra Mundial, lo que contribuyó al éxito aliado en el Atlántico Norte y la victoria en la batalla de Midway en el Pacífico entre otras aportaciones. Asimismo, este proyecto de crear la NSA era la mejor manera de continuar con los desciframientos de códigos en la post-guerra.[154]

Otro suceso histórico muy importante para la agencia es la orden ejecutiva 12333 bajo la era de Reagan, esto le ha permitido a la NSA barrer de forma encubierta vastas cantidades de datos privados de redes de comunicación en el extranjero sin la supervisión judicial,[155] que sería reutilizada en el programa *Stellarwind* usado en el gobierno de George W. Bush.

Ésta orden, apuntala un motor de búsqueda secreta de la NSA construido para compartir más de 850 mil millones de registros de llamadas telefónicas, correos electrónicos, sitios de teléfonos celulares, y chats de internet con otras agencias del gobierno de Estados Unidos, incluyendo la policía. El sistema de búsqueda, llamado ICREACH, contiene información sobre las comunicaciones privadas de los extranjeros, así como, al parecer, millones de estadounidenses que no estén acusados de cualquier delito.[156]

Es así que para el desciframiento de códigos -o comunicaciones- en la post-guerra, una directiva presidencial estableció el Servicio Central de Seguridad (CSS) en 1972, que trabaja en conjunto con la NSA y está compuesto por elementos de las fuerzas armadas, el Ejército, la Armada, las Fuerzas Aéreas, la Infantería de Marina y la Guardia Costera. El director de la NSA también sirve como el Jefe del Servicio Central de Seguridad, lo que permite un esfuerzo unificado en criptología. Los miembros de la del CSS trabajan lado a lado con el personal de la NSA en diversos lugares del mundo, para garantizar un apoyo

[154] National Security Agency, *About NSA FAQS,* NSA/CSS, 3 de mayo de 2016, Disponible en línea: https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml Consultado: mayo 2016
[155] Ryan Gallagher, Obama faces calls to reform Reagan-era Mass Surveillance Order, The Intercept, 2 de septiembre de 2014, Disponible en línea: https://theintercept.com/2014/09/02/obama-12333-surveillance-nsa-rights-groups-letter/ Consultado: junio 2016
[156] *Idem.*

consistente a los líderes, políticos y tomadores de decisiones, ya sea militar o civil, desde las misiones de guerra hasta la Casa Blanca.

De esta manera se puede vislumbrar que la creación de la NSA tiene que ver con el irrumpimiento de las comunicaciones estratégicas enemigas, siendo así que la obtención de la información a través de las infraestructuras de las comunicaciones fungen como objetivo principal de las operaciones de la agencia desde sus principios.

Dicho esto, podemos aseverar que los métodos usados por la institución, son acorde a un complejo de vigilancia que utiliza diversos medios de las TIC, electrónicos principalmente, con fines estratégicos y de inteligencia.

En este sentido, es indispensable mencionar que las dos misiones principales que tiene la agencia con su país son: "prevenir que adversarios extranjeros adquieran acceso a información sensible o clasificada vinculada con la seguridad nacional",[157] además de "recolectar, procesar y diseminar información de inteligencia de fuentes externas para propósitos de inteligencia y contrainteligencia y para respaldar operaciones militares".[158]

De este modo, la NSA maneja dos operaciones interconectadas, en un primer momento están las conocidas *Signals Intelligence* (SIGINT),[159] aquella recopilación de información estratégica o de inteligencia de los adversarios, consta del desciframiento de códigos y de encriptados, por lo que este tipo de actividad requiere de grupos de criptoanalistas con un alto grado de especialización en el tema.

---

[157] BBC Mundo, La NSA, la agencia de espionaje más secreta de Estados Unidos, 10 de junio de 2013, Disponible en línea:http://www.bbc.com/mundo/noticias/2013/06/130610_internacional_ee_uu_national_security_agency_perfil_nc Consultado: junio 2016

[158] *Idem.*

[159] *About NSA FAQS,* op.cit

La segunda operación de la NSA, es el *Information Assurance* (IA),[160] es la estrategia de contrainteligencia, se busca que el proceso que se utiliza para la misión de SIGINT no sea aplicada a las comunicaciones e información estadounidense, en este sentido la IA sirve para defender los intereses de Estados Unidos en contra de aquellos países que desean realizar algún daño; por ende, la seguridad de la información y de los sistemas de información son de vital importancia en un siglo con múltiples escenarios de conflicto. Por lo que se puede observar que ambas se complementan y retroalimentan.

La NSA tiene la encomienda de tener una meta superior al cumplir con estas dos misiones anteriormente mencionadas, apoyar en el ámbito militar, permitiendo y protegiendo la Red de Guerra (Network Warfare). Puesto que hay que resaltar que los MSC se complementan para crear este CSC que Estados Unidos necesita construir para proyectarse al exterior como una superpotencia.

En este sentido, NSA dentro de todo el gobierno de Estados Unidos lidera los esfuerzos y actividades en criptología, abarcando tanto las operaciones SIGINT y los productos y servicios del IA, a la vez permite a la *Computer Network Operations* (CNO) con el fin de obtener una ventaja de decisión para el país y sus aliados en todas las circunstancias. En cuanto a las misiones difíciles de lograr (objetivos difíciles de espiar) están las *Tailored Access Operations* (TAO), en las que se estudian a funcionarios de alto nivel o personas en específico, como la operación *White tamale* en la que se espió al presidente de México, Enrique Peña Nieto.[161]

Asimismo, esta agencia identifica que hoy en día la guerra y las relaciones internacionales e interpersonales han escalado a un nivel digital, donde la información estratégica pasa a un nivel de bien nacional, pues las amenazas

---

[160] *Ídem.*

[161] Jens Glüsing, Laura Poitras, Marcel Rosenbach y Holger Stark, *Fresh Leak on US Spying: NSA Accessed Mexican President's Email*, Der Spiegel, 20 de octubre de 2013, Disponible en línea: http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html Consultado: mayo 2016

provienen de un ambiente prolífico, evolutivo y de bajo costo para causar daños y robar la propia información. En este sentido, el robo de la propiedad intelectual es de las amenazas cibernéticas contra las que lucha la agencia, al mismo tiempo lucha en contra de aquellos actores que detentan en contra de los recursos de información del gobierno de los Estados Unidos, por lo que uno de los principales objetivos de la NSA será mantener conocimiento sobre el flujo de la información lo que refuerza el complejo de vigilancia con un alcance global.

De esta misma forma, la NSA sugiere que la estrategia que las empresas estadounidenses deben adoptar es una agresiva,[162] en la que las empresas entiendan que la inversión en la seguridad cibernética puede ser mucho más adquisitiva y sostenible que remendar los daños. Pero que dichas iniciativas provengan de un "gobierno aumentado"[163] construido mediante asociaciones comerciales y programas encaminados al aseguramiento de la información, vigilancia y resguarde las redes y las actividades en ellas.

Lo que preocupa es hasta dónde se deben aumentar las capacidades del gobierno con estos fines, ya que esto puede incitar a generar un gobierno fisgón que vigila o supervisa las actividades sin el respeto de la privacidad y libertad, respecto a ésto último la propia página oficial de la NSA se declara que todas sus actividades van de acuerdo a la Constitución, y en lo que respecta a los derechos de privacidad, se cumplen con el mayor cuidado.

Sin embargo, podemos encontrar muchos casos en lo que esto no siempre es cumplido o su cumplimiento no es en términos de la ley como las violaciones de asociaciones de la NSA con una de las muchas compañías de telecomunicaciones como fue el caso AT&T.[164]

---

[162] NSA/CSS, *What We Do: Cyber,* NSA/CSS, 3 de mayo de 2016 Disponible en línea: https://www.nsa.gov/what-we-do/cyber/ Consultado: mayo 2016

[163] *Ídem.*

[164] Julia Angwin, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras y James Risen, *AT&T Helped US Spy on Internet On A Vast Scale*, The New York Times, 15 de agosto de 2015,

A lo largo de toda la federación estadounidense, la Comunidad de Inteligencia tiene como obligatorio respetar las libertades civiles y la privacidad durante sus actividades para resguardar la seguridad nacional. Ante esto, la NSA ha realizado grandes esfuerzos por cumplir con los pronunciamientos de Obama respecto a una NSA más transparente y confiable para la ciudadanía, haciendo los resultados y los procedimientos de las operaciones un poco más claras para el público en general.[165]

Cabe destacar, que aunque hay un compromiso público, este tipo de misiones no pueden parar debido al beneficio de la obtención de información de inteligencia por parte de las distintas operaciones de vigilancia ejercida por la NSA, además algo que hay que rescatar, es que para Estados Unidos es tradición recolectar información estratégica de los demás Estados. Es decir, las operaciones de espionaje e inteligencia (a la par, de contrainteligencia) tienen sus comienzos desde la creación de la Nación norteamericana con George Washington padre de la Patria.[166] Por lo que es de esperarse, que con el creciente flujo de información y su disponibilidad, a pesar de su censura a los reporteros y la libertad de expresión[167] establecidos en la Primera Enmienda de la Constitución.

Sin embargo, la construcción de un complejo de vigilancia requiere de un respaldo legal, en este sentido, hay ciertas leyes que utiliza la NSA para sus actividades de vigilancia e inteligencia, como la ley FISA aprobada en el año 1978 que básicamente fija los procedimientos de vigilancia física y electrónica y la recolección de información de inteligencia extranjera.

Disponible en línea: http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0 Consultado: mayo 2016

[165] Abby D, Phillip, *President Obama: NSA Spying Programs "Transparent"*, 17 de junio de 2013, Disponible en línea: http://abcnews.go.com/blogs/politics/2013/06/president-obama-nsa-spying-programs-transparent/ Consultado: mayo 2016

[166] Central Intelligence Agency, *History of American Intelligence*, Kids Zone, 23 de marzo de 2013, Disponible en línea: https://www.cia.gov/kids-page/6-12th-grade/operation-history/history-of-american-intelligence.html Consultado: mayo 2016

[167] Reporters Without Borders, *Enemies of the Internet 2014: Entities at the heart of censorship and surveillance*, Reporters Without Borders, Paris, 11 de marzo de 2014.

Inicialmente, FISA estaba dirigida únicamente a la vigilancia electrónica, pero ha sido modificada de forma sustancial para la utilización de registros de llamadas y dispositivos de trampa y rastreo (*trap and trace*),[168] registros físicos, y los registros comerciales.

Para entender el principal objetivo de esta ley hay que entender el concepto de inteligencia extranjera que en términos de la ley significa:

1. La información que se relaciona con, y si involucra una persona ciudadana de Estados Unidos, la capacidad de Estados Unidos de protegerse contra[169]:
    a. Un ataque real o potencial u otros actos hostiles graves de una potencia extranjera o un agente de una potencia extranjera;
    b. el sabotaje, el terrorismo internacional, la proliferación internacional de las armas de destrucción masiva por una potencia extranjera o un agente de una potencia extranjera; o
    c. las actividades clandestinas de inteligencia por un servicio de inteligencia extranjera o de la red de una potencia extranjera o por un agente de una potencia extranjera;
2. La información con respecto a una potencia extranjera o territorio extranjero que se relaciona con, y si involucra con una persona ciudadana de Estados Unidos, necesaria para;
    a. la defensa nacional o la seguridad nacional de los Estados Unidos; o
    b. la conducta de las relaciones exteriores de los Estados Unidos.[170]

[168] El término "trampa y rastreo" se refiere a un dispositivo o proceso que captura los impulsos electrónicos o de otro tipo entrantes, que identifican el número de origen u otra marcación, enrutamiento, direccionamiento, e información razonablemente probable para identificar la fuente de un cable o comunicación electrónica, no obstante, dicha información no incluirá el contenido de la comunicación. La diferencia con los “registros de pluma (pen register)” es un dispositivo electrónico que registra todos los números de llamada de una línea de teléfono en particular. El término ha llegado a incluir cualquier dispositivo o programa que realiza funciones similares a un registro original de “pluma”, incluyendo los programas monitoreando las comunicaciones por Internet.

[169] Este inciso es utilizado para la creación del programa PRISM, el cual es mencionado más adelante

Podemos darnos cuenta de que la ley busca obtener y prevenir cualquier asunto de defensa nacional o seguridad nacional mediante la vigilancia de cualquier persona sospechosa de actividades como el tráfico de armas de destrucción masiva, el terrorismo, el espionaje, el sabotaje o la conspiración.

Lo anterior se basa únicamente al tipo de información que desean obtener, sin embargo, los métodos de búsqueda son el factor elemental que debemos tomar en cuenta. Uno de ellos, y el más recurrido por la NSA, es la vigilancia electrónica, y por vigilancia electrónica podemos entender que es:

1. La adquisición por parte de un dispositivo electrónico, mecánico, u otro aparato de vigilancia de contenidos de cualquier comunicación por cable o radio enviadas por o destinadas a ser recibidas por un conocido persona en particular de los Estados Unidos, que está en los Estados Unidos, bajo circunstancias en las que una persona tiene una expectativa razonable de su privacidad, se requerirá una orden judicial para hacer cumplir la ley;
2. La adquisición por parte de un dispositivo electrónico, mecánico, u otro aparato de vigilancia de contenidos de cualquier comunicación por cable para o de una persona en los Estados Unidos, sin el consentimiento de cualquiera de las partes, si su adquisición se produce en los Estados Unidos, pero no incluye la adquisición de aquellas comunicaciones de los intrusos informáticos, que sería permisible solamente bajo la sección 2511 (2) (i) del título 18;[171]
3. La adquisición intencional por parte de un dispositivo electrónico, mecánico, u otro dispositivo de vigilancia, de contenidos de cualquier comunicación

[170]University of Cornell, *50 U. S. Code 1801 Definitions*, Cornell Law University, Disponible en línea: https://www.law.cornell.edu/uscode/text/50/1801 Consultado:abril 2016

[171]No será ilegal en virtud de este capítulo para un operador de un tablero de conmutadores, o un funcionario, empleado o agente de un proveedor de cable o servicio de comunicación electrónica, cuyas instalaciones se utilizan en la transmisión de un cable o comunicación electrónica, para interceptar, revelar, o usar dicha comunicación en el curso normal de su trabajo en el ejercicio de cualquier actividad ya que es un incidente necesario para la entrega de su servicio o para la protección de los derechos o la propiedad del prestador de dicho servicio, excepto que sea un proveedor de servicio de comunicaciones por cable al público no se deberá utilizar el servicio de observación o monitoreo al azar a excepción de los controles de calidad mecánicos o de servicios.

por radio, en circunstancias en las que una persona tiene una expectativa razonable de privacidad y se requiere una orden judicial para hacer cumplir la ley, y si ambos, el remitente y todos los destinatarios se encuentran dentro de los Estados Unidos; o

4. La instalación o el uso de un dispositivo electrónico, mecánico, o de otro tipo de vigilancia en los Estados Unidos para el seguimiento con el fin de adquirir información, aparte de una comunicación por cable o radio, bajo circunstancias en las que una persona tiene una expectativa razonable de privacidad y se requerirá orden judicial para el cumplimiento de la ley.[172]

Se puede observar que en todo momento se hace explícita la delimitación geográfica a únicamente dentro del territorio estadounidense. El contexto en el que se aprobó la Ley FISA el Congreso pretendía proporcionar una supervisión judicial y del Congreso en las actividades de inteligencia y vigilancia extranjera a la vez que se mantenía el nivel de secrecía necesario para supervisión efectiva de las amenazas a la Seguridad Nacional.

Esta ley establecía su propia corte, la Corte de Vigilancia de Inteligencia Extranjera de los Estados Unidos (FISC), la cual sesiona en privado y únicamente con miembros del gobierno. Una vez mencionado esto cabría poner en duda sobre qué tanta discusión se tiene dentro de la FISC respecto a los programas de vigilancia. También sobre la manera en cómo se encubren ciertas actividades bajo errores tal cual dice el inciso 1806 de FISA, en el que en caso de que:

> […] el gobierno haya accidentalmente interrumpido comunicaciones de un individuo y sus receptores dentro de Estados Unidos y que éste desee conservar sus expectativas de privacidad y se requiera una orden judicial, está obligado a eliminar los registros a menos que el Abogado General demuestre que dichos registros deben mantenerse por el resguardo de vidas inocentes.[173]

FISA provee de un año de análisis y conservación de la información para demostrar que hay algún peligro de amenaza o para levantar una orden de

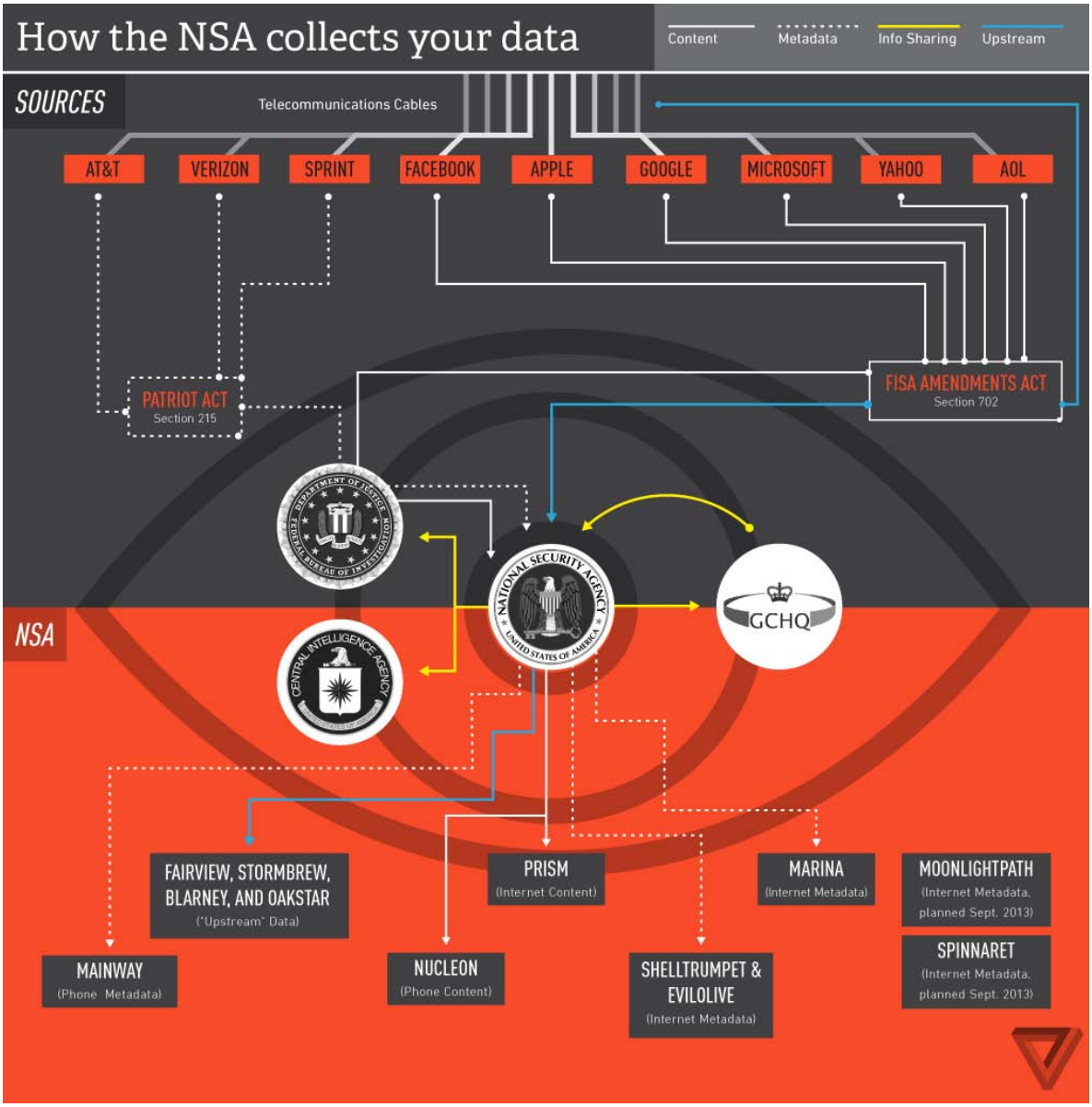
[172] *50 U. S. Code Definitions*, op.cit.
[173] Justice Information Sharing, *The Foreign Intelligence Surveillance Act 1978*, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance; 19 de septiembre de 2013, Disponible en línea: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286

investigación en contra de un presunto culpable con el FBI, sin embargo, los datos permanecen ahí y se utilizan muchos métodos para identificar los posibles sujetos que sean un peligro para la nación como es el análisis de tráfico de datos o el uso del *big data* para realizar perfiles.

En este sentido, es indispensable hacer referencia a la ley Patriota, gracias a ésta ley el estudio y desarrollo de las políticas en contra del terrorismo han sido excesivas e inclusive han constituido una violación a la libertad de expresión y privacidad, como fue el almacenamiento en masa de registros telefónicos por parte de la NSA, y generó como respuesta un proyecto de ley llamado *USA freedom act* que cambiaba de localidad del almacenamiento de la información a las compañías telefónicas, sin quitar el acceso de la NSA a la información,[174] y que fue aprobada por el Senado el día 2 de junio de 2015; en la que podemos encontrar 5 objetivos claros: termina la recolección *en masa* de datos; impide que las autoridades continúen con la recopilación indiscriminada y a larga escala de información; protege las libertades civiles;[175] incrementa la transparencia de los programas del gobierno haciéndolos públicos y "mantiene a Estados Unidos seguro" eliminando las lagunas que impiden que las agencias investiguen a terroristas extranjeros.[176] Un ejemplo sobre la manera en la que opera la NSA se puede ver explicada en el Esquema 3.

[174] Y le proveía seis meses a la agencia para cerrar el programa considerando que el programa sería cerrado después de que la ley pasara, sin embargo, el programa cerró durante el medio término de la discusión de esta ley, lo cual la NSA aprovechó para reabrir el programa por el tiempo determinado.
[175] Como por ejemplo creando jurados conformados por expertos en las áreas de libertades civiles y privacidad, para que den una revisión a las demandas del gobierno para obtener cierta información.
[176] Chairman Bob Goodlatte, *USA Freedom Act*, Judiciary Comittee, House of Representatives, junio 2015, Disponible en línea: https://judiciary.house.gov/issue/usa-freedom-act/ Consultado:abril 2016

Esquema 3. Cómo recolecta la NSA tus datos



Fuente: The Verge, 2013. http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet

Se puede observar que los principales aliados institucionales al interior de Estados Unidos para la NSA es la CIA y el FBI, mientras que el principal socio extranjero es el *Government Communications Headquarter* (GCHQ), aliado estratégico para intercambio de información y tecnologías útiles para la recolección de datos. La línea azul indica el uso de la interceptación de comunicaciones telefónicas y tráfico de Internet desde la red troncal de Internet. La línea amarilla indican los

flujos de la compartición de información. La línea punteada explica el flujo de los metadatos facilitados por socios comerciales de telecomunicaciones que tienen bajo orden judicial (basándose en la ley Patriota) la cesión de su información. Mientras que la línea blanca es aquella que muestra la extracción de contenidos de las principales redes sociales y metabuscadores por parte de la NSA bajo las enmiendas a la ley FISA, utilizada para respaldar las acciones de la propia agencia.

No se puede hablar de la NSA sin hablar de sus programas de vigilancia global que tiene con aliados estratégicos extranjeros y que los principales programas (más bien los de conocimiento público) son PRISM,[177] XKeyscore,[178] Tempora,[179] MUSCULAR,[180] Project 6,[181] Stateroom,[182] Lustre[183] y Five Eyes / Echelon[184] como los más ejemplares. En cuanto a las operaciones de vigilancia en general que involucran instituciones de los Estados Unidos podemos encontrar se pueden observar en el Esquema 4.[185]

---

[177] Con socios comerciales como Youtube, Skype, Yahoo, AOL, Microsoft, Facebook, Apple, Dropbox y Google.

[178] Cuyos aliados son el F6 (Special Collection Source) (CIA-NSA), FORNSAT, SSO (Special Source Operations) (NSA), Bundesnachrichtendienst (BND), Bundesamt für Verfassungsschutz (BfV), National Defence Radio Establishment (FRA).

[179] Liderado por el GCHQ, y en asociación entre las Special Source Operations de la NSA y el GCHQ únicamente.

[180] Liderado por el GCHQ trabajando con la NSA sobre las plataformas de Yahoo y Google.

[181] Liderado Bundesnachrichtendienst (BND) y el Bundesamt für Verfassungsschutz (BfV) en asociación con la CIA en contra del terrorismo, es la única operación que tiene la CIA con las dos agencias alemanas. Se comparten información estratégica como fotos, matrículas vehiculares, historiales de búsqueda por internet, y otros metadatos de presuntos jihadistas.

[182] Participa el Australian Signals Directorate con su Defense Signals Directorate (DSD), Communications Security Establishment Canada (CSEC), el GCHQ, y las Special Collection Service (SCS) del DoD para integrar a la NSA con los Elementos Criptológicos de Servicios de las FFAA, para la Seguridad de la Información.

[183] Asociación entre la NSA y la Direction Générale de la Sécurité Extérieure (DGSE) de Francia.

[184] El más complejo de todas las alianzas de vigilancia con sus orígenes desde 1941 con el UKUSAgreement, está compuesto por la NSA de EEUU., el GCHQ de Reino Unido, el DSD de Australia, el CSE de Canadá y el GCSB de Nueva Zelanda. Tiene cuatro áreas de acción operadas bajo sus respectivas dependencias gubernamentales y que son: Señales de Inteligencia, Inteligencia de Defensa, Inteligencia de Seguridad e Inteligencia Humana.

[185] Por cuestión de espacio señalamos aquí las fuentes con las se construyó el esquema 4. NY Times, http://www.nytimes.com/interactive/2015/04/25/us/25stellarwind-ig-report.html?_r=0; Electronic Frontier Foundation https://www.eff.org/es/nsa-spying/timeline; The Guardian, http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2; About US Government, http://usgovinfo.about.com/library/weekly/aa121401a.htm; Der Spiegel,

Esquema 4. Programas de vigilancia de Estados Unidos

---

http://www.spiegel.de/international/germany/cia-worked-with-bnd-and-bfv-in-neuss-on-secret-project-a-921254.html; The Washington Post http://www.washingtonpost.com/wp-dyn/content/article/2006/06/23/AR2006062300167.html; Time Magazine, http://time.com/3909293/edward-snowden-obama-nsa-spying/

Como se puede observar en el esquema la NSA juega un papel principal en el ejercicio de la vigilancia gubernamental estadounidense, en el que podemos encontrar los más sofisticados sistemas informáticos y al personal más calificado para cumplir con la misión del complejo, sin embargo, toda acción de inteligencia o ciberseguridad depende de la fortaleza de la ingeniería social de los funcionarios o empleados a cargo, lo que nos lleva a discutir este tema en el siguiente subcapítulo.

3.2 Wikileaks y los *whistle-blowers*

Los principales aciertos de los programas de vigilancia es que son intrusivos y secretos; tras ser considerados un tema de Seguridad Nacional, los Estados, y en específico, los Estados Unidos, construyen sus mecanismos de una manera sigilosa, progresiva y secreta que es casi imposible que un ciudadano promedio consiga acceso a información veraz sobre lo que ocurre.

A pesar del alto grado de confidencialidad y escrupulosidad, ha habido numerosas y significantes aportaciones de aquellos empleados y funcionarios que no están de acuerdo con la ética o el propósito de alguno o varios de los programas llevados a cabo en su lugar de trabajo, lo que nos lleva a señalar el concepto de *whistle-blower* o "denunciante", cuyo significado es aquél individuo que señala una acción o actividad como indebida, ilegal o poco ética dentro de una institución.[186]

El *whistle-blowing* es una práctica legítima con respaldo legal en diversos países aplicable dentro del sector público y el privado. En el caso estadounidense, el apoyo constitucional de la Primera Enmienda se limita para aquellos empleados que trabajan con temas de seguridad nacional por el impacto negativo que puede tener sobre el país; [187] en el caso de aquellos empleados que trabajan en la

[186] 101st United States Congress, *Whistleblower Protection Act*, 10 de abril de 1989.
[187] Cuyo texto expresa que: "El Congreso no podrá hacer ninguna ley con respecto al establecimiento de la religión, ni prohibiendo la libre práctica de la misma; ni limitando la libertad de

recopilación de inteligencia y análisis son obligados (como parte de su trabajo) a firmar un contrato o declaración de no divulgación de información.

Hubo largas discusiones sobre si este tipo de acuerdos entre empleadores y empleados sobre la "no divulgación" de información de la institución, viola los derechos constitucionales, sin embargo, la Corte Suprema tras el juicio de Frank W. Snepp,[188] determinó que Snepp violó el acuerdo que tenía con la CIA al publicar documentos clasificados y su derecho civil sobre la Primera Enmienda no había sido violado.[189]

Es así que en la actualidad, los *whistle-blowers*, quedan desprotegidos de la ley debido a su contrato laboral y peor aún, tienen penas mayores a las de un homicida o un narcotraficante, habría que meditar respecto al nivel de democracia en el que operan las instituciones gubernamentales sobre seguridad nacional, que sólo se encuentran preocupadas para acrecentar el poder nacional en este llamado "quinto espacio" y que simplemente actúan de acuerdo a las élites del poder, en el que la sociedad queda sin representación alguna frente a las decisiones que se toman respecto a mecanismos de vigilancia y la violación de la privacidad.

Retomando el tema de los *whistle-blowers*, algo que habría que destacar y agregar, es que la NSA podría tener todas las herramientas más sofisticadas y podría captar toda la información personal que desease, pero no tiene capacidades para procesarlas, es decir, no importa que tan potente sea la máquina si el que la opera sólo trabaja ocho horas al día.

---

expresión, ni de prensa; ni el derecho a la asamblea pacífica de las personas, ni de solicitar al gobierno una compensación de agravios".

[188] Fue analista de la CIA, el encargado de la caída de Saigón y fue uno de los últimos estadounidenses a abandonar la embajada de Estados Unidos, antes de la caída de la ciudad de Saigón por los vietnamitas del Norte, el 30 de abril de 1975. Snepp fue evacuado con personal estadounidense durante la Operación Viento Frecuente. Él escribió un libro de memorias del evento, en 1977, que critica la tardía e improvisada evacuación y se lamenta de los abandonos de muchos de los vietnamitas que trabajaron para los americanos y que habían quedado atrás.

[189] Justia, *Snepp v. United States 444 U.S. 507*, U.S. Supreme Court,19 de febrero de 1980, Disponible en línea: https://supreme.justia.com/cases/federal/us/444/507/case.html

Es así que algunos de los empleados que manejan estos recursos y esta información han tomado conciencia sobre las actividades y programas gubernamentales, por lo que es preciso remitirnos a hablar del primer *whistle-blower* de la NSA, Thomas Drake, hizo aportaciones relevantes sobre los métodos de la vigilancia e inteligencia de los Estados Unidos arriesgando su libertad manteniendo pláticas e intercambiando información con un periodista de *Baltimore Sun*, Siobhan Gorman en 2006, durante la Administración Bush-Cheney.

Drake antes de entrar a trabajar en la NSA trabajaba como oficial en la Fuerza Aérea, en noviembre del año 2007 el FBI cateó el domicilio de Drake confiscando su ordenador y haciendo interrogatorios a toda persona relacionada con él y este afidávit[190] originó que la agencia parara las investigaciones.[191] Sin embargo, el caso será retomado en el primer periodo de Obama, y para el 15 de abril del 2010 el *Department of Justice* (DOJ) acusó al ex empleado de 53 años de haber filtrado información clasificada referente al malgasto de la NSA y aspectos legales dudosos sobre las actividades de la agencia en sus programas contraterrorismo como el programa *Trailblazer.* [192] A pesar de no tener una condena por la cual pagar, Drake ha sido el único *whistle-blower* enjuiciado que se ha librado de perderlo todo.

La parte curiosa del caso de Drake fue que la investigación en su contra llegaba a *leaks* realizados durante los años de la administración de Bush-Cheney y es bajo la administración de Barack Obama cuando se le vuelve a procesar e investigar, el mismo Obama quien durante su año electoral de 2009 se pronunció

[190] Declaración bajo juramento
[191] Se hizo un sobre esfuerzo durante las investigaciones en las que se confiscaron demasiado indumentario como parte de evidencias y se hicieron más de 10 interrogatorios que no llevarían a ningún lugar.
[192] Fue un programa de la Agencia de Seguridad Nacional (NSA) destinado a desarrollar una capacidad para analizar datos llevados a cabo en las redes de comunicación en Internet. Fue pensado para realizar un seguimiento de las entidades que utilizan métodos de comunicación tales como teléfonos celulares y correo electrónico, una actividad que se considera ilegal bajo la Cuarta Enmienda de la Constitución de los Estados Unidos.

a favor de los *whistle-blowers*, diciendo que ellos representaban "la mejor fuente de información sobre abuso, malgasto y fraude en el gobierno".[193]

Sin embargo, Barack Obama es el presidente con mayores enjuiciamientos en contra de *whistle-blowers*, incluso duplica la cifra en utilizar la Ley de Espionaje de 1917 de todos los presidentes anteriores sumados. Esto refleja la dureza e intolerancia de su administración hacia los activistas defensores de los derechos civiles y los derechos humanos.

Tal cual se presenta en el Anexo Uso de la ley de Espionaje podemos observar persecución y procesamiento a través del tiempo de los *whistle-blowers* bajo la ley de Espionaje durante toda la historia de Estados Unidos, que no es por otro motivo que el de ser intrusos maliciosos y siendo incriminados muchas veces por considerárseles como espías o traidores, siendo que la información que revelan es de interés público pero atentan contra el sistema y, en este sentido, el complejo de vigilancia.

Podemos observar, que durante la administración de Obama cinco personas han sido condenadas bajo la ley de Espionaje, el caso más ejemplar fue el del efectivo del Ejército estadounidense, Chelsea Manning (anteriormente Bradley) quien fue torturado y maltratado por parte de las autoridades para hacer de él un ejemplo de disuasión; pero de las siete personas acusadas en total, dos fueron acusadas pero no fueron procesadas, entre esas, está Edward J. Snowden a quien retomaremos en el siguiente subcapítulo.

En la sociedad actual, las plataformas y los medios de divulgación tienen un gran trasfondo por la necesidad de sacar a la luz cuantiosas actividades de dudosa intensión por parte de los gobiernos, tal fue el caso en un primer momento *Wordpress*, y como lo es ahora con 142 caracteres, *Twitter*. No se puede decir que

[193] Jane Mayer, *The Secret Sharer: Is Thomas Drake an enemy of the State?*, A Reporter At Large, The Newyorker, 23 de mayo de 2011, Disponible en línea: http://www.newyorker.com/magazine/2011/05/23/the-secret-sharer#ixzz1MXdUFeE9

las redes informáticas y este tipo de plataformas fomenten los movimientos sociales, pero sí podemos afirmar que facilitan su organización e impacto.

En este sentido es importante mencionar el nacimiento de *Wikileaks*, una de las más grandes plataformas de información en la actualidad, que busca divulgar información de primera mano protegiendo la identidad de los *whistle-blowers* que la proporcionan.

Esta organización tiene relevancia a nivel global gracias a poseer las cualidades de un foro confiable y sin el control de intereses en específico, que expone documentos clasificados y/o confidenciales a través de fuentes de primer nivel, que no sólo es la pesadilla de los gobiernos sino también de las grandes corporaciones.

La organización surge en el año 2006 fundada por Julian Assange[194] programador y hacker, experto en temas de vigilancia y espionaje, decide buscar un host en Islandia.[195] Las actividades de *Wikileaks* comienzan a tener gran relevancia en el primer periodo de Barack Obama. Desde el 2008 hasta la fecha ha ganado 17 premios y ha estado nominado seis años consecutivos (2010-2015) para obtener el Premio Nobel de la Paz.

La misión de *Wikileaks* según Julian Assange es "[funcionar] como una librería gigante de los documentos más perseguidos.[196] Les damos asilo a estos documentos, los analizamos, los promovemos y obtenemos más".[197]

---

[194]Quien permanece asilado en la Embajada de Ecuador y limitado para salir de ahí por su apresamiento y extradición a los Estados Unidos.
[195]Islandia es considerado un país de ciber-refugio, ya que los servidores en este país están bajo estrictas leyes de privacidad, mejores que las de Estados Unidos, por lo que sus servicios de comunicación son cifrados y esto resulta en una zona libre de expresión. Como dato curioso, los servidores de *Silk Road*, también estaban localizados en Islandia, pero no se sabe cómo Estados Unidos ingresó a ellos.
[196]En el sentido de sujeto a la hostilidad y malos tratos por su posesión o divulgación.
[197]Michael Sontheimer, *Spiegel Interview with Julian Assange: We are drowning in Material*, Der Spiegel, 20 de julio de 2015, Disponible en línea: http://www.spiegel.de/international/world/spiegel-interview-with-wikileaks-head-julian-assange-a-1044399.html Consultado: mayo 2016

Wikileaks sufrió varios ciberataques a su infraestructura, e incluso se tuvo que hacer recortes en un 40% a la paga de los empleados de la organización para contratar nuevos sistemas informáticos y fortalecer la infraestructura técnica de la página web, pero esto no es sorpresa para su fundador puesto que Assange ya era familiar con las técnicas utilizadas por la NSA y el GCHQ, para la vigilancia masiva y la ciberguerra, por lo que gran porcentaje de las donaciones se destinan principalmente hacia los más sofisticados mecanismos de carga de archivos para proteger a los contribuidores.

Wikileaks recupera muchos de los principios del movimiento de la Ilustración, en el que la verdad es una divisa invaluable, y en el que la racionalidad de las acciones gubernamentales se ven realmente cuestionadas y se demuestra que existe una cuasi-democracia, en la que el ciudadano común deja sus intereses a manos de una élite reducida que desea mantenerse en el poder y realiza una cacería en contra de aquellos detractores.

Wikileaks tiene su plusvalía en la manera en que maneja sus publicaciones, los documentos que divulga son completamente idénticos a las versiones oficiales de donde se originaron, constan de copias electrónicas, pero que en estricto sentido, son indistinguibles pues no hay diferencia entre ellas.[198] La respuesta del gobierno estadounidense hacia los casi 1 mil millones de documentos divulgados por Wikileaks en una manera agresiva, a funcionarios públicos se les envió un memorándum donde quedaban bajo aviso de no tener contacto alguno con la página y para los contratistas, en caso de que tuvieran en su posesión algún documento clasificado, debían reportarlo a la oficina de seguridad de la institución.[199] Pero este tipo de avisos no quedó únicamente en el sector público, sino que incluso en la Universidad de Columbia advirtió a sus estudiantes de no publicar enlaces de los archivos o hacer comentarios al respecto e incluso evitar

[198] Julian Assange, *The Wikileaks Files: The world according to US Empire*, Verso, London, 2015, pp.594
[199] *Idem*

compartirlo en sus redes sociales[200] puesto que en el futuro podría costarles el trabajo. Wikileaks no sólo proporciona información clasificada para la población en general y de manera gratuita, sino que brinda datos que aportan significativamente al análisis de conflicto y al estudio del complejo de seguridad que países como Estados Unidos construyen bajo la superficie.

Mientras existan leyes que respalden actividades que deberían ser consideradas anti constitucionales, como lo es la ley FISA, o mientras exista la ley de Espionaje, que ha servido no para enjuiciar a verdaderos traidores del país sino aquellos que exponen a los gobiernos, la lucha por la verdad será un camino difícil para quienes decidan defenderla contra los poderosos, en un principio por ser tratados como detractores o "traidores" y llevar el juicio penal en contra de toda la unión.

A pesar de tener toda la ventaja sobre el gobierno de Estados Unidos por poseer información clasificada, uno de los precios que hay que pagar al usar el *whistle-blowing* como protesta es la libertad, Sin embargo, esta lucha en contra de aquellos programas y actividades que violan las libertades civiles continúa, y el personaje más emblemático de ello es Edward J. Snowden de quién hablaremos a continuación.

3.3 Edward J. Snowden y la crisis de la estructura de vigilancia

Obama ha sido calificado como el presidente menos transparente de la historia de Estados Unidos tras los *leaks* de Edward Snowden, a pesar de sus declaraciones de su primer campaña en 2009 donde afirmaba que "su administración estaba comprometida a crear un nivel sin precedentes de apertura [y transparencia] en el gobierno"[201]. Pero a pesar de todas estos intentos fallidos por hacer parecer que el gobierno estadounidense no actúa como estadounidense, dejan en claro que lo

[200] *Idem*
[201] The White House, *Transparency and Open Government*, Memorandum for the Heads of Executive Departments and Agencies, Disponible en línea: https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment Consultado: mayo 2016

que buscan es darle legitimidad a las actividades que estas agencias de vigilancia e inteligencia realizan dentro y fuera de Estados Unidos y que no son de reciente creación sino que representan la culminación de un proyecto mucho más ambicioso.

Edward Snowden, el hombre más buscado del siglo XI, logró ser contratado por la CIA a los 22 años de edad, un joven muy activo y de gran agudeza intelectual comenzó a trabajar en inteligencia por su gran audacia y dominio de los sistemas informáticos. A la edad de 26 fue contratista de la NSA trabajando para la empresa *Booz Allen Hamilton*, de esta manera, Snowden obtuvo acceso a los más grandes secretos del país a una edad muy temprana y su preocupación comenzó cuando descubrió que el gobierno de los Estados Unidos tenía programas con procedimientos ilegales y sin ningún respaldo de la ley, como el programa *Stellarwind* que fue mencionado en este capítulo.

Snowden pasará a la historia y representará un héroe y patriota para gran parte de la sociedad civil, sin embargo, para el complejo de vigilancia, Edward J. Snowden conforma el más grande error de las agencias de inteligencia. Era tanta la importancia de extraditarlo y enjuiciarlo para el *establishment* estadounidense, que las relaciones exteriores de Estados Unidos fueron tensas en el año 2013 y 2014 debido a la coerción y presión ejercida por sus diplomáticos en las embajadas de los países que probablemente visitaría o pediría asilo.

La Casa Blanca y el *Department of State*, procedieron a amenazar a los Estados para que retuvieran y arrestaran a Snowden para enviarlo de regreso y que enfrentara un juicio con acusaciones bajo la ley de Espionaje, pero por coincidencias y fallas técnicas por parte del proceso jurídico[202] logró con la ayuda de Wikileaks planear su escape y buscar asilo en 19 países, pero al llegar a Rusia, país de tránsito, se vio obligado a cambiar de planes y pedir el asilo político, el

[202] El error que tuvo la orden de aprensión girada en contra de Edward James Snowden, cuando su nombre es Edward Joseph Snowden y la anulación tardía de su pasaporte cuando planeaba escapar de Hong Kong.

cuál le fue otorgado el 1 de agosto de 2013 con una duración de un año, pero actualmente tiene un asilo temporal de 3 años. La situación de Snowden refleja un escenario de resistencia política, sus filtraciones no tienen un fin económico o anárquico o para otro Estado, recae en una acción civil de protesta y divulgación de actividades realizadas por el gobierno en secreto y que violan las garantías de los ciudadanos. Sin embargo, Snowden representa el único caso de los 7 acusados en la administración de Obama que tuvo apoyo de una prensa mundial[203] para conservar su vida y su libertad, Wikileaks, inclusive el periódico *The Guardian* le negó cualquier tipo de apoyo a pesar de haber trabajado con él para sacar a la luz toda la información sobre las actividades que la NSA estaba realizando.

El daño que ocasionó Edward Snowden fue hacia la estructura del complejo de vigilancia, critica fuertemente el uso de la vigilancia gubernamental mediante la exposición del amplio alcance de la NSA y el uso espionaje sobre los registros de teléfono e Internet sobre suelo estadounidense y el exterior. De esta forma, las declaraciones de Snowden tuvieron un impacto sobre la manera en la que se obtiene la información y la capacidad de generar ideas sobre lo que los grupos terroristas están haciendo,[204] a pesar de que los programas de vigilancia no previene el terrorismo en sí, pero sí genera valor para la nación [205] estadounidense.

Hay que destacar que de acuerdo a lo declarado por Snowden, las tácticas de la NSA incluyen el uso de *software* malicioso o *malware* para infectar y secuestrar los ordenadores de empresas, las organizaciones militares y gubernamentales en docenas de países extranjeros, y con ello obtener información secreta y/o estratégica, lo cual representa un grave peligro para el estado de ciberseguridad de las infraestructuras. Es pertinente aclarar que el

[203]Definida en términos de la propia organización.
[204] Tom Risen, *NSA Chief Mute on Spyware, Critical on Snowden*, US News, febrero 2015, Disponible en línea: http://www.usnews.com/news/articles/2015/02/23/nsa-chief-mute-on-spyware-critical-on-snowden Consultado: junio 2016
[205] *Idem.*

surveillance malware o *spyware* pone en peligro a cualquier sistema, sin importar si es el gobierno o algún criminal, ya que debilita las protecciones y es muy difícil de erradicar y 100% propagable.

Se comprobó que la NSA utilizó un *spyware* llamado *Stuxnet* creado para luchar contra el proyecto nuclear Iraní, al haber divulgado esta información Snowden, manchó mundialmente el tipo de negociaciones que hubo para la firma del Programa Nuclear de Irán.

Se puede observar que la utilización de mecanismos de coerción a través del ciberespacio no han sido descartados por los Estados Unidos, y que incluso, se sospecha de un intento por parte del gobierno de proyectar su poder a través de las redes y tener un impacto significativo en sus relaciones exteriores.

Dicho esto, se puede vincular la creciente necesidad por parte de las instituciones pertenecientes al complejo de vigilancia por obtener marcos legales para irrumpir con los procesos de encriptamiento de datos y líneas, ya que se maneja como "necesario" el saber qué ocurre en estos mensajes y ver si están vinculados con el crimen o el terrorismo. Sin embargo, esto refleja la necesidad de continuar expandiendo los mecanismos del complejo haciendo su alcance más certero. Sin duda ha habido una respuesta por parte de las corporaciones dedicadas a las TIC, en donde *Apple*, a pesar de trabajar con la NSA, públicamente aclaró que crear puertas traseras en sus dispositivos con motivo de análisis forenses, viola los términos de privacidad y daña la privacidad de sus clientes; por otra parte, *Whatsapp* encriptó todas sus comunicaciones fin-a-fin, los mensajes no están encriptados, pero sí las líneas de comunicación por lo que intervenir dichas costaría mucho tiempo.

Las severas divulgaciones de Snowden y Assange sobre *Google*, han afectado al complejo de vigilancia en la medida en que ésta compañía es la aliada principal para realizar actividades de ese tipo, ya que controla el "80% de la

información que fluye a través de los teléfonos inteligentes",[206] siendo así un aliado estratégico para entender el comportamiento del Internet, sin embargo, resalta un tema a mencionar, el de la cesión de la seguridad nacional estadounidense a las grandes corporaciones, sin duda requiere de una discusión mucho más profunda; mientras, este comportamiento se puede afirmar con el caso de Snowden en el que siendo un contratista, obtuvo acceso a muchos de los más delicados documentos sobre el sistema de vigilancia que ejerce la NSA, es de esta forma que él obtuvo mejor información que si hubiera trabajado dentro de la misma agencia.

Retomando el caso del encriptamiento como una respuesta a las operaciones de vigilancia realizadas por el gobierno de Estados Unidos, resulta que este tipo de solución implementada por las compañías de los TIC es sólida en la medida del compromiso de las empresas por hacer efectivo y funcional éste tipo de mecanismos, ya que al ver las recientes peticiones por la directiva de la NSA y el FBI, el crear este tipo de puertas traseras resulta una ilógica decisión por parte de los usuarios, ya que estarían cediendo su privacidad a *software* comprometido con los aparatos de vigilancia de Estados Unidos e incluso si lo hicieran, éste tipo de *software* debilitaría la ciberseguridad y haría que los consumidores estén vulnerables a los propios *hackers*.

Debido al gran impacto que han tenido las declaraciones de Snowden y las diversas filtraciones de documentos han ocasionado que haya una serie de modificaciones a este complejo de vigilancia que proporcionan bienes invaluables y que ayudan al país a llevar a cabo negociaciones en diferentes rubros.

El mayor problema que enfrenta la IC es sobre la recolección de inteligencia, al haber ensuciado la imagen de la NSA ante el público restó de autoridad para realizar actividades de espionaje, la principal fuente para la

[206] Blanche Pietrich, Google, "parte integral del Estado" estadounidense, La Jornada, 8 de junio de 2016, Disponible en línea:http://www.jornada.unam.mx/2016/06/08/mundo/023n1mun Consultado:junio 2016

generación de inteligencia, de este modo, al oponer a la opinión pública, puso de cabeza a la administración de Obama para encontrar los medios legales para reafirmar su autoridad y darle la legitimidad que el complejo de vigilancia necesita.

La NSA procura la seguridad nacional estadounidense mediante las SIGINT, de este modo, la agencia obtiene un papel base proporcionando inteligencia extranjera clave para mantener a Estados Unidos y sus aliados a salvo. Las declaraciones de distintos funcionarios públicos estadounidenses giran entorno a que las filtraciones de Snowden dañaron severamente las operaciones militares y ponen en riesgo las vidas de todos los efectivos en activo, ya que muchas de las estrategias en suelo son llevadas a cabo con información de inteligencia obtenidas a través de los mecanismos de vigilancia.

Una de las preguntas clave es, cuáles son los estándares que la NSA está utilizando para focalizar a los sospechosos de intrusión, ya que no queda claro si buscan descubrir a organizaciones criminales o gobiernos, y supuestamente la agencia debería de enfocarse en la inteligencia extranjera y no la aplicación de la ley, sin embargo, esta discusión nos lleva a mencionar, que la estrategia de Barack Obama sobre ciberseguridad, no tuvo nunca una discusión con la ciudadanía y ésto hubiera tenido significativos alcances para la población, motivo principal de la estrategia, pero esto apuntala que la estrategia planteada por la administración de Obama tiene como propósito justificar la estructura y métodos de la IC para obtener información, justificar la vigilancia disfrazándola por estrategias de ciberseguridad.

Sin duda, Edward J. Snowden es un personaje histórico del siglo XXI, no por su persona sino por lo que representa, un verdadero patriota que defiende las libertades expresadas en la Constitución y los derechos humanos, que defiende la libertad y privacidad que han sido fragmentadas o suprimidas por los mecanismos gubernamentales y que han desaparecido la existencia de una verdadera democracia.

CONCLUSIONES

En el primer capítulo observamos que la tendencia internacional sobre la creación de lineamientos y políticas para regular el ciberespacio se han dado en el marco de la hegemonía estadounidense en relación con los temas de seguridad internacional, reflejando una estructura de complejos de seguridad; cuyo alcance para intervenir en los procesos de securitización sin duda es único.

La definición y el escrutinio de los términos clave es vital para comprender el objeto de estudio, por lo que al esclarecer los significados de las palabras amenaza, riesgo y peligro, nos damos cuenta que los primeros dos son de carácter subjetivo, es decir, en el sentido en que el Estado lo interpreta, tomando en consideración las cualidades del actor considerado amenaza; la valuación de los riesgos va de acuerdo a lo que está en juego y qué otras consecuencias puede tener si el sistema u objeto en cuestión sufre efectos negativos, sin embargo, el término peligro nos remite a la seguridad humana que pocas veces aparece en las políticas sobre el ciberespacio y que a opinión personal se debería manejar con frecuencia, ya que no todos los ciudadanos perciben claramente los términos riesgo y amenaza con el grado de relevancia con el que se espera y mucho menos lo es sobre peligro de *malware* u otros.

La ciberseguridad, de acuerdo al discurso gubernamental, tiene su razón de ser por el incremento del “internet de las cosas”, en el que la conectividad de los dispositivos portátiles y domésticos que forman parte de la cotidianeidad del individuo llegan a tener un papel significativo para el desarrollo del mismo; sin embargo, hay que considerar que la estructuración del complejo de vigilancia de Estados Unidos requiere un desarrollo pleno y el control o dominio sobre las herramientas que son usadas para operar dentro del ciberespacio, es decir, el gobierno en particular, necesita ejercer su hegemonía y con esto, la plenitud de sus capacidades sin tener riesgos que minen su desarrollo a través de este medio, teniendo en cuenta que éste, es considerado el nuevo escenario de conflicto y beneficio.

Podemos decir que el inicio de la construcción de este complejo de ciberseguridad y vigilancia tiene sus principios con el presidente Bill Clinton debido a que durante su periodo presidencial se dieron a conocer las nuevas manifestaciones delictivas y terroristas a través del uso del internet y los sistemas informáticos, claro ejemplo de esto fue el gusano Morris. En el periodo de George W. Bush se da un cambio en la política de seguridad nacional por uno más intrusivo con sus ciudadanos como es el caso de la ley Patriota, ésta les sirvió en su momento a la NSA almacenar los registros telefónicos de decenas de miles de ciudadanos estadounidenses y demuestra la ambición que tienen por controlar el flujo de información.

Al estar Barack Obama en el poder, las instituciones y mecanismos de vigilancia, como la NSA principalmente, contaban con gran libertad de operación para sus programas con la más alta tecnología y un respaldo legal seguido de lagunas legales que unidas, les daban un alcance inimaginable. Sin embargo, no sólo el complejo de vigilancia se fortaleció, también el complejo de ciberdefensa se benefició de este tipo de precedentes; liderado por el DoD, ha sido poco criticado el recorte de tropas y su reubicación en los UAS, claro que al ser para la protección de la patria y el *American way of life*, cualquier medio es necesario, aunque eso implique el uso de drones con propósitos de vigilancia o en la utilización de los mismos en la guerra. Tampoco se cuestiona el constante conflicto cibernético que hay entre tres potencias mundiales, Rusia, China y Estados Unidos, a pesar de que se han dedicado al *hackeo* y robo de información con fines políticos y económicos, creando así un estado de tensión y recelo por demostrar quién tiene mejores capacidades en el ciberespacio.

Al tener un respaldo legal como la ley Patriota y la ley FISA, Estados Unidos es capaz de espiar a todo individuo en territorio estadounidense como medida contra el terrorismo, una lucha que no va a acabar y que da los suficientes motivos para tener en consideración la suspensión de las libertades civiles a

cambio de una “seguridad” que queda en términos ambiguos y que trabaja a favor de aquellos que están de acuerdo con el *establishment*.

El *Department of Defense* es el líder en las operaciones militares a través del ciberespacio, utilza las redes y las infraestructuras informáticas para agilizar el intercambio de información y para mejorar las comunicaciones durante las operaciones; así, el uso del encriptamiento de las redes de información es vital para el mantenimiento en confidencial de las las mismas, y asegurar la operatividad de los drones; el USCYBERCOM le sirve al DoD para desintegrar la infraestructura de las telecomunicaciones del enemigo y defender las propias, es así, que el uso del ciberespacio con motivos bélicos va en incremento, y esto resulta preocupante para todos aquellos Estados cuya ciberdefensa es baja, tal cual ocurrió con el ataque de Estonia o en la ciberguerra de Kosovo, en donde la importancia no radica en si es un país rico o pobre, sino en la preparación que tiene.

De esta forma, la estrategia del DoD para el ciberespacio representa el *hardpower* estadounidense dentro del medio, que es una extensión del poder nacional cuyos fines son para la defensa y ataque del país, y por ende, la seguridad nacional; sin embargo, el enfoque de seguridad humana es retomado en parte por el DHS, sin dejar a un lado la seguridad nacional, éste departamento es responsable de la resiliencia de los sistemas de comunicación y las infraestructuras críticas en caso de desastre, elaborando planes a través de sus análisis de riesgos y vulnerabilidades, que dan una estrategia *ad hoc* a las circunstancias, que han demostrado tener una alta efectividad, y que sin duda muestran que el complejo de seguridad centrado estadounidense está y estará preparado para recuperarse y mantenerse después de cualquier tipo de incidente.

No hay que dejar de lado la importancia que tiene el DHS para el complejo de vigilancia, ya que éste tiene dentro de sus subdivisiones la protección de las fronteras y los asuntos de inmigración, que son el primer filtro para proceder con

las investigaciones de los sospechosos y los movimientos que realizan, si provienen de un país no amistoso, qué nacionalidad poseen, entre otros.

Sin duda el impacto que tuvo el atentado del 11 de septiembre de 2001 sobre el pueblo estadounidense es tal, que se presta para dar cabida al tipo de operaciones de vigilancia, que si bien falta mayor exactitud en los filtros de búsqueda y elección de blancos, recopilan toda información que sea de interés gubernamental estadounidense. Sin embargo, surgen cuestionamientos sobre qué tan efectiva es la coordinación entre agencias y el grado de cooperación que manejan, ya que como se discutió en este trabajo, existe un recelo por la asignación del presupuesto de acuerdo al "rendimiento" que tengan y a la imagen que mantienen frente a la ciudadanía, de este modo, podemos ponderar que la agencia que resulta más beneficiada por el complejo de vigilancia y por los recientes *leaks* sobre las operaciones de vigilancia de la NSA, es sin duda la CIA, una institución dedicada a monitorear y a entender, y que a pesar de tener una imagen muy estigmatizada frente a la población, ha mantenido en completa discreción sus operaciones, y más aún las de vigilancia, también su imagen se preserva gracias a que su presupuesto es secreto, sus operaciones son secretas y se desconocen el nombre de sus funcionarios y tiene alianzas muy poderosas a nivel global que le permiten derrocar, crear e influenciar gobiernos por lo que se conforma de una infraestructura intragubernamental subrepticia.

Cabe agregar, que la CIA también utiliza los recursos de los complejos de ciberdefensa y ciberseguridad y no cabe duda que la astucia de la agencia recae en mantener sus operaciones en lo clandestino, en lo encubierto. De esta manera, al no hacer públicas sus actividades, la rendición de cuentas es nula y sólo mediante *whistle-blowers* y *leaks* es cuando se dan a conocer datos sobre la agencia.

Para mantener el balance de poder dentro de el gobierno estadounidense se da origen a la creación de la NSA, juntas comparten el *need-to-know* o la

necesidad de saber, obteniendo información de inteligencia secreta, que comparten con personas autorizadas dentro y fuera del gobierno quienes reaccionan a dicha información, cuando les es conveniente, con planes, actividades y asesoramiento. El actual director de la NSA declara que los valores que la información de inteligencia obtenida mediante los diversos mecanismos de vigilancia crean un bien nacional insustituible, y que las recientes filtraciones han minado el desarrollo de las relaciones exteriores y las operaciones militares.

La NSA es enigmática puesto que es la estructura técnica y tecnológica de toda la recopilación de información, la infraestructura con la que cuenta es de primer nivel y sus funcionarios integran un cuerpo sofisticado de personas dedicadas a mantener las operaciones de vigilancia a lo largo y ancho del globo, así la obtención de información es pieza fundamental para la elaboración y conducción de las políticas gubernamentales estadounidenses, ya que al tener el conocimiento sobre datos y cifras de otros Estados les ofrece ventajas significativas para las pláticas y negociaciones, es así, que el complejo de vigilancia es columna vertebral para la formulación de la política exterior estadounidense, esa necesidad de saber, los lleva a mantenerse como hegemones y conseguir sus objetivos frente a cualquier contra.

Aunque las capacidades de esta estructura sean inigualables en cuanto a alcance, también presentan un grado alto de vulnerabilidad si no existe un nivel exigente de confidencialidad, es decir, mientras estas operaciones de vigilancia salgan a la luz causarán dificultades para continuar con su operación debido a las represalias políticas, económicas y sociales como resultado de la exposición al público, tal es el caso de los diferentes *leaks* publicados por Wikileaks, ya que ésta plataforma ha logrado mantenerse íntegra en cuanto a su imagen pública, a pesar de las diversas estrategias utilizadas por los gobiernos para manchar la identidad de Julian Assange, quien permanece en asedio a pesar de que todas las actividades de Wikileaks son realizadas vía remota con el uso del ciberespacio y el

internet, demostrando que el precio de la libertad de expresión y la exposición de los oscuros programas gubernamentales es la libertad individual.

El *whistle-blowing* se encuentra en peligro desde la llegada de Obama al poder, curiosamente como se mostró en este trabajo, el presidente aprobaba y apoyaba la acción durante su candidatura pero será en sus periodos presidenciales donde se creó un sistema dentro de todas las agencias para disuadir la divulgación de documentos clasificados, como el "The Insider Threat, PVT Manning" catalogando a cada uno de los funcionarios de acuerdo a su vida personal y su personalidad, creando un mecanismo donde los individuos se espían entre sí y dan informes a las autoridades para evitar que éstos filtren documentos.

También Edward J. Snowden es parte fundamental de la crisis ocasionada por toda la serie de divulgaciones que realizó exponiendo las estructuras del complejo de vigilancia, siendo la persona más buscada y que sigue dando dolores de cabeza a la administración de Barack Obama gracias a que tuvo refugio en Rusia, no se sabe a ciencia cierta si él coopera con las autoridades rusas para proteger sus infraestructuras de las intrusiones estadounidenses, pero el simple hecho de tener a Snowden en Rusia demuestra una incapacidad de las autoridades para hacer cumplir la ley, pero más aún porque el gobierno es incapaz de silenciarlo y esto continúa vulnerando la seguridad nacional. El análisis de las capacidades de las instituciones es enriquecedor académicamente ya que se mide el alcance de las potencias para así entender la definición de las políticas de seguridad en un nivel global.

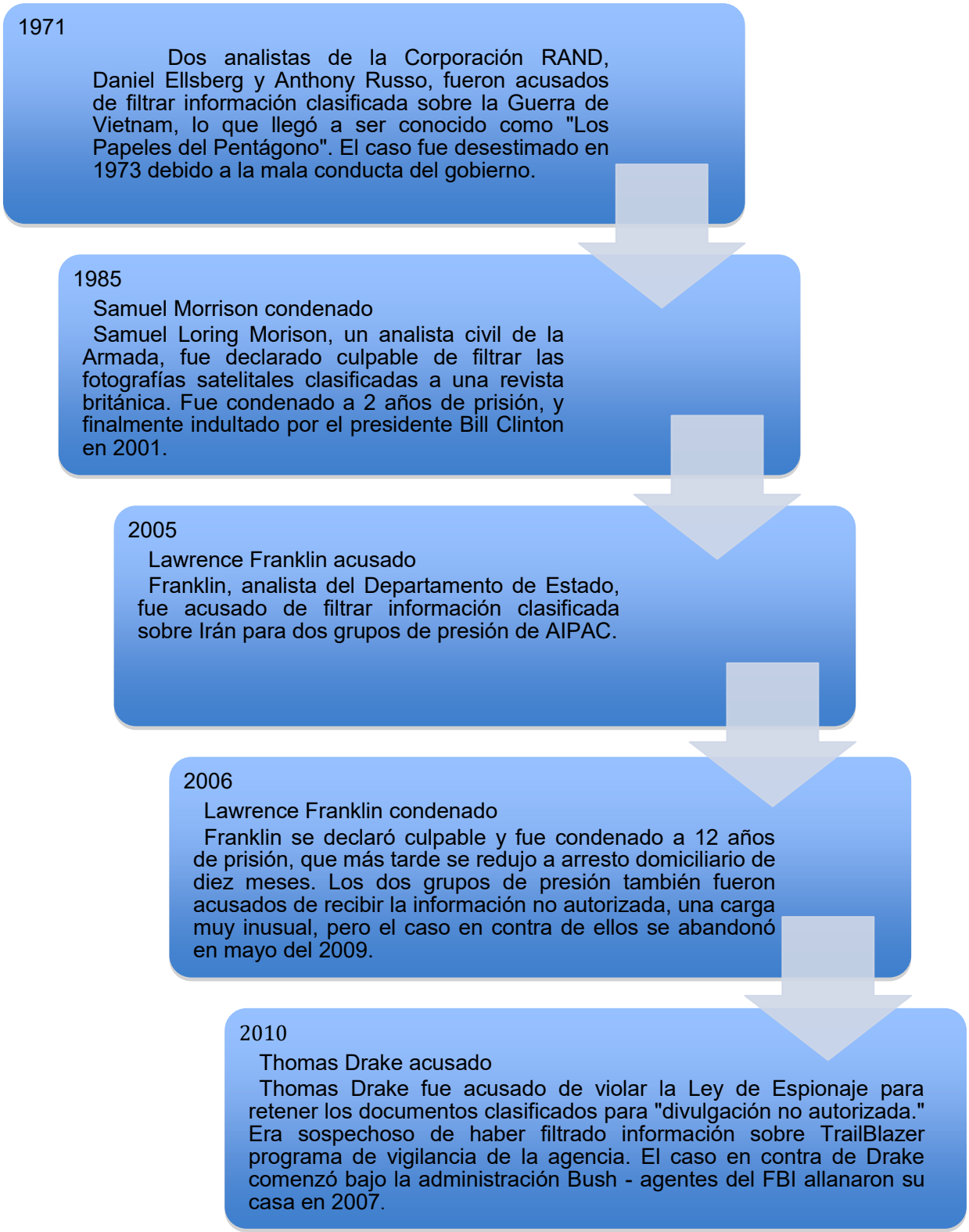
A título personal me gustaría señalar que si bien la vigilancia por parte el gobierno es una violación la privacidad no figura como amenaza para la ciudadanía ya que la vigilancia *per se* es una híper vigilancia selectiva regida bajo principios matemáticos, que demuestran que es improbable realizar una vigilancia universal puesto que no todos figuramos como enemigo público, de esta manera,

se hace evidente que el principal interés del gobierno es vigilar o en otras palabras espiar a los gobiernos extranjeros y aquellas personas de interés.

Sin embargo, es indispensable mencionar que ante la creciente contratación de empresas privadas desarrolladas en éste ámbito genera preguntas sobre quién procesa y obtiene ésta información, y si existe algún riesgo de que llegue a manos indeseables.

La hipótesis de este trabajo se comprueba porque se exponen los puntos ambiciosos de la expansión del poder del gobierno de Estados Unidos a través del ciberespacio. Una expansión del centro a la periferia conformada por una estructura jurídico-política que tiene como propósito la supervivencia del *status quo* del gobierno estadounidense como policía mundial y un vigía permanente, con la búsqueda inalcanzable del enemigo, amenazas no tradicionales que se envuelven y coquetean con los Estados, y que traen consigo el proyecto de realizar una estructura compleja de seguridad que en un primer momento proteja a la nación estadounidense y en consecuencia, el liderazgo del país en el escenario internacional.

Anexo Uso de la ley de Espionaje



-

Shamai Leibowitz condenado

Leibowitz, un lingüista y traductor para el FBI, se declaró culpable de filtrar información clasificada a un *blogger*. Fue condenado a 20 meses de prisión. En el momento de su condena, ni siquiera el juez sabía exactamente lo que se había filtrado, a pesar de las revelaciones posteriores indicaron que era escuchas telefónicas del FBI de conversaciones entre diplomáticos israelíes sobre Irán.

-

Bradley Manning detenido

Bradley Manning, miembro del Ejército de 22 años, fue detenido después de que él le dijo a alguien en línea que era la mayor fuente de Wikileaks con un cuarto de millón de cables del Departamento de Estado.

Pasaron casi dos años antes de que al final recayera en un tribunal militar. En febrero de 2013, se declaró culpable de proporcionar archivos de Wikileaks, pero no de haber violado la Ley de Espionaje y otros cargos. Los tribunales han mantenido un nivel sin precedentes de secreto sobre el caso, así como la retención de documentos y permitir que los testigos declararan en secreto.

Stephen J. Kim acusado

Kim, un analista que trabajaba en el Departamento de Estado, fue acusado de dar información clasificada a Fox News sobre Corea del Norte. Un informe de julio 2013 en fallo en el caso, un juez federal dijo que el gobierno no tenía necesidad de demostrar que la información filtrada podría haber dañado la seguridad nacional, sólo que Kim sabía que podía filtrar información y la había filtrado voluntariamente.

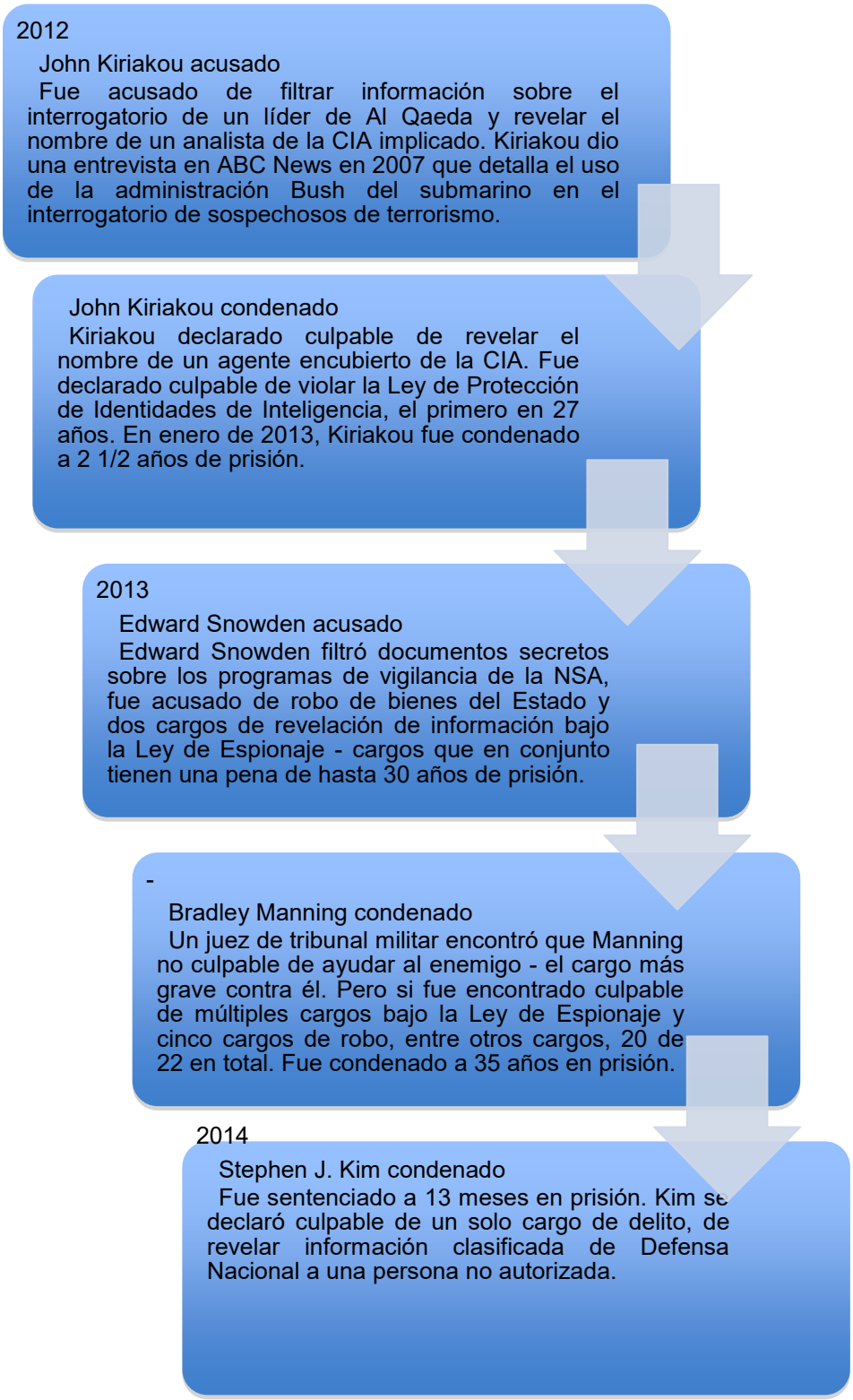
Jeffrey Sterling acusado

Sterling, un agente de la CIA, fue acusado de filtrar información sobre los esfuerzos de la CIA contra el programa nuclear de Irán. En el New York Times, a James Risen se le ordenó a declarar en el juicio de Sterling. Los fiscales creen que había filtrado material para el libro de Risen "Estado de guerra." Risen peleó en contra de la citación, con el argumento de que era para proteger la confidencialidad de su fuente. En julio de 2013, Risen perdió esa pelea, cuando un tribunal federal de apelaciones dijo que no había "reporteros con privilegio" y no podría permitir que él no testificara.

2011

Cierran caso de Thomas Drake

Se le declaró culpable de un cargo menor, que no está bajo la Ley de Espionaje, por lo que no sirvió ninguna hora de prisión. El gobierno había decidido que no podían procesar sin revelar detalles acerca de los documentos que supuestamente filtró. Los críticos vieron la retirada del gobierno como una señal de que se habían excedido en el uso de la Ley de Espionaje.


2012
John Kiriakou acusado
Fue acusado de filtrar información sobre el interrogatorio de un líder de Al Qaeda y revelar el nombre de un analista de la CIA implicado. Kiriakou dio una entrevista en ABC News en 2007 que detalla el uso de la administración Bush del submarino en el interrogatorio de sospechosos de terrorismo.
John Kiriakou condenado
Kiriakou declarado culpable de revelar el nombre de un agente encubierto de la CIA. Fue declarado culpable de violar la Ley de Protección de Identidades de Inteligencia, el primero en 27 años. En enero de 2013, Kiriakou fue condenado a 2 1/2 años de prisión.
2013
Edward Snowden acusado
Edward Snowden filtró documentos secretos sobre los programas de vigilancia de la NSA, fue acusado de robo de bienes del Estado y dos cargos de revelación de información bajo la Ley de Espionaje - cargos que en conjunto tienen una pena de hasta 30 años de prisión.
-
Bradley Manning condenado
Un juez de tribunal militar encontró que Manning no culpable de ayudar al enemigo - el cargo más grave contra él. Pero si fue encontrado culpable de múltiples cargos bajo la Ley de Espionaje y cinco cargos de robo, entre otros cargos, 20 de 22 en total. Fue condenado a 35 años en prisión.
2014
Stephen J. Kim condenado
Fue sentenciado a 13 meses en prisión. Kim se declaró culpable de un solo cargo de delito, de revelar información clasificada de Defensa Nacional a una persona no autorizada.

2015

Jeffrey Sterling condenado

Fue sentenciado a 3 años y medio en prisión. Fue declarado culpable de nueve delitos graves incluido el espionaje.

Fuente: Elaboración propia con información de: Propublica, https://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks

Como se puede observar en ésta línea de tiempo, durante los dos periodos presidenciales de Barack Obama es cuando más se reprime ésta actividad a pesar de demostrar una gran legitimidad, es gracias a esta caza de *whistle-blowers* que los funcionarios públicos tienen un temor a perder sus vidas a cambio de dar información clasificada, ya que como se puede observar en la línea, sólo dos individuos no fueron condenados, uno de ellos terminó en un trabajo insignificante y otro está asilado en Rusia.

BIBLIOGRAFÍA

- 101st United States Congress, *Whistleblower Protection Act*, 10 de abril de 1989.
- 108º Congreso de los Estados Unidos de América, Reforma de Inteligencia y Acta de prevención terrorista del 2004, Ley Pública 108-458, Estados Unidos, Diciembre 17 2004, Disponible en línea: https://www.gpo.gov/fdsys/pkg/PLAW-108publ458/pdf/PLAW-108publ458.pdf Consultado: abril de 2016
- AFCEA Intelligence Committee, *The Need to Share: The US. Intelligence Committee and Law Enforcement,* White Paper, Estados Unidos, Abril de 2007, Disponible en línea: http://www.afcea.org/mission/intel/documents/SpringIntel07whitepaper_000.pdf Consultado: mayo de 2016
- Aguayo, Sergio y Bangley, Bruce Michael (coordinadores). *En búsqueda de la Seguridad nacional perdida. Aproximaciones a la seguridad nacional mexicana*, México, Siglo Veintiuno Editores, 1990, p. 27.
- Angwin, Julia, Savage, Charlie, Larson, Jeff, Moltke, Henrik, Poitras, Laura y Risen, James *AT&T Helped US Spy on Internet On A Vast Scale*, The New York Times, 15 de agosto de 2015, Disponible en línea: http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0 Consultado: mayo 2016
- Assange, Julian, *The Wikileaks Files: The world according to US Empire*, Verso, London, 2015, pp.594
- Buzan, Barry, *The National Security in International Relations, People States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, Harvester Wheatsheaf, Londres, 1991. pp. 1-34
- Brandom, Russell *How far did the NSA go to weaken cryptography standards?*, The Verge, 11 de septiembre de 2013, Disponible en línea: http://www.theverge.com/2013/9/11/4718694/how-far-did-the-nsa-go-to-weaken-cryptography-standards Consultado: mayo de 2016

- BBC Mundo, *La NSA, la agencia de espionaje más secreta de Estados Unidos*, 10 de junio de 2013, Disponible en línea:http://www.bbc.com/mundo/noticias/2013/06/130610_internacional_ee_uu_national_security_agency_perfil_nc Consultado: junio 2016
- Carr, Feffrey, *Inside Cyber Warfare*, United States of America, O'reilly Media, Inc, second edition. 2012, p.59
- Central Intelligence Agency, *History of American Intelligence*, Kids Zone, 23 de marzo de 2013, Disponible en línea: https://www.cia.gov/kids-page/6-12th-grade/operation-history/history-of-american-intelligence.html Consultado: mayo 2016
- Chairman, Goodlatte, Bob *USA Freedom Act*, Judiciary Comittee, House of Representatives, junio 2015, Disponible en línea: https://judiciary.house.gov/issue/usa-freedom-act/ Consultado:abril 2016
- Coqui, Martha Bárcena, *La reconceptualización de la seguridad* en Senado de la República. Memoria del Seminario Informativo. Seguridad Internacional en el siglo XXI: los retos para América Latina y el Caribe, México, Senado de la República, 2004, p.19
- Correa, Guillermo, *Ciberseguridad, Seguridad Ampliada: los nuevos temas de seguridad*, Diplomado de Seguridad Internacional, División de Educación Continua y Vinculación, FCPyS, enero 29 de 2016. Disponible en línea: http://decyvpoliticas-unam.org/pag/temarios/seguridad/Cibert.%20Ponente%202.pdf Consultado: enero de 2016
- Comité Internacional de la Cruz Roja, *Cuál es la definición de "conflicto armado" según el derecho internacional humanitario?*, Dictamen de marzo de 2008, Disponible en línea: https://www.icrc.org/spa/assets/files/other/opinion-paper-armed-conflict-es.pdf Consultado: mayo de 2016
- Currier, Cora, *Charting Obamas crackdown on National Security Leaks*, Propublica, julio 2013, Disponible en línea:

https://www.propublica.org/special/sealing-loose-lips-charting-obamas-crackdown-on-national-security-leaks Consultado: junio de 2016

- Department of Defense, *Quadrennial Review Report 2010*, DoD, Estados Unidos, Enero 29 de 2010, p.ix, Disponible en línea: http://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf Consultado: mayo de 2016
- Department of Defense, *Quadrennial Defense Review Report 2014*,Estados Unidos, p.vii Disponible en línea:http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf Consultado: mayo de 2016
- Department of Homeland Security, *Enabling Distributed Security in Cyberspace, DHS*, 23 de marzo de 2011, p. 2 Disponible en línea: https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf Consultado: mayo de 2016
- Department of Homeland Security, "Privacy Impact Assessment for EINSTEIN 3 Accelerated (E3A)", U.S. Department of Homeland Security, 19 de abril de 2013, Disponible en línea: https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf Consultado: mayo 2016
- Department of Homeland Security, *US-CERT Infosheet*, DHS Cybersecurity, septiembre de 2013, Disponible en línea en: https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf Consultado: mayo 2016
- Desarrollo web, *¿Qué es el domain name system?*, Disponible en línea: http://www.desarrolloweb.com/faq/50.php Consultado: mayo de 2016
- Espinosa, Alejandra Morán, Camaño, Alejandro Servín y Gálvez, Oscar Alquicira, TIC (Internet) y Ciberterrorismo, Revista de Seguridad, No. 23, UNAM. Disponible en: http://revista.seguridad.unam.mx/numero23/tic-internet-y-ciberterrorismo Consultado: octubre de 2015

- Espinosa, Alejandra Morán, Camaño, Alejandro Servín y Gálvez, Oscar Alquicira op.cit.
- FEMA, National Preparedness Goal 2015, Disponible en línea: http://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf Consultado: mayo 2016
- Gaddis Lewis, John, *Surprise, Security, and the American Experience*, Cambridge, MA, Harvard University Press, 2004. 160 pp.
- Gallagher, Ryan, Obama faces calls to reform Reagan-era Mass Surveillance Order, The Intercept, 2 de septiembre de 2014, Disponible en línea: https://theintercept.com/2014/09/02/obama-12333-surveillance-nsa-rights-groups-letter/ Consultado: junio 2016
- Glosario de Términos de inteligencia y Seguridad Nacional, Serie Manuales y Guías Núm. 3, México, Noviembre de 2011
- Glüsing, Jens, Poitras, Laura, Rosenbach, Marcel y Stark, Holger, *Fresh Leak on US Spying: NSA Accessed Mexican President's Email*, Der Spiegel, 20 de octubre de 2013, Disponible en línea: http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html Consultado: mayo 2016
- Hamblen, Matt, *Clinton commits 1.46 B to fight cyberterrorism*, CNN, enero 1999, Disponible en línea: http://edition.cnn.com/TECH/computing/9901/26/clinton.idg/ Consultado: junio 2016
- Harper's Magazine, The paranoid style in American politics, noviembre de 1964 de Disponible en línea: http://harpers.org/archive/1964/11/the-paranoid-style-in-american-politics/ Consultado: febrero de 2016
- ISO, *Guide 73:2009*, International Standard Organization, Disponible en línea: https://www.iso.org/obp/ui/es/#iso:std:iso:guide:73:ed-1:v1:en Traducción personal, Consultado: febrero de 2016
- ISACA and RSA Conference Survey, State of Cybersecurity: Implications for 2015, Cybersecurity Nexus, Disponible en línea en:

http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf Consultado: mayo de 2016

- IT Law, Meridian Conference Process, IT Wiki Law, Disponible en línea: http://itlaw.wikia.com/wiki/Meridian_Conference_and_Process Consultado: mayo de 2016
- Justia, *Snepp v. United States 444 U.S. 507*, U.S. Supreme Court,19 de febrero de 1980, Disponible en línea: https://supreme.justia.com/cases/federal/us/444/507/case.html Consultado:abril 2016
- Justice Information Sharing, *The Foreign Intelligence Surveillance Act 1978*, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance; 19 de septiembre de 2013, Disponible en línea: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286 Consultado:abril, 2016
- Kamp, Karl-Heinz, *Intervenciones militares cautelares (preemptive strikes): ¿una nueva realidad de la política de seguridad?,* Instituto de Investigaciones Jurídicas, UNAM, Disponible en línea: http://www.juridicas.unam.mx/publica/librev/rev/dconstla/cont/2004.2/pr/pr22.pdf Consultado: enero de 2015
- Legal Information Institute, 18 U.S.C. § 1839-Definitions, Cornell University Law School, Disponible en línea: https://www.law.cornell.edu/uscode/text/18/1839 Consultado: mayo de 2016
- Mayer, Jane. *The Secret Sharer: Is Thomas Drake an enemy of the State?*, A Reporter At Large, The Newyorker, 23 de mayo de 2011, Disponible en línea: http://www.newyorker.com/magazine/2011/05/23/the-secret-sharer#ixzz1MXdUFeE9
- Mead, Walter Russell, *A Hegemon's Coming of Age. A Brief History of U.S. Foreign Relations*", *Foreign Affairs*, July-August 2009. Disponible en línea: http://www.jstor.org/stable/20699628?seq=2#page_scan_tab_contents Consultado: marzo de 2016

- Moran, E. Alejandra, Servin C., Abraham A. y Alquicira, G. Oscar, TIC (internet) y ciberterrorismo, seguridad prevención para ti, UNAM, numero 23, 5 marzo 2015: http://revista.seguridad.unam.mx/numero23/tic-internet-y-ciberterrorismo Consultado: mayo de 2016
- Nakashima, Ellen, *DHS Cybersecurity Plan Will Involve NSA, Telecoms*, The Washington Post, 3 de julio de 2009 Disponible en línea: http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771.html Consultado: mayo de 2016
- National Counterintelligence and Security Center, Glossary, NCSC, Disponible en línea: http://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf
- National Initiative for Cybersecurity Careers and Studies. *Explore Terms: A Glossary of Common Cybersecurity Terminology*. Homeland Security Department. Disponible en línea: https://niccs.us-cert.gov/glossary#letter_c Consultado: octubre de 2015
- National Security Agency, *About NSA FAQS,* NSA/CSS, 3 de mayo de 2016, Disponible en línea: https://www.nsa.gov/about/faqs/about-nsa-faqs.shtml Consultado: mayo 2016
- NSA/CSS, *What We Do: Cyber,* NSA/CSS, 3 de mayo de 2016 Disponible en línea: https://www.nsa.gov/what-we-do/cyber/ Consultado: mayo 2016
- Obama, Barack, *Woodrow Wilson Center Speech*, Council on Foreign Relations, Estados Unidos, 1 de agosto de 2007, Disponible en línea: http://www.cfr.org/elections/obamas-speech-woodrow-wilson-center/p13974 Consultado: marzo de 2016
- Obama, Barack, *Statement by the President*, The White House, Fairmont Hotel, San José California, junio de 2013, Disponible en línea: https://www.whitehouse.gov/the-press-office/2013/06/07/statement-president Consultado: marzo de 2016
- ODNI, *Requested Budget Figure for FY 2016 Appropiations for the National Intelligence Program*, ODNI, Estados Unidos, Febrero 2 2015, Disponible en

línea: http://www.dni.gov/files/documents/FY%202016%20NIP%20Fact%20Sheet.pdf Consultado: abril de 2016.

- ODNI, *Requested Budget Figure for FY 2017 Appropiations for the National Intelligence Program*, ODNI, Estados Unidos, Febrero 9 del 2016, Disponible en línea:http://www.dni.gov/files/documents/Newsroom/Press%20Releases/FY2017NIPRequestedfactsheet.pdf Consultado: mayo de 2016
- Of-course-they-do, *FBI And CIA Use Patriot Act's Bulk Data Collection To Get Money Transfer Data*, TechDirt, noviembre 2013, Disponible en línea:https://www.techdirt.com/articles/20131115/02480125256/ Consultado: junio 2016
- Parks, Bob, *Obama's 2007 Promise 'No more illegal wiretapping of American Citizens',* Disponible en línea: http://www.cnsnews.com/blog/bob-parks/obamas-2007-promise-no-more-illegal-wiretapping-american-citizens Consultado: abril de 2016
- Phillip, Abby D, *President Obama: NSA Spying Programs "Transparent"*, 17 de junio de 2013, Disponible en línea: http://abcnews.go.com/blogs/politics/2013/06/president-obama-nsa-spying-programs-transparent/ Consultado: mayo 2016
- Pietrich, Blanche, Google, "parte integral del Estado" estadounidense, La Jornada, 8 de junio de 2016, Disponible en línea:http://www.jornada.unam.mx/2016/06/08/mundo/023n1mun Consultado: junio 2016
- Reporters Without Borders, *Enemies of the Internet 2014: Entities at the heart of censorship and surveillance*, Reporters Without Borders, Paris, 11 de marzo de 2014.
- Risen, Tom, *NSA Chief Mute on Spyware, Critical on Snowden*, US News, febrero 2015, Disponible en línea: http://www.usnews.com/news/articles/2015/02/23/nsa-chief-mute-on-spyware-critical-on-snowden Consultado: junio 2016

- Rodriguez, Stephen M., *USCYBERCOM: A Centralized Command of Cyberspace*, Joint Military Operations Department and the Naval War College, Mayo 31 de 2011, archivo en PDF.
- Savage, Charlie, *Power Wars: Inside Obama's post-9/11 presidency*, Little brown and Company, Estados Unidos, noviembre de 2015, pp. 769
- Sontheimer, Michael, *Spiegel Interview with Julian Assange: We are drowning in Material*, Der Spiegel, 20 de julio de 2015, Disponible en línea: http://www.spiegel.de/international/world/spiegel-interview-with-wikileaks-head-julian-assange-a-1044399.html Consultado: mayo 2016
- Stolberg, Allan G., *The International System in the 21st Century* en Bartholomees, Jr., J. Boone (edit.), *The U.S. Army War College Guide to National Security Issues,* volumen II, Strategic Studies Institute, EE.UU. pp. 153-225. Disponible en línea: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1005 Consultado: abril 2016
- The Secretary of Defense, *The DoD Cyber Strategy*, The Department of Defense, Abril 2015, Disponible en línea: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf Consultado: mayo de 2016
- Thielman, Sam, Silk Road Operator Ross Ulbricht Sentenced to Life in Prison, The Guardian, Nueva York, Estados Unidos, 29 de mayo de 2015, Disponible en línea: https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced Consultado: mayo de 2016
- Ullman, Richard, *Redefining Security*, en *International Security*, EE.UU. vol.8, no.1, 1983. Pp. 129-53.
- UNISDR, *Terminología sobre reducción de riesgo de desastres*, 2009. Disponible en línea: http://www.unisdr.org/files/7817_UNISDRTerminologySpanish.pdf Consultado: noviembre de 2015

- Unión Europea, *Internet of Things,* Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers, 2013 Disponible en línea: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf Consultado: abril de 2015
- United States Defense Department, *The DoD Cyber Stategy 2015*, Disponible en línea: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf Consultado: febrero de 2016
- United States Government Publishing Office, *USA PATRIOT Act*, 107th Congress of the United States of America, Disponible en línea:https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf Consultado: junio 2016
- University of Cornell, *50 U. S. Code 1801 Definitions*, Cornell Law University, Disponible en línea: https://www.law.cornell.edu/uscode/text/50/1801 Consultado:abril 2016
- US-CERT EINSTEIN 2, *Privacy Impact Assessment*, DHS, 19 de mayo de 2008, Disponible en línea: https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf Consultado: mayo de 2016
- Vinton, Kate, Alleged Silk Road Creator Ross Ulbricht Fourth Amendment Rights Were Violated, Lawyers Say, Forbes, 4 de agosto de 2014, Disponible en línea: http://www.forbes.com/sites/katevinton/2014/08/04/alleged-silk-road-creator-ross-ulbrichts-fourth-amendment-rights-were-violated-lawyers-say/#6af0036d11a5 Consultado: mayo de 2016
- The White House, *President Clinton: Working to Strengthen Cybersecurity*, White House at work, 16 febrero de 2000, Disponible en línea: https://clinton4.nara.gov/WH/Work/021600.html Consultado: junio de 2016

- The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, White House, Mayo 2011, Disponible en línea: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf Consultado: mayo de 2016
- The White House, *Transparency and Open Government*, Memorandum for the Heads of Executive Departments and Agencies, Disponible en línea: https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment Consultado: mayo 2016
- Wolfers, Arnold, *National Security as an ambiguous symbol*, en *Discord and Collaboration: Essays on International Politics*. The Johns Hopkins University Press, Baltimore, EE.UU.1962. pp. 5-10