UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

CIBERSEGURIDAD EN ESTADOS UNIDOS: VULNERABILIDAD EN EL HACKEO Y ESPIONAJE SOBRE INFORMACIÓN CLASIFICADA EN MATERIA DE POLÍTICA EXTERIOR (2009- 2012.)

TESIS

PARA OBTENER EL TITULO DE

LICENCIADA EN RELACIONES INTERNACIONALES

P R E S E N T A:

SANDRA YARELLI CRUZ NAVA

ASESOR: MTRO. ALEJANDRO MARTINEZ SERRANO

NEZAHUALCÓYOTL, ESTADO DE MÉXICO, 2017

Agradecimientos

A mis padres.

Por su amor, trabajo y sacrificios en todos estos años, gracias a ustedes he logrado culminar una de mis grandes metas, mi carrera profesional, al brindarme siempre su confianza, apoyo incondicional, aconsejarme y guiarme en el camino de la vida, ustedes son mi ejemplo de superación a pesar de las adversidades.

A mi hermano.

Gracias por brindarme tu apoyo incondicional y siempre estar a mi lado en las buenas y en las malas, gracias por escucharme y ayudarme, te quiero mucho.

A mi alma máter.

La UNAM y especialmente a la Facultad de Estudios Superiores Aragón, por permitirme formar parte de esta gran institución y por brindarme las herramientas necesarias para poder desarrollarme académica y profesionalmente.

Mtro. Alejandro Martínez Serrano.

Gracias por guiarme y brindarme su apoyo en la realización del presente proyecto de investigación, junto con ello me llevo aprendizaje el cual me ayudó a tener un panorama más amplio acerca de la carrera de R.R.I.I. y del mundo que nos rodea, además de poner en práctica un buen porcentaje de los conocimientos adquiridos durante mi formación estudiantil.

A mis sinodales

Gracias por sus brindarme su conocimiento, tiempo, apoyo, recomendaciones y consejos para la culminación y enriquecimiento de este trabajo de investigación.

Índice

Imágenes

Cuadros

Graficas

Esquemas

Índice de siglas y abreviaturas

ANT	Access Network Technology
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Project Agency Net
CCDCOE	Cooperative Cyber Defense Centre of Excellence
CIA	Central Intelligence Agency
CISPA	Cyber Intelligence Sharing and Protection Act
CNCI	Comprehensive National Cybersecurity Initiative
CSNET	Computer Science Network
CYBERCOM	United States Cyber Command
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DNS	Domain Name System
DOD	Deparment of Defense
DODIN	Deparment of Defense Information Network
FBI	Federal Bureau of Investigation
FISA	Foreing Intelligence Surveillance Court
GCHQ	Goverment Communications Headquaters
ICS	Industrial Control System
IED	*Improvised Explosive Device*
IP	Internet Protocol
NATO	North Atlantic Treaty Organization
NCTC	National Counter Terrorism Center

NICE	National Iniciative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSB	National Security Branch
OCDE	Organización para la Cooperación y Desarrollo Económicos
OEA	Organización de los Estados Americanos
ONG	Organización No Gubernamental
ONU	Organización de Naciones Unidas
SCADA	Supervisory Control And Data Acquisition
TAO	Tailored Access Operations
TCP	Transfer Control Protocol
TIC	Tecnologías de la Información y Comunicación
TOR	The Onion Router
UIT	Unión Internacional de Telecomunicaciones
USCYBERCOM	United States Computen Emergency Readness Team
VANT	Vehiculos Aéreos No Tripulados

CIBERSEGURIDAD EN ESTADOS UNIDOS: VULNERABILIDAD EN EL HACKEO Y ESPIONAJE SOBRE INFORMACIÓN CLASIFICADA EN MATERIA DE POLÍTICA EXTERIOR (2009- 2012.)

Introducción

El tema de tesis es: Ciberseguridad en Estados Unidos: Vulnerabilidad en el hackeo y espionaje sobre información clasificada en materia de política exterior (2009- 2012).

El tema de la presente tesis se enfoca en la primera administración del presidente Barack Obama durante la cual impulsó iniciativas de ciberseguridad debido a las amenazas de grupos terroristas y ataques focalizados a una desestabilización tanto política, económica y social, convirtiendo el tema en una prioridad en la agenda de seguridad nacional de Estados Unidos al reconocer los riesgos en el ciberespacio con el uso de internet y los elementos referentes a la infraestructura de la información norteamericana.

Debido a la revolución tecnológica que avanza rápidamente, Estados Unidos se ve en la necesidad de reforzar sus medidas de seguridad a partir de ataques cibernéticos que han provocado riesgos para la soberanía, por pequeñas fracturas en los candados de seguridad que los hackers han aprovechado para tomar posesión de los hardwares y softwares para manejar información restringida y hacerla pública, por este motivo la seguridad de la información es uno de los principales vectores dentro de la ciberseguridad para inhibir ataques; La seguridad cibernética estadounidense, se ha visto vulnerable por organizaciones criminales que han utilizado armas cibernéticas como han sido virus, *botnets*[1], ataques *phishing* (robo de contraseñas),bombas lógicas que se han filtrado por agujeros en la seguridad de los programas informáticos, a continuación se hará

[1] Un *botnet* es una red de ordenadores, denominados zombies, controlados por el propietario de bots (programas maliciosos).

mención de casos donde la vulnerabilidad de los candados de seguridad y contraseñas han sido tomadas por hackers :

A) “Ataque a la Casa Blanca el 19 de Julio de 2001 a media noche, más de 350,000 máquinas conectadas a internet se lanzan al unísono contra el sitio web de la Casa Blanca. Es un ataque que acabará tumbando parte de los sistemas informáticos presidenciales.”[2]

B) “Se filtran en 2010, diversas contraseñas del proyecto WikiLeaks. Las contraseñas protegían archivos que contenían cables diplomáticos aun no revelados a la opinión pública y con nombres de persona aun sin borrar.”[3]

Como se muestra en los ejemplos anteriores existe fragilidad en los sistemas de seguridad a pesar de tener candados sofisticados; los hackers utilizan cualquier error aunque sea insignificante para penetrar a las cuentas oficiales como fue el caso del ex-presidente Barack Obama, debido a que simpatizantes del Estado Islámico que se autodenominan “ Cibercalifato” tomaron control de la cuenta en una red social muy popular como lo es Twitter, en la cual postearon mensajes alusivos al Estado Islámico y realizaron amenazas a la familia Obama.

El caso de wikiLeaks se desarrollará durante la investigación, sin embargo las filtraciones del portal WikiLeaks, por su fundador Julián Assange es otro ejemplo de la vulnerabilidad en la infraestructura cibernética al hacer de manera pública documentos e imágenes confidenciales, lo que provocó una gran molestia entre los Estados, debido a que se dieron a conocer cables diplomáticos, conversaciones, correos electrónicos de Jefes de Estado, ministros, embajadores, etc. que fueron vigilados por el Departamento de Estado de Estados Unidos a través de sus delegaciones.

Los riesgos y amenazas del siglo XXI ha llevado a los Estados a enfrentarse con nuevas tecnologías derivadas de la revolución tecnológica, la cual ha avanzado rápidamente y hoy en día juega un papel importante para el desarrollo de cada

[2] Medina Manel, Molist Mercé, Cibercrimen ¡Protégete del Bit-Bang!, Los ataques en el ciberespacio a: Tu ordenados, tu móvil, tu empresa, Ed. Tibidabo, Barcelona, 2015, p.88.
[3] Ibidem., p.25

Estado, porque se ha convertido en una herramienta para el ser humano que le ha permitido tener una mejor calidad de vida, obtención rápida de conocimientos, concentración de datos estadísticos de la sociedad y ocio, sin embargo el ciberespacio no está controlado y cualquier persona puede entrar de forma anónima, robar ,atacar, modificar y suplantar información de las redes sociales o paginas institucionales a fin de causar descontento y problemas político-sociales, debido a que la población utiliza el ciberespacio sin tomar medidas de protección, las redes criminales aprovechan la situación para filtrarse por cables cibernéticos vulnerables a la confidencialidad e integridad del Estado-Nación.

La globalización se definiría como un proceso de cambio, que permite la conexión entre los Estados, organizaciones, empresas y sociedad civil, provocando efectos políticos, económicos, sociales y culturales a nivel mundial, por medio de la interacción de todos los actores involucrados con el uso de tecnología, por ello la seguridad es uno de los principales vectores dentro del proceso de adaptación y cambio para inhibir ataques o crímenes por la vulnerabilidad en el mundo digital. Es por este motivo que representa un problema para las Relaciones Internacionales, por la participación de Estados, empresas, ONG´s y la sociedad internacional en el uso de las tecnologías de la información y comunicación como consecuencia del progreso de la humanidad en materia tecnológica y telecomunicaciones, que al haber un desequilibrio puede provocar un nuevo orden mundial que se basará en las reacciones e interacciones de los Estados para tomar sus medidas de seguridad, en el caso de las medidas de la seguridad nacional estadounidense, la cual se centra principalmente en proteger sus áreas de influencia para la permanencia de su liderazgo y supremacía en el escenario internacional, provocando inconformidades y conflictos bélicos lo que ha llevado a Estados Unidos a tomar medidas drásticas e instaurar programas de defensa, que involucra espionaje a los Estados y a sus ciudadanos para la obtención de información que atente a su seguridad nacional, invadiendo la soberanía de los países para la protección de cualquier ataque terrorista.

Por lo cual Estados Unidos en los últimos años ha invertido en el uso de la tecnología para desarrollar mecanismos complejos y evitar ataques cibernéticos así como espionaje, cibercrimenes y hackeo de bases de datos institucionales por grupos terroristas para desestabilizar el desarrollo de la Nación, se han empleado mecanismos para proteger bases de datos oficiales y de gran importancia para el funcionamiento económico y político de Estados Unidos, por lo que es un tema muy importante y significativo para estudiar Relaciones Internacionales, ya que analiza y explica cómo van a operar los Estados de acuerdo a las medidas de ciberseguridad implementadas por EE.UU. a través de agencias de inteligencia con el fin de lograr superar los desafíos que obstaculicen la dinámica armónica, económica y política, debido a que las relaciones diplomáticas que ha tenido Estados Unidos con los demás Estados se han establecido a partir del espionaje por las distintas agencias de inteligencia, seguridad, por el Secretario de Estado y también por medio de reportes de embajadores de EEUU.

El tema de ciberseguridad en Estados Unidos es factible para ser estudiado por un internacionalista, ya que involucra la política nacional estadounidense y cómo el Estado toma decisiones en el escenario internacional con sus amigos, enemigos y posibles amenazas de grupos terroristas, en este ámbito un internacionalista tiene las herramientas necesarias para explicar los acontecimientos internos y externos de Estados Unidos, debido a la formación multidisciplinaria que se adquiere a lo largo de la licenciatura.

El tema de ciberseguridad es viable para investigación, porque está vigente hoy en día con ataques cibernéticos y filtraciones de documentos clasificados para desequilibrar a Estados Unidos lo que puede desembocar en guerras a través de las redes tecnológicas.
El objetivo general de esta tesis es: Analizar las medidas de ciberseguridad que se implementaron a partir de la vulnerabilidad en el hackeo y espionaje sobre información clasificada durante la primera administración del presidente Barack Obama 2009-2012.

Los objetivos particulares de esta tesis son:

a. Conocer las amenazas en el ciberespacio y los actores internacionales que están involucrados en la implementación de las medidas de ciberseguridad para reducir ataques cibernéticos.
b. Explicar los antecedentes de los ataques cibernéticos en Estados Unidos y las repercusiones en la implementación de los programas de ciberespionaje.
c. Analizar las medidas de Seguridad Nacional junto con las alianzas estratégicas del sector privado para implementar herramientas de inteligencia y contrarrestar vulnerabilidades en el hackeo de información clasificada.
d. Explicar las medidas de ciberseguridad y las repercusiones en el escenario internacional por las operaciones de ciberespionaje por parte de las agencias de inteligencia de Estados Unidos.

La hipótesis de la presente investigación parte de la siguiente premisa: La vulnerabilidad en el ciberespacio es un problema que enfrenta Estados Unidos al no haber una regulación en el sistema internacional para enfrentar ataques cibernéticos, por lo que a partir de la primera administración de Barack Obama (2009-2012), EEUU ha intensificado las medidas de ciberseguridad que fueron implementadas durante la administración de George W. Bush para controlar ataques y acciones de espionaje por grupos terroristas, después de los atentados del 11 de Septiembre de 2001 que afectaron el desarrollo económico, político y social estadounidense.

En la siguiente premisa se pretende demostrar el impacto de las medidas de ciberseguridad hacia la comunidad internacional, mediante programas de ciberespionaje implementados por las agencias de inteligencia; provocando desconfianza entre los Estados por las prácticas de vigilancia que no solo están enfocadas en la búsqueda de grupos terroristas, afectando las relaciones diplomáticas con EEUU por los métodos de espionaje invasivos a la soberanía de los Estados.

La presente investigación se explicará y se desarrollará mediante la teoría de la globalización:

El término globalización se puede definir como: “Un movimiento planetario en que las sociedades renegocian su relación con el espacio y el tiempo por medio de concatenaciones que ponen en acción una proximidad planetaria bajo su forma territorial (el fin de la geografía), simbólica (la pertenencia de un mismo mundo) y temporal (la simultaneidad)”[4]

La globalización explica e interpreta los acontecimientos internacionales de acuerdo al desarrollo de cada Estado, así como su economía, sus influencias culturales, educativas y políticas, a través de las cuales se van a definir los sistemas de comunicación internacional donde las fronteras parecen dejar de tener significado y el tiempo porque puede adquirir notoriedad mundial en segundos.

De acuerdo al autor Giovanni E. Reyes:

> “El uso de novedosos procesos tecnológicos, permite una mayor interacción entre instituciones, gobiernos, entidades y personas alrededor del mundo, por lo que los sistemas de comunicación global adquieren una creciente importancia en la actualidad, debido a la interacción entre los Estados, grupos sociales y las personas que interactúan de manera más fluida tanto a nivel nacional como en el entorno internacional, volviéndose el ciberespacio un gran campo de espionaje y una amenaza latente para la seguridad nacional.”[5]

La teoría de la globalización, se enfoca principalmente en un sistema internacional de interdependencias, donde todo el mundo está interconectado por medios de comunicación, como es el uso del ciberespacio que está al alcance de cualquier persona para desarrollar actividades de la vida cotidiana, lo cual representa un peligro para los Estados, debido a que los usuarios no tienen los estándares de

[4] Cruz Soto Luis Antonio, Hacia un concepto de globalización, Revista Contaduría y Administración, No. 195, Ed. Facultad de Contaduría y Administración, UNAM, México, Octubre diciembre 1999, p. 37, disponible en línea: http://www.ejournal.unam.mx/rca/195/RCA19504.pdf, Fecha de consulta: 21 de Noviembre de 2017.

[5] E. Reyes Giovanni, Teoría de la globalización: Bases fundamentales, Revista de la Facultad de ciencias Económicas y administrativas, Vol. II, No.1, Universidad de Nariño, Colombia, 2001, p. 46.

seguridad adecuados provocando debilidad en la infraestructura informática, por lo que las relaciones internacionales se ven frágiles a partir de las interacciones de los actores estatales y no estatales.

Esta teoría no sólo involucra la relaciones de poder vinculadas a los Estados en el escenario internacional, sino que también toma en cuenta a los actores que se desenvuelven en actividades políticas, comerciales, económicas, delictivas y terroristas; para los globalistas todo se resume en una red de interacciones entre los Estados y las Organizaciones Internacionales por medios de comunicación más rápidos y seguros en los cuales se implementan aplicaciones de seguridad eficientes y poco vulnerables, debido a los errores de diseño en los software y el uso de internet por el cual se pueden filtrar virus en redes vulnerables o programas de interrupción de actividades que se convierten una vía fácil para los hackers para cometer actos terroristas, motivados principalmente por defender sus ideologías religiosas y culturales de políticas de occidente, las actividades que realizan para desestabilizar un país es la: desfiguración de páginas gubernamentales, amenazas a líderes políticos o penetrar a ordenadores y filtrar documentación oficial por medidas de espionaje en el ciberespacio, que muchas veces viola la privacidad de los usuarios y la soberanía del Estado.

De acuerdo a Juan Camilo Restrepo, define la teoría de la globalización de la siguiente manera:

> La teoría de la globalización enfoca su análisis en un sistema internacional de interdependencia, pues las Relaciones Internacionales se mueven a partir de las interacciones de gran cantidad de actores además de los Estatales.[6]

En este sentido, la teoría de la globalización se adapta a la presente investigación, debido a que esta teoría se enfoca a las interdependencias entre los Estados para un buen funcionamiento en el resguardo de la seguridad nacional y la ciberseguridad en el ciberespacio donde las fronteras son inexistentes por medio

[6] Restrepo Vélez, Juan Camilo., La Globalización en las Relaciones Internacionales: Actores internacionales y sistema internacional contemporáneo, Facultad de Derecho y Ciencias Políticas, Medellín Colombia, 2013, p.635.

del uso de internet, donde un Estado se vuelve más vulnerable a un ataque anónimo en la infraestructura informática.

Para la elaboración de esta tesis, se utilizara los métodos de investigación descriptivo y analítico.

El método descriptivo se utilizará para describir y explicar las medidas, estructuras, y dinámicas que utiliza Estados Unidos para proteger su infraestructura informática para contrarrestar ataques cibernéticos y minimizar riesgos en la transferencia de datos y que puedan ser interceptados por hackers.

También se hará recopilación de datos, por medio de libros, revistas especializadas, paginas oficiales de la CIA, NSA, White House, WikiLeaks, y seguimiento en notas periodísticas por los distintos medios de comunicación, para tener una mejor comprensión del tema a partir de la explicación de los antecedentes, causas y los efectos que provoca en el escenario internacional.

En segunda instancia se utilizará el método analítico para disolver y separar el origen de la problemática, para ir reestructurando la información a partir de la observación y explicación de las causas y efectos a nivel nacional e internacional.

En el primer capítulo se abordará el marco teórico- conceptual y se explicaran los antecedentes que dieron origen a los avances tecnológicos para la seguridad nacional con el lanzamiento del primer satélite llamado Sputnik por la Unión Soviética, este avance tecnológico significó un parte aguas para la protección de la información en el ciberespacio, donde las fronteras físicas se vuelven imaginarias, así mismo se abordara la teoría de la globalización con la cual se podrá explicar el tema de la presente investigación.

En adición se explicarán las amenazas emergentes como es el uso de virus para penetrar en las vulnerabilidades de la infraestructura cibernética y se analizará la postura de los organismos internacionales para llevar acciones junto con el gobierno para un buen funcionamiento de la ciberseguridad en el ciberespacio mediante el uso de internet y los protocolos de seguridad que se han

implementado para evitar filtraciones en el ámbito político, social, económico y militar; Por último en este capítulo se explicará el origen del espionaje y ciberespionaje.

En el segundo capítulo se realiza un recuento histórico de los ataques cibernéticos durante la primera administración de Barack Obama y las medidas de seguridad cibernética a partir de los atentados terroristas del 11 de septiembre con la administración de George W. Bush, de igual manera se analizará, las estrategias de cibeseguridad a partir de los ataques cibernéticos a la infraestructura critica estadounidense.

Por otro lado en el segundo capítulo se analizará las alianzas estratégicas que tiene el gobierno norteamericano con las empresas para proteger la infraestructura crítica del país.

Por ultimo en el segundo capítulo se analizarán las filtraciones en el portal WikiLeaks y como se conforma la organización empezando desde su fundador Julián Assange y las acciones que tomó el gobierno estadounidense para evitar posibles infiltraciones. El propósito de este capítulo es conocer la dinámica en la agenda de seguridad nacional norteamericana y comprender las limitaciones de las agencias de inteligencia en el ciberespacio para enfrentar ataques cibernéticos y filtración de documentos clasificados.

En el tercer capítulo se analizarán las acciones de ciberseguridad y se abordaran los sistemas de ciberespionaje por las agencias de inteligencia y las repercusiones en el ámbito diplomático al filtrarse información en diarios internacionales que obtuvieron la información por medio del ex agente de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA) Edward Snowden.

También se explicará el combate contra el ciberterrorismo por parte de Estados Unidos y los principales grupos terroristas que atentan a su Seguridad Nacional y las medidas que se están adoptando para contrarrestar y neutralizar ataques de hackers pertenecientes a las células terroristas que tienen como finalidad provocar desestabilización en los sectores económicos políticos y sociales.

CAPÍTULO I: TEORÍA DE LA GLOBALIZACIÓN Y MARCO CONCEPTUAL DE CIBERSEGURIDAD: NUEVAS AMENAZAS A LA SEGURIDAD INTERNACIONAL.

1.1 Teoría de la globalización

Las teorías dentro de las Relaciones Internacionales ayudan a explicar hechos concretos de la realidad de acuerdo a la esencia de un conflicto político, económico o social asimismo nos apoyan a comprender la configuración del Estado-Nación de acuerdo al grupo de poder que este al mando y cómo van a solucionar las exigencias de las nuevas amenazas con el uso de tecnología de punta.

La teoría de la globalización que propone Keohane y Nye también se le conoce como globalismo, "enfoca su análisis en un sistema internacional de interdependencias, pues las relaciones internacionales se mueven a través de las interacciones de gran cantidad de actores además de los estatales."[7]

El sistema globalista o trasnacionalista no solamente involucra las relaciones de poder vinculadas a los Estados, en dicho escenario también participan todo tipo de actores cuyas acciones giran en torno a las actividades económicas, comerciales, políticas y financieras.

La globalización es un fenómeno que se manifiesta a partir de los años ochenta del siglo XX, debido al desarrollo de los medios de comunicación, agilización de aspectos financieros y comerciales.[8]

La teoría que se abordará en la presente investigación es la teoría de la globalización, para comprender el papel del Estado en el escenario internacional a partir de cómo se desenvuelven las relaciones bilaterales y multilaterales, tomando

[7] Restrepo Vélez Juan Camilo, La globalización en las relaciones internacionales: actores internacionales y sistema internacional contemporáneo, Ed. Facultad de Derecho y Ciencias Políticas, Vol. 43, No. 199, Enero- Junio, Colombia, 2013, p. 635.
[8] Gambrill Mónica, La globalización y sus manifestaciones en América del Norte, Ed. Centro de Investigaciones sobre América del Norte, México, 2002, p.29.

en cuenta las fuerzas sociales internas y externas de poder y la revolución de las computadoras con acceso a internet logrando una interconexión más rápida y cómoda para el ser humano.

La teoría de la de globalización, explica e interpreta los acontecimientos internacionales de acuerdo al desarrollo de cada Estado, así como su economía, sus influencias culturales, educativas y políticas, a través de las cuales se definen los sistemas de comunicación internacional que se relacionan con los flujos de información y comunicación.

Con la globalización se rompen fronteras nacionales atravesando tanto regímenes políticos y culturales debido al uso de recursos tecnológicos se establecen nuevas directrices en el sistema internacional a partir de las condiciones y posibilidades de cada Estado para adaptarse a la nueva reorganización mundial.

Los aspectos que estudia la corriente teórica de la globalización se refieren a:

- Integración en los diferentes niveles de poder, tanto dentro como entre las naciones, y en términos comparativos, con las diferentes modalidades de integración y marginación que ocurren a nivel mundial.
- Formas dinámicas, mediante las cuales los nuevos patrones de comunicación están afectando a los grupos minoritarios dentro de las sociedades.

Los aspectos que estudia la globalización implican una integración tanto de los Estados, instituciones, empresas, ONG´s y la sociedad internacional para evitar asimetría en las diferentes regiones del mundo, afectando la interconectividad y dinamismo de los flujos de información entre las Naciones mediante la tecnología, provocando vulnerabilidades en el ciberespacio al no tener accesibilidad a mecanismos confiables de comunicación.

En los últimos años el término de globalización se utiliza en relación a la revolución tecnológica en las comunicaciones y la creación del ciberespacio, para

entender mejor la teoría de la globalización, David Held y Antony McGrew definen el concepto de globalización:

> "La globalización designa un proceso acelerado, qué impacta en los flujos y patrones transcontinentales de interacción social. La globalización remite a un cambio o transformación en escala de la organización humana que enlaza comunidades distantes y expande el alcance de las relaciones de poder a través de regiones y continentes de todo el mundo"[9]

El concepto de globalización trae consigo cambios y transformaciones de acuerdo a la interacción de la sociedad, a partir del concepto de globalización se desprende la definición de sociedad global de acuerdo al autor Octavio Ianni, donde explica que el ser humano está desplazándose a diferentes partes del globo terráqueo mediante el uso de la tecnología en instantes:

> La sociedad global se constituye en la época de la electrónica, dinamizada por los recursos de la informática. Este es, también, un motivo que explica porque la sociedad global se muestra visible e incógnita, presente y fugas, real e imaginaria. Ella está articulada por emisiones, ondas, mensajes, signos, símbolos, redes y alianzas que tejen los lugares y las actividades, los campos y las ciudades, las diferencias y las identidades, las naciones y las nacionalidades.[10]

Debido a los diferentes recursos con los que cuenta la sociedad global, con el uso de las tecnologías de la información y comunicación (TIC´s), la ciberseguridad cobra mayor relevancia para la seguridad de las naciones por medio de la supervisión de la entrada y salida de la información digital así como la protección de ataques a los sistemas informáticos provocando una desestabilización en el desarrollo de país.

Con la sociedad global, la globalización construye un nuevo enfoque de acuerdo al presente, en el cual las fronteras son modificadas o anuladas y la soberanía se diluye a través del tiempo, debido a las "fuerzas que operan hacia la mundialización, inmediatamente emergiendo provincialismos, nacionalismos, regionalismos, etnicismos, fundamentalismos, que expresan tanto reivindicaciones

[9] Held D. y McGrew A., Globalización/Antiglobalización. Sobre la reconstrucción del orden mundial, Ed. Paidós, Barcelona, 2003, p.13.
[10] Ianni Octavio, La era del globalismo, Ed. Siglo Veintiuno Editores, s.a. de c.v. , España, 1999, p.27.

e identidades antiguas como la decadencia del Estado-Nación como instituto de soberanía.” [11]

En relación al desarrollo asimétrico de los grupos sociales, la sociedad global se ha organizado de acuerdo a su entorno geográfico, tomando en cuenta sus costumbres, su religión, su cultura, lo cual han formado su ideología de acuerdo al entorno en el que se desenvuelven, donde los actores internacionales fuertes y desarrollados, son los que predominan en la organización de la sociedad, formando una aldea global donde se incluye a países subdesarrollados provocando asimetrías debido a que no cuentan con la infraestructura tecnológica necesaria, volviendo el ciberespacio un campo de batalla difícil de manejar.

Para comprender mejor la inclusión mediante una “aldea global”, se citará el siguiente concepto:

“El término de “aldea global” sugiere que, finalmente, la formación de la comunidad mundial, concretada en realizaciones y las posibilidades de comunicación, información y fabulación abiertas por la electrónica. Sugiere que están en curso de armonización y la homogenización progresiva.”[12]

Como se menciona anteriormente el concepto de “aldea global”, se fundamenta en la existencia de una organización, la cual se basa en el funcionamiento colectivo que estimula un cambio de vida social en constante actualización el cual es provocado por la globalización; lo que ocasiona el uso de medios electrónicos para la difusión de información, que rápidamente las naciones y regiones, son permeadas y articuladas por los medios de comunicación y manipuladas por actores internacionales de gran envergadura como son las organizaciones gubernamentales, Estados nacionales, grupos terroristas y delincuentes que pueden actuar desde cualquier parte de la tierra provocando interdependencia entre las naciones.

[11] Ibídem, p. 28.
[12] Ibídem, p. 5.

Las características más significativas de la globalización se pueden resumir en el siguiente punto:

Los sistemas de comunicación global: Estos adquieren una creciente importancia en la actualidad, gracias a lo cual las naciones, grupos sociales y personas están interactuando de manera más fluida, tanto dentro, como entre las naciones.

Pese a que los sistemas más avanzados de comunicaciones se concentran en las naciones más desarrolladas, estos hacen sentir sus efectos en las naciones menos avanzadas. Esta situación permite que los grupos marginales de los países más pobres, puedan comunicarse e interactuar dentro del contexto global, usando las nuevas tecnologías y, por consiguiente, pueden integrarse con la “aldea global”, que representa el actual escenario de las comunicaciones.

La teoría de la globalización se dirige en un sistema internacional de interdependencias, donde todo el mundo está interconectado por medios de comunicación al alcance de cualquier Estado u empresa, lo cual representa un peligro por no tener los estándares de seguridad adecuados, provocando debilidad en la infraestructura informática, por lo que las relaciones internacionales se ven frágiles y vulnerables a partir de las interacciones de los actores estatales y no estatales. Esta teoría no solo involucra las relaciones de poder vinculadas a los Estados en el escenario internacional, sino que también toma en cuenta a los actores que se desenvuelven en actividades políticas, comerciales, económicas, militares, delictivas y terroristas.

Para los globalistas todo se resume en una red de interacciones entre los Estados y Organizaciones Internacionales por medios de comunicación más rápidos y seguros en los cuales se implementan aplicaciones de seguridad eficientes y poco vulnerables, debido al uso de internet por el cual se pueden filtrar virus en redes vulnerables.

1.2 Marco conceptual

El marco conceptual que se utilizará en la presente investigación se conforma por los conceptos de seguridad internacional, ciberseguridad, ciberespacio, ciberataques, ciberterrorismo, ciberguerra, ¿Qué es un Hacker? y la definición de política exterior, para entender el planteamiento de la presente investigación, a continuación se desglosan las definiciones de los conceptos antes mencionados para una mejor interpretación del tema.

La seguridad internacional ha influido a través de los años para que los Estados delimiten su política exterior de acuerdo a las amenazas o agresiones a las que estén expuestos, otro factor que se determina es la dinámica de cómo van a actuar los Estados en el escenario internacional para proteger y resguardar su soberanía.

A lo largo del tiempo ha cambiado la forma en que la gente se comunica hoy en día, lo que representa desafíos para la seguridad nacional estadounidense, la ciberseguridad surge por la necesidad de concientizar a la población de protección en el espacio cibernético debido a que las amenazas digitales se transmiten desde cualquier ordenador utilizando robo de identidades y por ende es fácil para la mafia de hackers entrar a los sistemas operativos sin ser detectados para obtener información y utilizar armas cibernéticas para introducir programas o virus que colapse la red nacional y permitirles acceder a los ordenadores para cometer actos de espionaje.

1.2.1 Ciberespacio

Concepto de Ciberespacio: De acuerdo a George Kortopoulos “El ciberespacio es una parte integral de la sociedad estadounidense y una infraestructura muy importante para todos los aspectos de la vida.”[13] Derivado a esto el autor propone adoptar una estrategia global de seguridad nacional, así como aumentar el número y la cantidad de profesionales de la seguridad cibernética.

[13] K. Kostopoulos George, Cyberspace and Cybersecurity, Ed. CRC Press Taylor Francis Group editor, United States, 2013, p.159.

El ciberespacio se mueve por la interacción del ser humano mediante internet, el cual ha sido una herramienta con una gran importancia y valor para los Estados Unidos, para prevenir futuras amenazas o ataques terroristas debido a la inseguridad de esta red de comunicación de fácil acceso para burlar los sistemas de seguridad por los hackers.

El ciberespacio es un medio que avanza rápidamente, en el cual se puede interactuar desde cualquier espacio del planeta, “es un lugar donde se mueve la sociedad virtual, donde se modifica la percepción espacio-tiempo; los usuarios, los actores, los observadores de la sociedad virtual crecen exponencialmente y clarifican sus derechos , los comparten y los refuerzan; el ciberespacio se vuelve un terreno educativo, de investigación, de transacciones comerciales y de mercado, de política económica, de denuncia, de lucha social y de crimen.”[14]

Antes era imposible pensar en la existencia de un mundo virtual, hoy en día es una parte fundamental para la vida humana, con el uso de las redes sociales, correos electrónicos, páginas web, foros y tiendas en línea, la forma de interacción del ser humano ha cambiado, convirtiéndose en un medio de interacción paralelamente con el mundo físico.

De acuerdo a Luis Joyanes Aguilar, define el ciberespacio como “un conjunto o realidad virtual donde se agrupan usuarios, páginas web, chat y demás servicios de internet además de otras redes.”[15]

El ciberespacio es un nuevo escenario dinámico en el sistema internacional por su fácil alcance y rapidez en la comunicación entre individuos, sin embargo tiene vulnerabilidades que son utilizadas para infringir daño a cualquiera en el planeta sin ser detectado por medio de las plataformas electrónicas.

[14] Alfredo A. Reyes Krafft, “Ciberespacio y sociedad”, Seguridad y defensa en el ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p.11.
[15] Aguilar Joyanes Luis, “Introducción Estado del arte de la ciberseguridad”, Ciberseguridad Retos y amenazas a la seguridad Nacional en el Ciberespacio, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, España, 2010, p. 29.

Del mismo modo el ciberespacio se ha convertido en un hábitat para la sociedad, creando una vida paralela, una codependencia en el uso de dispositivos electrónicos en los cuales comparten información sin tomar en cuenta los riesgos en la transmisión de información, por ejemplo: Las vulnerabilidades se pueden ocultar en los datos, en códigos, y más a menudo en procesos que descuidadamente permiten acceso que no es autorizado como es el uso de intranet, donde la mayoría de las veces la seguridad no es tan fuerte.

"En el documento nombrado Directiva Presidencial de Seguridad Nacional número 54 de 2006"[16], se menciona al ciberespacio como red interdependiente de infraestructuras de tecnología de la información, la cual engloba internet, las redes de telecomunicaciones, los sistemas de computadoras (Software), y los procesadores y controladores incluidos en industrias fundamentales (Hardware).

"En 2008 el Subsecretario de Defensa de Estados Unidos: Gordon England, definía como ciberespacio el dominio global dentro de un ambiente de información constante de redes interdependientes de infraestructuras de tecnologías de la información, incluyendo internet, redes de telecomunicaciones, sistemas de computadoras, procesadores y controladores incluidos."[17]

De acuerdo al artículo: Ciberdefensa Activa: Mejorando la Ciberseguridad; la Doctora Elena Jeannetti Dávila define las características del ciberespacio en el cual se deben de adoptar medidas de prevención y protección del Estado:

- El ciberespacio es un entorno único, en el que el atacante puede estar en cualquier parte del globo y es difícil localizarlo.
- La confrontación en el ciberespacio presenta frecuentemente las características de un conflicto asimétrico; y es frecuentemente anónimo y clandestino.
- Permite obtener información sobre objetivos sin necesidad de destruir ni neutralizar ningún sistema, y a menudo sin dilatarse.

[16] Gregory J. Rattray, Strategic Warefare in Cyberspace. Defining the problem, Ed. MIT Press, Washington D.C., 2009, pp.26-27.
[17] Ídem.

- El ciberespacio no puede considerarse aisladamente a efectos de la defensa puesto que esta interrelacionado estrechamente con los demás espacios.[18]

Para la seguridad Internacional el uso de redes impacta en las áreas económicas, políticas, sociales y militares, que forman parte de la seguridad de un Estado, a causa de los riesgos en las redes, el departamento de seguridad nacional de los Estados Unidos mantiene un extenso equipo de preparación para emergencias, los especialistas en informática advierten a los ciudadanos de la existencia de vulnerabilidades en los software que son ampliamente utilizados, la National Security Agency divide los ciberataques de acuerdo a la magnitud del riesgo (véase en anexo 3).

Las estrategias de ciberseguridad marcadas durante la primera administración de Barack Obama entre los periodos de 2009 y 2010, fueron posteriormente retomadas por el subsecretario de defensa William J.Lynn, estableciendo cinco principios básicos para tomar en cuenta en las siguientes estrategias de ciberseguridad y confrontar las amenazas en el futuro en el ciberespacio:

- El ciberespacio debe de ser reconocido como un territorio de dominio igual que la tierra, mar y aire en lo relativo a la guerra.
- Cualquier posición defensiva debe de ir más allá del mero mantenimiento del ciberespacio (limpio de enemigos) para incluir operaciones sofisticadas y precisas que permitan una reacción inmediata.
- La defensa del ciberespacio (ciberespacial) debe de ir más allá del mundo de las redes militares-dominio.mil y.gov. del Departamento de Defensa, para llegar hasta las redes comerciales (dominios.com, .net, .info, .edu, etc.) y que deben estar subordinados al concepto de Seguridad Nacional.

[18] Jeannetti Dávila Elena, “Ciberdefensa Activa: Mejorando la Ciberseguridad”, Seguridad y Defensa en el Ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p. 193.

- La estrategia de Defensa Ciberespacial debe de realizarse con los aliados internacionales para una política efectiva de (alerta compartida) ante las amenazas mediante establecimiento de ciberdefensas con países aliados.
- El Departamento de Defensa debe de contribuir al mantener e incrementar el dominio tecnológico de Estados Unidos y mejorar el proceso de adquisiciones y mantenerse al día con la agilidad que evoluciona la industria de las tecnologías de la información.[19]

Los cinco principios básicos antes mencionados, muestran un panorama amplio sobre las técnicas de guerra que van evolucionando rápidamente, convirtiendo al ciberespacio en una bomba de tiempo si los gobiernos no toman las medidas necesarias para protegerse de los riesgos en la infraestructura crítica de cada país, por lo cual se deben de tomar acciones con aliados internacionales para evitar que se propaguen los ataques cibernéticos.

Es necesario recalcar que la interdependencia entre las naciones incita a involucrarse en las actividades de seguridad para evitar posibles amenazas, debido a que no todos los Estados cuentan con el desarrollo tecnológico para emplear operaciones de defensa.

En general, existen soluciones de seguridad pero son insuficientes debido al crecimiento acelerado de los sistemas de comunicación, donde se utilizan herramientas las cuales se vuelven inoperables por los gobiernos, porque:

- Se utilizan herramientas que rápidamente se ven desplazadas por lo que no se analiza, el proceso y la gestión de estos.
- Las herramientas no son efectivas y son suficientemente flexibles, los que las vuelve fácil de manipular.
- Las herramientas ofrecen una respuesta estática y específica a un problema dinámico y global.

[19] Aguilar Joyanes Luis, “Introducción Estado del Arte de la ciberseguridad”, Ciberseguridad Retos y amenazas a la seguridad Nacional en el Ciberespacio, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, España, 2010, p.31.

- Existen normas o recomendaciones internacionales de seguridad, que no se les ha dado gran difusión para que haya mejor capacitación en el uso de dispositivos y en el uso de las redes de la información.
- También se pueden encontrar disposiciones legales que han sido especificadas por personas que no tienen el conocimiento de los medios tecnológicos.[20]

Otro factor importante es la asimetría en los conflictos de acuerdo a la capacidad de cada Estado, en el ámbito político, económico, tecnológico y militar, por lo que la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés) propone que las naciones desarrolladas deben de poner énfasis en el desarrollo de medidas de ciberseguridad y no desestimar la capacidad de cada país por mínima que sea, por lo que es necesario:

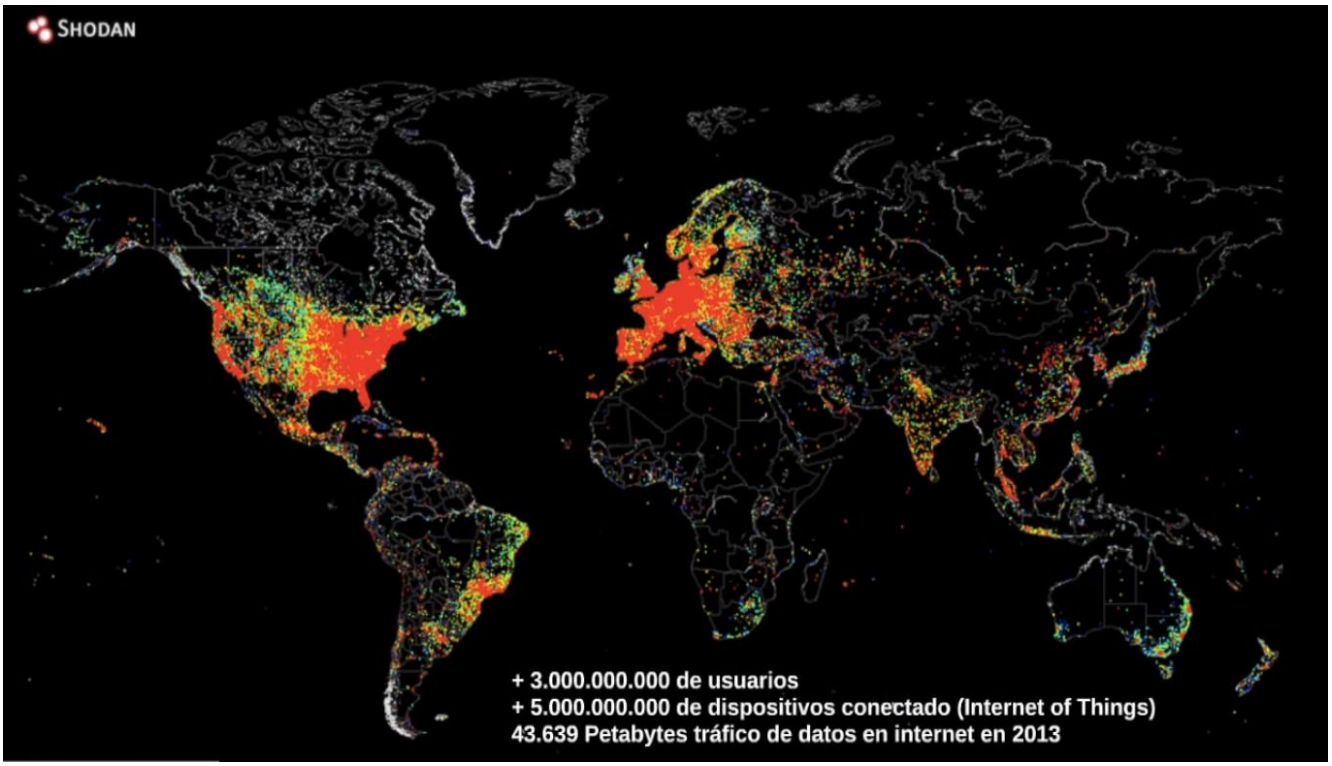
> "Asegurar la necesaria cooperación internacional, mediante el establecimiento de los acuerdos correspondientes y la implantación de los instrumentos necesarios.
> Dotarse de las impredecibles capacidades en materia de inteligencia, orientadas a una detección temprana y a una valoración inequívoca de las capacidades y posibles actitudes del adversario.
> Ejercer el esfuerzo necesario en alcanzar y mantener una adecuada conciencia nacional, que garantice la cohesión de la propia sociedad, y de esta con sus instrumentos de defensa."[21]

Prácticamente del 50% de la población mundial, más de 3 mil millones de usuarios están conectados permanentemente en el ciberespacio, donde hay más de 5 mil millones de dispositivos conectados de los cuales ocupan alrededor de 43, 639 petabytes[22] para el tráfico de datos en internet (imagen 1), en este punto se puede observar como la hiperconectividad ha cambiado la interacción del ser humano gracias a la globalización, donde las fronteras no existen en el ciberespacio y no se sabe hasta dónde puede llegar a iniciar y terminar la jurisdicción de un país, teniendo interacción en el mundo físico, por lo cual debe de haber una mayor

[20] Ghernaouti Solange, Cyberpower, crime, conflicto and security in cyberespace, Ed. CRC Press, EE.UU, 2006, p. 335.
[21] Ibídem, p. 268.
[22] Un petabyte es una unidad de medida de almacenamiento de información equivalente a 1, 000, 000,000, 000, 000 bytes.

cooperación internacional para enfrentar las amenazas de manera rápida y precisa.

Imagen 1 Hiperconectividad en el ciberespacio



Fuente: International Telecommunicatios Union (ITU), ciberespacio, 2014.

En referencia a la hiperconectividad en el ciberespacio, crece aceleradamente; el ingeniero informático Adolfo Hernández Lorente, propone que las medidas de ciberseguridad deben de ir encaminadas hacia un trabajo en equipo con los demás países, para evitar las vulnerabilidades cibernéticas en el ciberespacio, debido a que es un "terreno intangible" y poco conocido que avanza rápidamente por lo cual se necesita establecer reglas en el escenario internacional sobre el uso y manejo que le da cada usuario.

1.2.2 Internet

Actualmente internet es una herramienta importante en la vida cotidiana del ser humano, convirtiéndose en una necesidad de la sociedad de la información. Se considera como una infraestructura crítica esencial de cada Nación, porque su nivel de importancia determina la supervivencia de quienes dependen de ella.

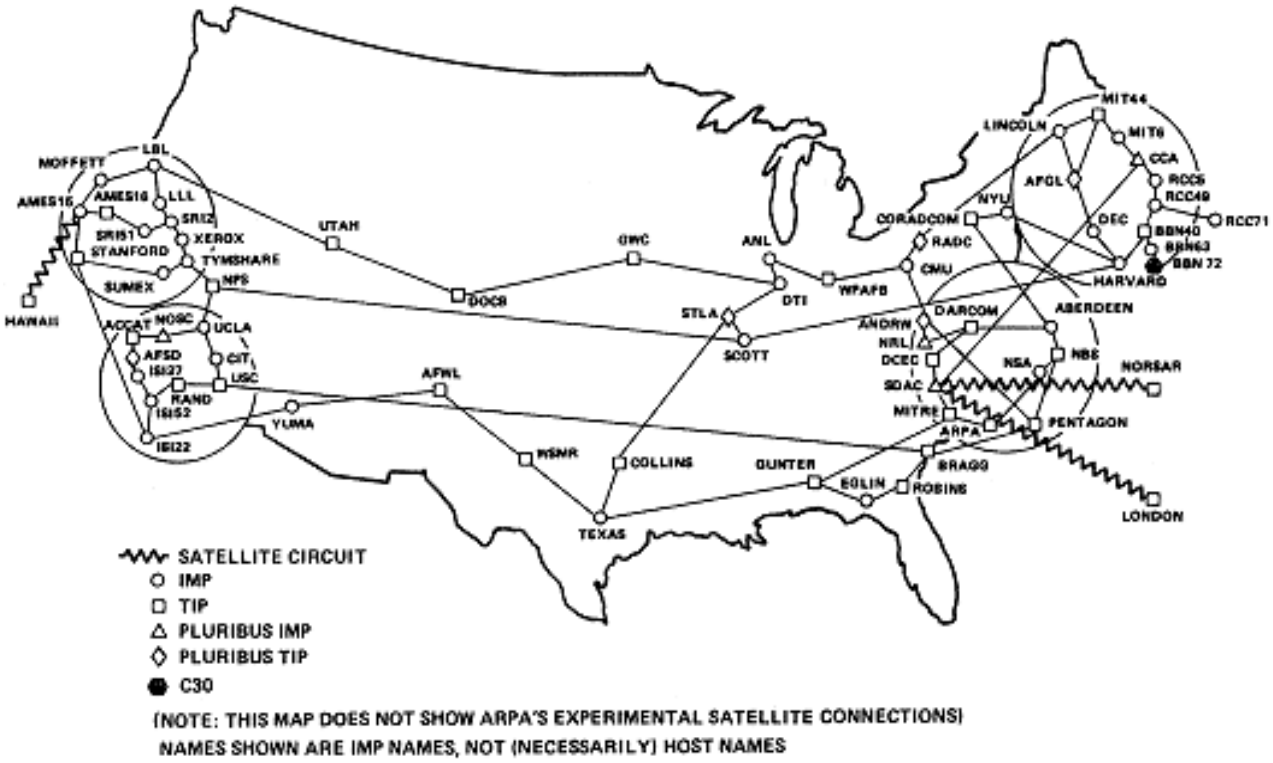
De acuerdo a la definición de la Real Academia Española, “internet es una red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de la comunicación.”[23]

La estructura de internet se caracteriza como una red integrada por miles de redes y computadoras entrelazadas entre sí a nivel mundial que sirven como medio de transferencia de datos y de comunicación, por medio de las redes la sociedad virtual se puede conectar desde cualquier punto facilitando la interacción entre los individuos.

Sin embargo antes de convertirse internet en una red mundial interconectada entre cualquier computadora del mundo, solo su uso estaba restringido para fines militares por parte del gobierno Estadounidense, con el proyecto ARPANET (*Advanced Research Project Agency Net* por sus siglas en inglés), el cual era una red sin servidores centrales, ya que disponían de varias rutas que estaban principalmente en universidades, donde se podían alternar las comunicaciones, por si eran atacados y no pudieran perder la comunicación, debido a las ventajas de interconexión, el proyecto ARPANET se fue popularizando en diversas instituciones y universidades internacionales avanzando rápidamente en el país debido a su gran eficacia aunque si tuvo algunos errores que posteriormente se fueron arreglando de acuerdo a la vulnerabilidad que representaba en las actividades de inteligencia militar(Imagen 2).

[23] Real Academia Española (RAE), Diccionario de la lengua Española, Disponible en línea: http://www.rae.es/, Fecha de consulta: 09 de Agosto de 2017.

Imagen 2 ARPANET 1980



Fuente: Aranda T. Vicente, Historia y evolución de Internet, Manual Formativo de ACTA, 2004, p.2.

Es hasta 1982, cuando el proyecto ARPANET se "[…] declaró como estándar el protocolo TCP/IP (*Transfer Control Protocol/Internet Protocol*) y es entonces cuando aparece la primera definición de internet: "conjunto de internets" conectadas por TCP/IP."[24]

El objetivo de este protocolo era facilitar la comunicación entre los ordenadores de las divisiones de las fuerzas armadas en sus operaciones militares, sin embargo no era tan fiable este sistema, por la interceptación de datos.

"Debido a la poca seguridad que brindaba el proyecto ARPANET en 1983, el Departamento de Defensa de Estados Unidos, abandonó el proyecto y estableció una red independiente llamada MILET"[25], destinada exclusivamente a cuestiones

[24] Aranda, T. Vicente, Historia y evolución de Internet. 2004, Manual formativo de ACTA, disponible en línea: https://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf, España 2004, p.2, Fecha de consulta 10 de Abril de 2017.
[25] Ídem

militares y ARPANET se sustituyó por el protocolo TCP/IP, que paso a unir servidores de todo el mundo con el fin de la investigación militar; y en "[…] 1983 también se creá la red CSNET con fines académicos"[26].Con la colección de redes que gradualmente se iban desarrollando, se empieza a llamar "internet".

A inicios del siglo pasado se empezó a popularizar el uso de internet en las universidades y el proyecto adquirió mayor madures en el ámbito internacional para formar una red global, es cuando aparece el concepto de "World-Wide-Web"[27]

"Tim Berns Lee fue el precursor del concepto "World-Wide-Web", basado en un documento HTML que es almacenado en un servidor y se conecta a la web, este gran paso convirtió la navegación por la red en algo sencillo gracias a sus programas "point-and-click"[28]. En 1991, gracias a la facilidad de manejo que supuso la implantación de la "web", los proveedores de servicio de conexión a Internet ganaron popularidad"[29]

Mark Andreessen, de la Universidad de Illinois, lanza el buscador "Mosaic" [30], un revolucionario navegador, que ayudo a difundir internet como una herramienta dominante en el sector empresarial, político y principalmente comercial.

Con relación en el crecimiento de uso de páginas web dentro de la red, el uso de internet se convierte en algo cotidiano e inseguro, que dificulta la regulación de su uso apropiado por los ataques cibernéticos que pueden provenir de cualquier parte del mundo de manera anónima, provocando un problema de seguridad.

Uno de los problemas más importantes en el uso de internet es la interconectividad desde cualquier parte del mundo, que se vuelve más difícil de

[26] Canay Pazos J. Raúl, El uso de entornos virtuales de aprendizaje en las universidades presenciales: Un análisis empírico sobre la experiencia del campus virtual de la USC, Ed. Universidad de Santiago de Compostela, España, 2008, p.49.
[27] Nebreda Rodrigo Iván, El origen de Internet. El camino hacia las redes, Ed. DIATEL, 2013, disponible en línea: http://oa.upm.es/22577/1/PFC_IVAN_NEBREDA_RODRIGO.pdf, Fecha de consulta: 10 de Abril de 2017.
[28] Es la acción de pulsar cualquier botón o tecla del dispositivo de la computadora que implique la función de señalar con un cursor determinado objeto.
[29] Ibídem, p.84.
[30] Ibídem, p. 89.

rastrear a personas que cometen actos ilícitos como es penetrar en la infraestructura cibernética y manipular los dispositivos de acuerdo a sus intereses, ejemplo de ello son los grupos terroristas que buscan la desestabilización de Estados Unidos mediante ataques focalizados a la infraestructura crítica.

El uso de internet como herramienta cotidiana para el ser humano ha logrado cambios socioculturales que ha impactado en el mundo, un ejemplo de ello es la interconectividad, sin embargo "solo el 16 % de internet es utilizado por la sociedad internacional, mientras el 84% considerado como internet profundo es utilizado para actividades ilegales, donde las personas que interactúan en este nivel de la red tienen amplios conocimientos del ciberespacio."[31]

"Las cifras antes mencionadas nos hablan sobre una descentralización del uso de internet, donde nadie gobierna o regula la red, lo que conlleva a cada red que se encuentra en el ciberespacio sea independiente y de difícil acceso para los motores de búsqueda convencionales como es la parte del internet profundo, en el caso de internet libre solo el 16 % es explotado a nivel internacional."[32]

"Para tener una idea de la magnitud de la información que existe en internet, en general, se cree que toda la información depositada en las redes privadas (intranets), más las páginas web generadas por las bases de datos estuvieran incluidas junto con el internet libre, el volumen alcanzaría los 550 billones de documentos y el 95 % sería accesible públicamente."[33]

Las redes que conforman internet son infinitas, sin embargo existe una clasificación sobre los espacios de internet, por los que interactúa la sociedad ya sea de forma legal o ilegal, facilitando su anonimato y dificultad para ser rastreado.

Para comprender mejor los espacios en los que está constituido internet, el autor Fermín Mantallana divide en tres espacios el uso de internet: conocidas como internet libre, internet profundo e intranet:

[31] Ezquer Matallana Fermín, Castellano D. José Manuel, Big to small: Las estrategias de las grandes corporaciones al alcance de la mediana empresa, Ed. Caixagalicia, España, 2010, p.18.
[32] Ídem.
[33] Ibídem, p. 20.

Cuadro 1 Los tres espacios de internet

Libre	Profundo	Intranet
Acceso ilimitado de las herramientas genéricas a los servicios públicos.	Acceso limitado por incapacidad de herramientas.	Acceso cerrado para herramientas genéricas.
Datos y documentos disponibles a través de las herramientas genéricas de búsqueda o navegación.	Información o datos solo accesibles a través de formularios y pasarelas (*gateway*) o claves (*passwort*).	Información y datos de las organizaciones comerciales, instituciones públicas… Acceso restringido (solo a personal autorizado e interno).
Base de datos de las casas genéricas (Google, Yahoo!, MSN…), servidores públicos.	Bases de datos, servidores no públicos, software, mails, animaciones e imágenes, catálogos de bibliotecas.	Base de datos internas, Mails, informes.

Fuente: Ezquer Matallana Fermín, Castellano D. José Manuel, Big to small: Las estrategias de las grandes corporaciones al alcance de la mediana empresa, Ed. Caixagalicia, España, 2010, p.21.

El internet libre es una parte de la red que esta accesible para cualquier persona para la interacción mediante servidores públicos, como pueden ser las redes sociales, e-mails, buscadores como Google, Yahoo!, YouTube sin haber alguna restricción de acceso.

En el caso de Intranet, "es una red de ordenadores basada en los protocolos de internet (TCP/IP) que pertenece a una organización y que es accesible únicamente por los miembros de la organización."[34]

Una intranet puede estar o no conectada a internet, se podría decir que es un sitio web que actúa como cualquier sitio web de internet, pero de forma interna de una empresa o institución que está protegida con un programa informático llamado firewall que controla el acceso de una computadora a la red para evitar intrusiones en el sistema .

A comparación del internet libre que es de fácil acceso y la intranet que tiene acceso restringido solo para personal autorizado, el internet profundo es lo

[34] Luján Mora Sergio, Programación de aplicaciones web: historia, principios básicos y clientes web, Ed. Club Universitario, España, 2002, p.53.

contrario ya que es de difícil acceso, pero cualquier persona con amplios conocimientos de programación puede entrar.

> "El internet profundo recibe ese nombre porque no es accesible con los motores de búsqueda convencionales, la información que se puede encontrar en esta parte de la red no es de fácil acceso, por lo que para ingresar se necesita cierto tipo de programas con los cuales se esconde la dirección (Internet Protocol)."[35]

Para poder ingresar a la Internet profunda se necesita el programa TOR (The Onion Router por sus siglas en inglés) , este programa fue diseñado por la marina de los Estados Unidos, el cual permite a los usuarios navegar en forma anónima, debido al contenido que en ella se encuentra y que se genera en forma real, como pueden ser valores de bolsa, bases de datos de agencias de inteligencia, disidentes políticos, mercados ilegales, sitios en donde se pueden comprar armas, drogas, órganos e incluso contratar asesinos, todas las transacciones se hacen mediante la criptomoneda conocida como bitcoin.[36]

"El programa Tor se creó en 1995 con la finalidad de proteger las comunicaciones del gobierno, cuando se iniciaron los trabajos de investigación sobre enrutamiento por capas (*Onion Routing*) en la oficina de Investigación Naval de la Marina de los Estados Unidos, sin embargo el 1997 el proyecto pasó a ser financiado por la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA) bajo el programa de redes de alta confidencialidad y en 1999 fue suspendido por falta de fondos."[37]

Es hasta 2003 cuando se vuelve a retomar el proyecto bajo la Agencia de Investigación de Proyectos Avanzados (DARPA) para la reconstrucción de servidores ocultos, sin embargo en octubre del mismo año la red Tor es desplegada y el código es liberado.

---

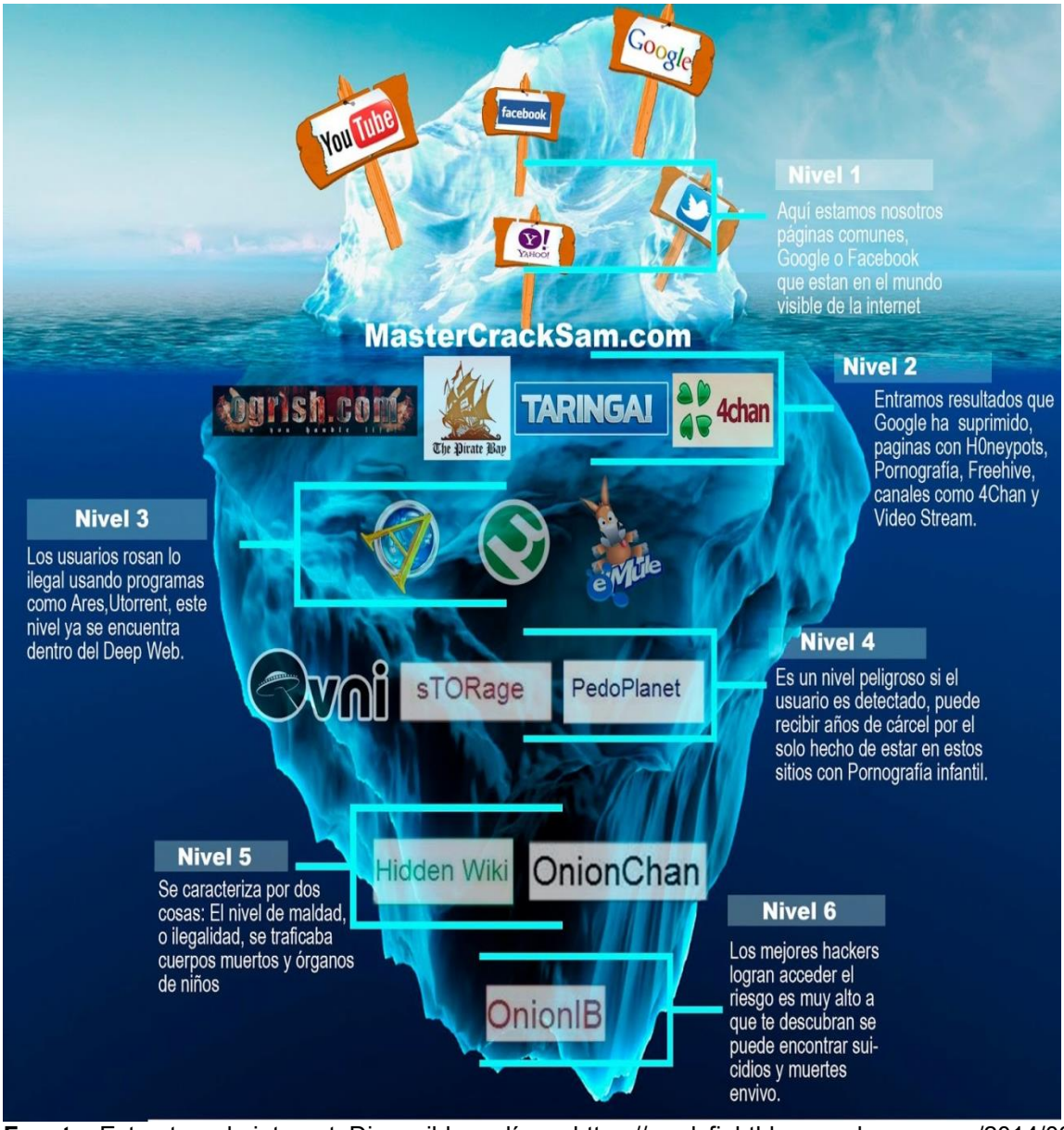
[35] Ídem.

[36] Bitcoin es una moneda electrónica permitiendo la realización de transacciones instantáneas con la tecnología peer to peer (entre iguales), evitando depender de una autoridad monetaria central que se encargue de la emisión y control de dinero y haciendo la transacciones a bajos costos o nulos y es imposible de rastrear.

[37] Stefano Pezzino, TOR (The Onion Router), Ed. Universidad Católica "Nuestra Señora de la Asunción", Facultad de Ciencias y Tecnología, Uruguay, 2014, p.3, Disponible en línea: http://www.uca.edu.py, Fecha de consulta: 09 de Agosto de 2017.

Como se muestra en la (imagen 3), la internet profunda es la parte del bloque de hielo que se encuentra debajo de la superficie, donde se pueden encontrar páginas que se dedican al mercado negro, páginas de grupos terroristas, páginas de tráfico de drogas, etc., sin embargo la internet profunda también se pueden encontrar paginas académicas, de instituciones, de gobiernos, donde solo se puede acceder por medio de un sistema de encriptación (contraseñas).

Imagen 3 La internet profunda



Fuente: Estructura de internet, Disponible en línea: https://readyfightblog.wordpress.com/2014/03/08/estructura-de-internet-visible-webdeep-web/, Fecha de consulta: 09 de Agosto de 2017.

1.2.3 Ciberseguridad

"La ciberseguridad es un conjunto de acciones de carácter preventivo que tienen por objetivo asegurar el uso de las redes públicas y privadas."[38]

De acuerdo a la Agencia de Seguridad Nacional (NSA por sus siglas en inglés), la seguridad cibernética es uno de los temas principales en sus estrategias de protección de la información de sus ciudadanos, empresas, programas gubernamentales, softwares con flujo de información referente al comercio exterior, como se cita a continuación:

"Las amenazas cibernéticas se han ampliado con la globalización de las telecomunicaciones digitales, la mayor dependencia de las redes informáticas y la convergencia de la tecnología.
Las amenazas cibernéticas también han evolucionado. Es importante señalar que el riesgo no es solo de Estados- Nación sofisticados, sino también de hackers, criminales y terroristas."[39]

El concepto de Ciberseguridad modifica el concepto de seguridad tradicional por el uso de las nuevas tecnologías de la información y comunicación en un espacio intangible el cual se modifica rápidamente por el flujo de comunicaciones instantáneas, debido a los riesgos se debe proteger la seguridad nacional norteamericana de las posibles amenazas que afecten el ciberentorno, por lo que se puede decir que la "ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno."[40]

Cabe destacar que la ciberseguridad surge como respuesta a los riesgos asociados con el uso de las tecnologías de información y comunicación en las actividades cotidianas del ser humano, como objetivo primordial en la ciberseguridad es proteger la infraestructura nacional y minimizar riesgos en el

[38] Ciberdefensa-Ciberseguridad Riesgos y Amenazas, 2013, disponible en línea: http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf, Fecha de Consulta: 11 de Febrero de 2017.
[39] Cyber, Nacional Security Agency, 2016, disponible en línea: http://www.nsa.gov/what-we-do/cyber/, Fecha de consulta: 1 de Febrero de 2017.
[40] Caro Bejarano María José, Alcance y ámbito de la seguridad en el ciberespacio, en ciberseguridad. Retos y Amenazas a la seguridad nacional del ciberespacio,Ed. Ministerio de defensa, Instituto Español de Estudios Estratégicos, España, 2011, p. 55.

ciberespacio, además de garantizar la seguridad de la información de cada persona.

La ciberseguridad se refiere a: "[…] cuestiones de seguridad de la información para los gobiernos, las organizaciones y las personas que se ocupan de la seguridad de las tecnologías de la información y las comunicaciones, y en particular con las tecnologías de Internet."[41]

La finalidad de la ciberseguridad es proteger, vigilar, monitorear, combatir y controlar el espionaje cibernético, el terrorismo internacional, la ciberdelincuencia, que desestabilizan al Estado por medio del flujo de información de uso restringido, que llega a ser manipulada.

Para que pueda haber seguridad en el ciberespacio, el autor Víctor Monjaraz recomienda que el Estado debe de aplicar una infraestructura estratégica en el espacio y tiempo; a continuación se mencionaran los aspectos que propone el autor Víctor Monjaraz para tomar en cuenta por parte del Estado y se pueda aplicar las medidas de ciberseguridad eficientemente:

- Obtener ciberinformación
- Tener una ciberinteligencia estratégica
- Conocimiento de Geopolítica, Geoestratégica y geoeconomía aplicadas a lo ciber mediante:
- Una organización social basada en el bienestar colectivo, popular o nacional.
- Con la aplicación, respeto y cumplimiento de las responsabilidades sociales, institucionales y constitucionales.
- Con énfasis de una cultura de responsabilidad, que premie el esfuerzo colectivo y castigue la corrupción, el abuso, el fraude y la impunidad.[42]

[41] Ghernaouti Solange, Cyberpower, crime, conflicto and security in cyberespace, Ed. CRC Press, EE.UU, 2006, p 329.
[42] Ortega Monjaraz Víctor, Nueva Inteligencia y Ciberseguridad, Ed. Secretaría de Marina, Revista del Centro de Estudios Superiores Navales, Volumen 37, México, 1 de Marzo de 2016, p. 64.

Dentro de las características de la seguridad de la información el autor Solange Ghernaouti menciona:

> "La seguridad de la información se ocupa de una serie de cuestiones, como la soberanía de los Estados, la seguridad nacional, la protección de las infraestructuras críticas, la seguridad de los bienes materiales e inmateriales y la protección de los datos personales, por mencionar sólo algunos. Además, cualquier mal funcionamiento potencial de las tecnologías de la información, en relación con su origen (accidente, error, malevolencia), constituye un riesgo operacional para las personas u organizaciones que dependen de las TIC, ya que implican un riesgo de pérdidas debido a la insuficiencia o falla de los procesos. "[43]

Como se puede observar en la definición anterior, la seguridad de la información, se ramifica en varias secciones, en las cuales la seguridad es primordial para resguardar su soberanía, las infraestructuras críticas, la confidencialidad de cada ciudadano mediante el resguardo de datos confidenciales, por lo cual al tener la protección adecuada evitara la vulnerabilidad en los sistemas informáticos.

Cabe señalar que "la ciberseguridad no puede abstraerse de su campo de aplicación y del entorno socio-cultural. Debe abordarse en un contexto interdisciplinario y multipartito, colocando al individuo en el centro de la cuestión de la seguridad de las Tecnologías de la Información y Comunicación (TIC´s) con el fin de promover el desarrollo de una sociedad de la información consiente e integradora"[44]

La seguridad de la información, engloba temas relacionados con las cuestiones de ciberdelincuencia y el uso indebido de las Tecnologías de la información y comunicación (TIC´s). También la ciberseguridad surge de la necesidad de que las tecnologías sean menos vulnerables, para disminuir el número de amenazas potenciales.

Para comprender mejor el interés por regular e inhibir amenazas, se definirá el término de las Tecnologías de la información y comunicación (TIC):

[43] Ghernaouti Solange, Cyberpower, crime, conflicto and security in cyberespace, Ed. CRC Press, EE.UU, 2006, p. 330.
[44] Ídem.

“Las TIC han sido definidas con sistemas tecnológicos mediante los que se recibe, manipula y procesa información, y que facilitan la comunicación entre dos o más interlocutores.”[45]

Lo que busca cada Estado con el uso de las TIC, es fortalecer relaciones multilaterales mediante la interacción electrónica entre el gobierno y los actores inmersos en el sistema internacional (véase en anexo 2) , por lo que Estados Unidos busca el desarrollo de nuevos sistemas informáticos que no sean propensos a futuros ataques en los espacios virtuales como son las redes sociales, las cuales son el escenario perfecto para perpetrar ataques cibernéticos robar identidades, lo que hace más difícil el rastreo de hacker involucrados en grupos terroristas.

Debido a que la seguridad de las TIC es una gran preocupación para los asuntos gubernamentales, diplomáticos y militares, la dimensión política completa los enfoques técnicos, gerenciales y legales de la seguridad de la información, ya que la seguridad cibernética también concibe la soberanía del Estado, la seguridad nacional y la seguridad de los ciudadanos.

Además la seguridad cibernética es esencial para el funcionamiento de Internet para el uso de los Estados, organizaciones y los ciudadanos, por lo cual la seguridad informática es multidisciplinaria, porque involucra una amplia información de diversas disciplinas, en la cuales se deben de tomar aspectos de acuerdo a la cultura de cada Estado porque a partir de la cultura se van a delimitar las legislaciones políticas y legales para que puedan tener mayor seguridad en el sistema informático.

[45] Yañez María Rebeca, S. Villatoro Pablo, Las nuevas tecnologías de la información y de la comunicación (TIC) y l institucionalidad social. Hacia una gestión basada en el conocimiento, Ed. CEPAL, Santiago de Chile, 2005, p.7.

1.2.4 Ciberinteligencia

Un elemento importante a considerar en la ciberseguridad es la inteligencia informática para hacer frente a las amenazas externas que puedan provocar la interferencia en los flujos de información y comunicación a nivel mundial en materia política exterior y evitar que se provoquen problemas entre los Estados.

La palabra inteligencia proviene del latín que significa intelligentia, como una facultad de comprender, de conocer, que se relaciona con la posibilidad de comprensión, conocimiento, habilidad y destreza.[46]

Willmoore Kendall[47], veía a la inteligencia como un apoyo a los decisores políticos para conseguir influir en el devenir de los acontecimientos internacionales, ayudándoles a comprender los factores externos e internos en los cuales Estados Unidos podía tener un cierto impacto.

Cabe señalar, que hoy en día hay un mayor flujo de datos y de flujos informativos, desde cualquier dispositivo, lo cual provoca una dispersión rápida de información, haciendo más complejo ejecutar una estrategia para controlar las redes de comunicación gubernamentales, sociales y privadas debido a que el problema ya no es la información como tal, sino la capacidad para su integración e interpretación en un sistema globalizado y la forma de ejercer poder.

En Estados Unidos durante la primera administración de Barack Obama, en promedio se realizaron 50 mil informes de ciberinteligencia por año, contando con 1.7 millones de comunicaciones inter agencias, relacionadas con información para la inteligencia y seguridad nacional. La relación del trabajo de análisis con los usuarios-consumidores de estos productos, requiere un claro esquema estratégico

[46] Diccionario de la Real Academia Española, Disponible en línea: www.rae.es,Fecha de consulta: 25 de Abril de 2017.
[47] Kendall, Willmoore, The function of intelligence, World politics, vol.1, n°4, Ed. Cambridge University Press, England, 2011, p. 552.

de prioridades para mantener vigente su rol preventivo y su actuación en la dinámica mundial.[48]

Debido a la complejidad para vigilar los flujos de información, la ciberinteligencia se nutre de varias vertientes, como es la inteligencia estratégica que sirve para evitar en el futuro ataques en la infraestructura crítica y resguardar en bienestar nacional.

De acuerdo a la *National Intelligence Strategy* de la casa Blanca de 2010 para mantener seguro el ciberespacio debe de implementarse una seguridad estratégica para realizar medidas de ciberseguridad de acuerdo a las capacidades de seguridad de cada Estado: "un método mediante el cual se informa a las decisiones ejecutivas ya que esta es un apoyo de las decisiones de la seguridad interior, estatal, local y gobiernos de países subdesarrollados, nuestras tropas y misiones nacionales esenciales. Estamos trabajando para mejorar la integración de la comunidad de inteligencia. Estamos fortaleciendo nuestra colaboración con servicios de inteligencia extranjeros y manteniendo fuertes lazos con nuestros aliados más próximos. Pero sobre todo porque incluye un elemento importante cuando sostiene que la seguridad y prosperidad de nuestro país dependen de la calidad de la inteligencia que recopilamos y el análisis que producimos, nuestra habilidad para evaluar y compartir a tiempo esta información y nuestra habilidad para contrarrestar las amenazas."[49]

1.2.5 Ciberterrorismo

El concepto de Ciberterrorismo: "Es el ataque deliberado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y

[48] Vizarreta Gonzales Emilio, Nueva Inteligencia y Ciberseguridad, Ed. Secretaría de Marina, Revista del Centro de Estudios Superiores Navales, Volumen 37, México, 1 de Marzo de 2016, p. 54.

[49] National intelligence strategy.White House, 2010, disponible en línea: http: //www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf., Fecha de consulta: 20 de Abril de 2017.

datos que pueden resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos"[50]

1.2.6 Ciberguerra

La ciberguerra: "Es aquel conflicto bélico que utiliza como campo de operaciones , en vez de los campos de batalla convencionales el ciberespacio y las tecnologías de la información y como las tecnologías de la información y como las armas las aplicaciones, comandos y herramientas diversas que proporcionan la informática y las telecomunicaciones."[51]

1.2.7 Hacker

El avance de la tecnología se ha desarrollado rápidamente lo que ha provocado investigar nuevos mecanismos para introducirse y tener acceso a información confidencial, por lo que las personas amantes de las redes informáticas han ampliado sus conocimientos y habilidades para penetrar en programas, bases de datos, computadoras para cambiar y extraer información.

De acuerdo con la definición de Luis Orlando Paloma, un Hacker es:

> "Un Hacker es una persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene permanentemente actualizado y conoce a fondo todo lo relacionado con la programación y sistemas complejos, es un investigador congénito que se inclina ante todo por conocer lo relacionado con cadenas de datos cifrados y las posibilidades de acceder a cualquier tipo de información segura. Su formación y las habilidades que posee le dan una experiencia mayor que le permite acceder a sistemas de información seguros, sin ser descubierto, y también le da la posibilidad de difundir los conocimientos para que las demás personas se enteren de como realmente funciona la tecnología y conozca las debilidades de sus propios sistemas de información. [52]

[50]Urueña Centeno J. Francisco, Ciberataques, la mayor amenaza actual, Ed. Instituto Español de Estudios Estratégicos, 2015, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09/2015_AmenazaCiberataques_co.Urueña.pdf, Fecha de consulta: 12 de Febrero de 2017.
[51] Ídem.
[52]Paloma Parra Luis Orlando, Delitos Informáticos (en el ciberespacio), Ed. Ediciones Jurídicas Andrés Morales, Bogotá, Colombia; Ciudad de Panamá, Panamá, 2012, p. 65.

1.2.8 Hacktivista

La definición de Hacktivista: “Son personas que se dedican a hacer hacking, ciberespionaje o crear tecnología para conseguir un objetivo político y social, considerando estas acciones como un método de información, por lo que no se contempla como una acción criminal, sino como una forma legítima de protesta que se concentra en objetivos gubernamentales o empresariales, para incitar un boicot, la desobediencia civil digital o convocar a un mitin ciberespacial.”[53]

1.2.9 Cibercrimen

Concepto de Cibercrimen: “Es toda aquella acción legal que se da por vías informáticas o que tiene como objetivo destruir o dañar ordenadores, medios electrónicos y redes de internet.”[54]

1.2.10 Política exterior

El concepto de Política Exterior: De acuerdo al Diccionario de política exterior de Edmundo Hernández-Vela Salgado, la política exterior se puede definir de la siguiente manera: “Conjunto de políticas, decisiones y acciones, que integran un cuerpo de doctrina coherente y consistente, basado en principios claros, sólidos e inmutables, forjados a través de su evolución y experiencia histórica; permanentemente enriquecido y mejorado; por el que cada Estado, u otro actor o sujeto de la sociedad internacional, define su conducta y establece metas y cursos de acción en todos los campos y cuestiones que trascienden fronteras o que pueden repercutir al interior de las suyas; y que es aplicado sistemáticamente con el objeto de encausar y aprovechar el entorno internacional para el mejor cumplimiento de los objetivos trazados en aras del bien de la nación […]”[55]

---

[53] Loreto Vicente, ¿Movimientos sociales en la red? Los hacktivistas, Ed. El cotidiano, vol. 20, núm. 126, Julio-Agosto, México, 2004, p. 3, disponible en línea: http://www.redalyc.org/articulo.oa?idp=1&id=32512615&cid=5255, Fecha de consulta: 13 de Noviembre de 2017.

[54] Urueña Centeno J. Francisco, Ciberataques, la mayor amenaza actual, Op cit. p. 2.

[55] Hernández-Vela Salgado Edmundo, Diccionario de política Internacional, Tomo ll, Letras J-Z, sexta edición, Editorial Porrúa, México, 2002, p.935.

CAPÍTULO II: ANTECEDENTES DE ATAQUES CIBERNETICOS EN EL CIBERESPACIO

2.1 Antecedentes de ataques cibernéticos

De acuerdo a Juan Puime, “Los avances tecnológicos que se fueron desarrollando a través del tiempo, como el telégrafo y la radio han marcado la evolución de los métodos y procedimientos de interceptación y encriptación de información, y con ello del espionaje. Un ejemplo de esta evolución es la legendaria máquina enigma[56], utilizada por el ejército alemán durante la segunda guerra mundial.”[57]

Por otra parte, el lanzamiento del primer satélite soviético llamado Sputnik, en 1957 que fue lanzado en órbita lo que provocó una gran conmoción para Estados Unidos, lo que produjo que se invirtiera en desarrollo científicos y agencias de defensa como fue ARPA (Advanced Research Projects Agency.)

Por lo que la seguridad siempre ha existido, pero históricamente se empezó a tomar en cuenta hasta mediados de los años noventa, la ciberseguridad adquirió mayor auge y se empezó a ver como una cuestión tecnológica.

El tema de la seguridad en las redes de comunicación en los años 90´s empezó a cobrar mayor importancia, por el acceso a internet que se empezó a extender rápidamente entre la sociedad, principalmente universidades, por lo que se requirió tomar medidas sobre los delitos informáticos.

A continuación se citará la legislación estadounidense, sobre delitos informáticos:

> “La legislación estadounidense adoptó en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. La nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec.1030(a)(5)(A). Esta ley sanciona los actos de transmisión de virus.”[58]

[56] La máquina enigma: Era una maquina encriptadora basada en una serie de Rotores que cambian una letra por otra.
[57] Maroto, Juan Puime, El ciberespionaje y la ciberseguridad, En La violencia del siglo XXI. Nuevas dimensiones de la guerra, Ed. Instituto Español de Estudios Estratégicos, España, 2009, p.2.
[58] Ibídem, p. 224.

El primer sistema operativo incluyó mecanismos de control de acceso y criptografía, que estaba fabricado solamente para aplicaciones de uso en actividades militares, el sistema financiero y bancario. La seguridad de la red es una parte integral de la gestión de la red, por medio de una correcta administración de la configuración de las redes o sitios que se visitan en el ciberespacio.

Desde entonces, las actividades de control para la seguridad utiliza herramientas de seguridad de manera no integrada y difícil de detectar, sin embargo los avances tecnológicos en el ámbito informático han avanzado con rapidez, lo que ha influido en las victorias de conflictos bélicos por ejemplo:

"A virus-infected chip was installed in the printers of the air defense weapon system the United States imported to Iraq before the 1991 Gulf war. During the Gulf war, the "back door" was remotely actived, causing the Iraqi air defense system to go hardware, which led to the defeat of Iraq in combat."[59]

Debido a la proliferación de guerras asimétricas ante la aparición de grupos terroristas la capacidad de destrucción aumentó, el enemigo para Estados Unidos se centró en la Unión Soviética y sus satélites enviados al espacio.

Estados Unidos, al finalizar la guerra fría, se consolidó como única potencia en el sistema Internacional, sus intereses nacionales cubrían al mundo por completo, lo cual lo posiciono como una nación indispensable para resguardar la paz mundial, siendo el primer paso para la reformulación en el escenario internacional donde la nueva vertiente es la "interdependencia entre las naciones"[60], como es el caso de Medio Oriente región importante para los intereses globales de Estados Unidos, principalmente por los recursos naturales, por otra parte el Presidente Barack Obama enfatiza que las estrategias de seguridad nacional deben de ir

[59] Se instaló un chip infectado con virus en las impresoras del sistema de armas de defensa aérea que Estados Unidos envió a Irak antes de la guerra del Golfo de 1991. Durante la guerra del Golfo, la "puerta trasera" se activó remotamente, provocando que el sistema de defensa aérea iraquí se viera mal, lo que llevó a la derrota de Irak en combate.(Traducción propia), R. Linosay John, Cheung Ming Tai, S. ReveronDerek, China and cybersecurity espionaje, strategy, and politics in the Digital Domain, Ed. Oxfort University, England, 2015, p.127.

[60] La interdependencia de las naciones se caracteriza por la multiplicidad de canales que conecta a las sociedades desde las elites gubernamentales hasta las no gubernamentales, la ausencia de una jerarquía en la agenda interestatal y el hecho de que la fuerza militar no sea utilizada por los gobiernos para resolver problemas.

encaminadas a la lucha contra el terrorismo considerado una amenaza latente a la estabilidad, libertad y seguridad de esta nación, como fue el atentado a las torres gemelas el 11 de septiembre de 2001 en Nueva York.

El atentado del 11 de septiembre a las torres gemelas, fue un parte aguas en la implementación de las medidas de seguridad estadounidense, porque confronta los conceptos de libertad y seguridad, al poner limitaciones en el uso de la red, además de usar métodos de espionaje para resguardar la seguridad nacional, lo que viola los derechos básicos de la sociedad.

Este estado de alarma se ha acentuado en los últimos tiempos originando un blowback como una consecuencia del financiamiento a células terroristas por parte de Estados Unidos en Medio Oriente, en represalia han aparecido individuos que actúan aisladamente (lobos solitarios), aunque con colaboración y difusión de las redes sociales, causando daño en cualquier parte del mundo, en nombre del Islam.

Otro caso que ejemplifica ataques en el ciberespacio es en 2007 y 2008 cuando Rusia envío un malware llamado *Botnet* que son redes de "[…] robots que se distribuyen en miles y miles de máquinas y que en un momento dado el creador puede ordenarles atacar"[61] en los servidores que se filtran, como fue el caso de Rusia que "lanzó un ataque completo de "enjambre" contra la red de Georgia mientras que las tropas rusas cruzaban la frontera georgiana. El ataque paralizó las redes en la televisión georgiana, el sistema financiero y de transporte."[62]

En 2009 el ataque llamado operación aurora, fue uno de los ataques más sofisticados proveniente de China, esté ataque consistió en el espionaje cibernético con el cual sustrajeron y robaron información digital de Estados Unidos, por lo cual la Secretaría de Estado Hillary Clinton, pidió un esclarecimiento al gobierno chino por los daños en el robo de propiedad intelectual como fue en el ámbito militar: "Los planos del Jet F-35 de última generación que fueron

[61] Paloma Parra Luis Orlando, Op.cit. p.40.
[62] R. Linosay John, Cheung Ming Tai, S. ReveronDerek, China and cybersecurity espionaje, strategy, and politics in the Digital Domain, Ed.Oxfort University, England , 2015, p.127.

sustraídos, los cuales formaban parte de un proyecto multinacional con un costo de 300 billones de dólares."[63]

Otro de los eventos más relevantes en el ámbito internacional fue el caso WikiLeaks en 2010 con la filtración de cables diplomáticos, provocando fracturas y desestabilización en las relaciones diplomáticas, posteriormente se encuentra la información de manera detallada.

En cuanto a los ataques físicos en el ciberespacio en julio de 2010 un sofisticado virus informático llamado "Stuxnet", fue enviado a Irán como respuesta a su progreso en investigaciones nucleares por lo que se convirtió en una preocupación para Estados Unidos e Israel como una posible amenaza a la seguridad internacional, el virus "Stuxnet" paralizó totalmente las centrifugadoras de enriquecimiento de uranio y causó el retaso de casi dos años en su planta de desarrollo nuclear.[64]

De acuerdo con los autores R. Linosay John, Cheung Ming Tai, S. ReveronDerek:

"[…] el virus Stuxnet es el primer virus reportado dirigido a sistemas de control industrial, y demuestra una nueva etapa de ciberguerra dedicada a daños de hardware, así como marcar la transformación de la seguridad de la red informática global en un problema para la protección de infraestructuras nacionales también."

Otro de los ciberataques que han causado conmoción en el sistema internacional fue el caso de Estonia; todo comenzó desde que el gobierno de Estonia tomara la decisión de trasladar de manera permanente la estatua conocida como "el soldado de bronce" del centro de la capital llamada Tonismäe hacia un cementerio militar, la situación provoco fricciones entre la comunidad rusa ya que para ellos significa un símbolo conmemorativo de sus caídos en la segunda guerra mundial, contrariamente a la comunidad de Estonia la estatua representa al opresor de la era soviética.

[63] García Hernández Arturo, "Una visión del poder económico en la Ciberseguridad", Seguridad y Defensa en el Ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p.40.
[64] Ídem, p.127.

La situación se empezó a complicar “el 9 de mayo de 2006 cuando la policía tuvo que intervenir en la trifulca entre miembros de la comunidad rusa que portaban banderas de la extinta Unión de Repúblicas Socialistas Soviéticas y estonios que portaban banderas de la República de Estonia, entre partidarios pro-kremlin y movimientos nacionalistas estonios, a partir de este hecho la sociedad estonia se fue polarizando y el soldado de bronce se convirtió en punto de encuentro de manifestaciones extremistas.”[65]

Debido a las constantes manifestaciones el gobierno estonio anuncia a principios de la primavera de 2007 el traslado de la estatua, provocando la intensificación de las manifestaciones y actos vandálicos, estos disturbios fueron conocidos como la “noche de los cristales”[66], pero a partir del 27 de abril de 2007 comenzaron ciberataques a sistemas de información de la infraestructura pública y privada estonia.

El autor Néstor Ganzúa Artiles diferencia los ciberataques es dos fases, a continuación se explicara cada fase:

- Fase 1, del 27 al 29 de abril, se caracterizó por el uso de herramientas de ciber ataque rudimentarias y simples, llevados a cabo por hacktivistas sin grandes conocimientos técnicos, las herramientas estaban especialmente diseñadas para atacar sitios web de Estonia y especialmente del gobierno, del ministerio de Defensa y de los principales partidos políticos.
- Fase 2, del 30 de abril al 18 de mayo, el conflicto toma otra dimensión al trasladarse totalmente al ciberespacio, durante este lapso de tiempo los conflictos internos entre la comunidad rusa y los estonios se calma por lo que se descartan ataques emocionales, sin embargo los ataques se volvieron más complejos y sofisticados debido a que necesitaban de un

[65] Artiles Ganzúa Néstor, “La situación de la ciberseguridad en el ámbito internacional y en la Otan”, ciberseguridad retos y amenazas a la seguridad nacional en el ciberespacio, Ed. Ministerio de defensa, Instituto Español de Estudios Estratégicos, España, 2010, p. 175.
[66] Ídem.

mayor conocimiento de las herramientas de ciberguerra y de un uso de grandes *botnets*.[67]

Al inicio de la administración de Barack Obama, los ataques cibernéticos se presentaron continuamente, teniendo repercusiones tanto en el sector público como privado, a continuación se mencionan algunos ataques cibernéticos que causaron daños en la infraestructura informática estadounidense:

"En 2008 el Subsecretario de Defensa de EEUU, William J. Lynn III, dio a conocer una filtración de un virus a través de las redes militares clasificadas de esa nación, el cual se propagó por medio de un dispositivo externo (USB) introducido en una computadora portátil en una base de Oriente Medio y se auto cargo en una red del Mando Central de Estados Unidos".[68]

"En abril de 2009 el diario The Wall Street Journal informó de la infiltración de un multimillonario proyecto del Pentágono para la construcción de un nuevo avión de combate en el ámbito militar, los hackers supuestamente se encontraban en China, que ha sido señalada como el origen de otros ciberataques."[69]

"El 4 de Julio de 2009, día en que se celebra la fiesta de Independencia de Estados Unidos, hubo una serie de ataques, Denegación de Servicio contra diferentes instancias gubernamentales como fue el caso de la Casa Blanca, el Departamento de Seguridad, el Servicio Secreto y la Agencia de Seguridad Nacional, el ataque consistió en una red de robots informáticos (*botnets*) de más de 50,000 ordenadores." [70]

---

[67] Ibídem, p. 179.
[68] La nación, Un pen drive provoco el mayor ataque a computadoras militares de EE.UU, 25 de agosto de 2010, disponible en línea: http://www.lanacion.com.ar/1297971-un-pen-drive-provoco-el-mayor-ataque-a-computadoras-militares-de-eeuu, Fecha de consulta: 20 de Mayo de 2017.
[69] BBC, Ciberespacio: el nuevo ámbito de la guerra para el pentágono, 27 de julio de 2011, disponible en línea: http://www.bbc.com/mundo/movil/noticias/2011/07/110722_eeuu_pentagono_ciberespacio_estrategia_wbm.shtml, Fecha de consulta: 20 de Mayo de 2017.
[70] Díaz del Rio Duran José Juan, "La ciberseguridad en el ámbito militar", Ciberseguridad retos y amenazas a la seguridad nacional en el ciberespacio, Ed. Ministerio de defensa, Instituto español de Estudios Estratégicos, España, 2010, p. 235.

Uno de los problemas más graves que ha tenido Estados Unidos en cuestión de ciberseguridad fue en 2010 cuando el The Washington Post publicó datos sobre "una campaña de contraespionaje chino contra sistemas informáticos de al menos, 34 importantes compañías estadounidenses en este ataque utilizó diversos códigos maliciosos que eran muy sofisticados."[71]

En el sector privado en 2010, la empresa que se vio afectada en ciberataques fue Google la cual anunció que había sido atacada mediante una vulnerabilidad de Adobe Reader en una acción denominada Operación Aurora por los expertos en seguridad; El mismo ataque afectó a más de 30 empresas, incluidas Yahoo, Symantec Adobe y Northrop Grumman.[72]

El ciberataque denominado Operación Aurora provino de China, debido a que vulneró el muro de seguridad de la compañía y agencias de inteligencia chinas tuvieron acceso a los servidores para acceder a las cuentas de correo electrónico de gmail de destacados opositores chinos.[73]

"En octubre de 2010, Bancos estadounidenses perdieron más de 12 millones de dólares en un ataque que empleo un virus troyano llamado Zeus para grabar las pulsaciones del teclado de los usuarios para robar datos de sus cuentas bancarias."[74]

Otra empresa que se vio afectada durante la administración Obama fue Sony en 2011 al sufrir un ataque cibernético en su plataforma online quedando paralizada

[71] The Washington post, Google, China *Cyberattack part of vast espionaje campaign experts say*, 14 de Enero de 2010, disponible en línea: http://www.washingtonpost.com/wpdyn/content/article/2010/01/13/AR2010011300359.html, Fecha de consulta: 20 de Mayo de 2017.
[72] Wood Teresa, Los 20 ciberataques perversos del siglo XXI, 13 de septiembre de 2015, Mit Technologies Review, disponible en línea: https://www.technologyreview.es/s/7413/los-20-ciberataques-mas-perversos-del-siglo-xxi, Fecha de consulta: 10 de Junio de 2017.
[73] González Veiguela Lino, Los ciberataques (conocidos) más importantes, Ed. esglobal, 2 de Julio de 2013, disponible en línea: https://www.esglobal.org/la-lista-los-ciberataques-conocidos-mas-importantes/, Fecha de consulta: 11 de Junio de 2017.
[74] Ídem.

durante varias semanas, se filtraron datos sensibles de sus clientes como tarjetas de crédito, correos, direcciones físicas y contraseñas.[75]

2.2 Ataques Cibernéticos

En el ciberespacio el uso de Internet por organizaciones radicales han incrementado para cometer ataques cibernéticos, las actividades de estos grupos terroristas se dividen en dos categorías: la primera son actividades de apoyo y la segunda son actividades operacionales.

Actividades de apoyo:

"Las actividades de apoyo terrorista en Internet incluyen la difusión de objetivos terroristas a través de la propaganda en apoyo de la radicalización del pensamiento, como el fomento de otros para creer que la violencia es la respuesta a un problema político particular."[76]

Por lo general estos grupos terroristas, tienen una buena organización y con solvencia económica para financiar sus actividades en la red por medio de la introducción masiva de propaganda, canales de video y estaciones de radio en Internet.

Los pasos que se utilizan para realizar un ciberataque en primera instancia es investigar y recopilar información sobre el objetivo que se quiere desestabilizar, al ya tener identificada a la víctima proceden los hackers a introducirse al sistema a través de las vulnerabilidades del sistema informático y obtener acceso no autorizado, al obtener el acceso proceden a realizar actividades delictivas o de espionaje hasta lograr su propósito.

Otro ejemplo es la tendencia de introducir pensamientos o ideologías terroristas por medio de juegos: "Existe una amplia evidencia de que los yihadistas

[75] El país, Los peores ataques cibernéticos en Estados Unidos, 5 de Junio 2015, disponible en línea:http://internacional.elpais.com/internacional/2015/06/05/actualidad/1433461961_205806.html, Fecha de consulta: 10 de Junio de 2017.
[76] S. Gal Cecilia, B. Kantor Paul, Brancha Shapira, Security Informatics and Terrorism: Patrolling the web, Ed. IOS Press, Amsterdam, 2008, p.11.

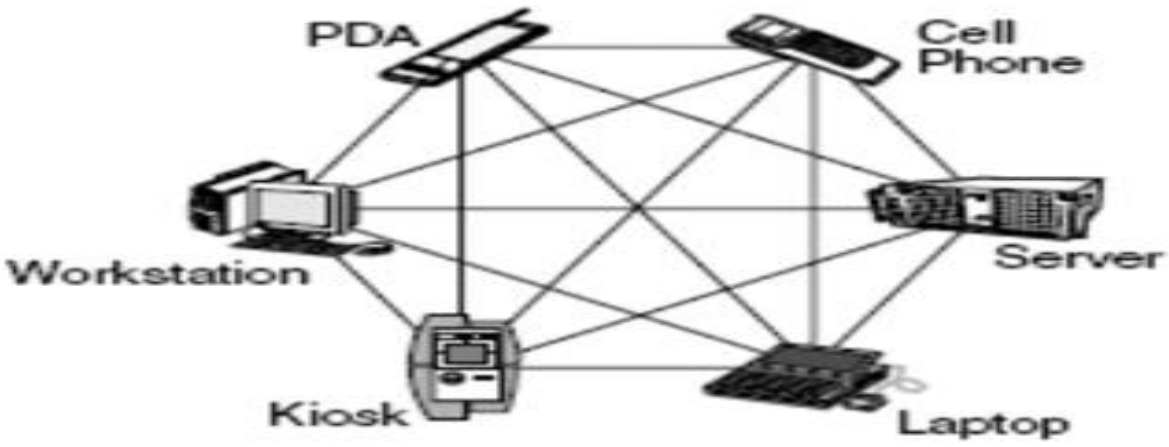
cibernéticos usan el código fuente de juegos y los modifican para crear juegos de computadora cuyo objetivo es matar a un soldado Israeli, a George Bush, a Tony Blair o asesinar al rey Abdullah II de Jordania. Esos tipos de juegos ciertamente existen y circulan libre y ampliamente en el ciberespacio como un medio para difundir un particular punto de vista violento y ciber jihadista. También hay organizaciones terroristas radicales que han elaborado mensajes de cyber yihadistas dirigidos específicamente a los niños, cuyo objetivo es la radicalización a una edad temprana para atraer nuevos miembros al grupo terrorista."[77]

En cuanto a las actividades operacionales, Internet ha facilitado las actividades terroristas operativas a través de sus capacidades de comunicación, permitiendo el mando de instrucciones y el control en el espacio cibernético, ya sea a través de redes peer-to-peer por medio de mensajes de texto SMS o protocolos de voz en Internet.[78]

Con las redes *peer to peer*, se puede compartir y distribuir recursos directamente entre dispositivos que estén en línea, además se puede distribuir información desde el lugar menos esperado directamente con el terrorista, sin la necesidad de entrar en un servidor web (Imagen 4), los recursos que se difunden van desde manuales de capacitación para convertirse en terroristas, elaboración de artefactos explosivos caseros, construcción de armas de destrucción masiva, también como involucrarse en comunicaciones secretas y evitar ser rastreados por la policía cibernética.

[77] Ídem.
[78] Ibídem, p.12.

Imagen 4 ***Red peer to peer***



Fuente: Leg Disanzo Mariano, Redes Peer to peer y tecnología JXTA, 2006, pp.4.

Otra categoría importante de la actividad operacional terrorista que se puede llevar a cabo en línea es la investigación y la planificación de un eventual ataque terrorista. Los terroristas pueden utilizar Internet para investigar sus objetivos, ya sea utilizando imágenes de satélite o simplemente Google TM para obtener información de recursos abiertos para identificar, seleccionar y prepararse para atacar a un objetivo en particular.

“Un ejemplo altamente divulgado fue el complot terrorista puesto en marcha para atacar el aeropuerto John F. Kennedy en la ciudad de Nueva York. En ese caso, el FBI en los Estados Unidos descubrió un complot en el que una pequeña célula terrorista, con vínculos con Guyana, planeaba atacar un oleoducto muy grande que suministraba combustible para el aeropuerto JFK, el oleoducto tenía más de 40 kilómetros de longitud y los terroristas planeaban explotar el oleoducto usando explosivos caseros. Los agentes de la ley descubrieron que al arrestar a los miembros de la célula terrorista habían utilizado google earth TM para ayudar a trazar el mapa del aeropuerto donde se encontraba el oleoducto.”[79]

[79] Ídem

"Estados Unidos ha sufrido ataques cibernéticos a gran escala, como es el caso de un virus cibernético llamado Nimda en septiembre de 2001"[80], por medio de un programa diseñado para replicarse y distribuirse automáticamente, provocó el control de ordenadores institucionales y la lentitud de estos, propagándose e infectando ordenadores en una hora a todo Estados Unidos, estimulando el acceso y destrucción de archivos alrededor de 86,000 software.

"Dos meses después del ataque Nimda, el ataque Código Rojo infectó a 150, 000 ordenadores en catorce horas"[81], siguiendo la misma mecánica que el ataque Nimda, sin embargo los daños fueron menores debido a el refuerzo en las medidas de seguridad en la infraestructura cibernética.

Sin embargo las infraestructuras críticas de Estados Unidos no han sido el único blanco de los grupos terroristas, también personajes políticos se han visto envueltos en ataques a sus servidores o hackeo en sus cuentas oficiales, una muestra clara fue en 2008, un miembro del equipo del todavía candidato Barack Obama, denunció un problema con un equipo de cómputo, que atribuía a un virus informático. Tras su revisión, se pudo comprobar que se había descargado información de la campaña electoral, sin embargo no fueron los únicos atacados, John McCain rival en la contienda electoral también sufrió espionaje e infiltración de documentos.

Por lo que al tomar el cargo en su primera administración Barack Obama, se enfocó en reforzar la revisión de la ciberseguridad de la nación para la protección de información y evitar ataques en la infraestructura cibernética.

John Brennan, Director de la Agencia Central de Inteligencia y principal asesor de Barack Obama menciona la importancia de la seguridad en el ciberespacio: "La seguridad nacional y la salud económica de los Estados Unidos dependen de la

[80] Maroto, Juan Puime. El ciberespionaje y la ciberseguridad, En La violencia del siglo XXI. Nuevas dimensiones de la guerra, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, España, 2009, p. 50.
[81] Ídem.

seguridad, la estabilidad y la integridad del ciberespacio de nuestro país, tanto en el sector público y privado"[82]

2.3 Origen del espionaje y del ciberespionaje.

De acuerdo a la Real Academia española, define la palabra espionaje como una: "Actividad secreta encaminada a obtener información sobre un país, especialmente en lo referente a su capacidad defensiva y ofensiva" [83]

A lo largo de la historia se han usado dos principales técnicas para llevarlo a cabo:

- Infiltración: Técnica usada para introducir individuos al enemigo con el fin de conseguir información relativa a estrategias, actividades y proyectos.
- Penetración: El objetivo es conseguir la colaboración consciente o inconsciente de un miembro de la organización o grupo contrario para que suministre datos e información secreta del grupo del que forma parte.[84]

El espionaje ha ido evolucionando constantemente hasta nuestros días, en la antigua Mesopotamia, se encuentran los primeros indicios de esta actividad:

Mesopotamia

"En Mesopotamia podemos encontrar durante el III milenio a.c. las primeras muestras de la utilización de los servicios de inteligencia y espionaje, en el reinado de Sargon I de Acad, cuyo imperio comprendía desde Siria hasta el sur de Irán. Para su creación, Sargon I sabía que necesitaba información confidencial fuera de sus territorios. Por ello utilizó espías a modo de exploradores para seguir informando de las características de las tierras a dominar."[85]

---

[82] Associated Press, Obama Asks For Review Of Online Security, 10 de Febrero de 2009, The Washington Post, disponible en línea en: http: //www.washingtonpost.com, Fecha de consulta: 17 de Marzo de 2017.
[83] Real Academia Española (RAE), Diccionario de la lengua Española, disponible en línea: http://www.rae.es/,Fecha de consulta: 20 de Abril de 2017.
[84] Jarabo Valdivieso, El espionaje-pasado y presente, 2015, disponible en línea: https://apavaldeluz.files.wordpress.com/, Fecha de consulta: 06 de Agosto de 2017.
[85] Ibídem, p.5.

Grecia

En el mundo Griego, en la primera epopeya de la literatura occidental, la Ilíada, se hace mención del espionaje utilizado en la guerra de Troya.[86]

Roma

En la antigua Roma, los principales políticos tenían su propia red de vigilancia, la cual les proveía información acerca de las intrigas en las distintas escalas del poder en el imperio.

"El famoso orador Cicerón se quejaba frecuentemente de que sus cartas eran interceptadas; Julio César también construyó una red de espionaje que lo tenía al tanto de los complots en su contra."[87]

Edad Media

"Tras la caída del imperio Romano, en Occidente el espionaje e inteligencia se llevaba a cabo únicamente durante los periodos de Guerra, así los espías seguían notificando sobre la topografía, las fortalezas, las armas, tanto ofensivas como defensivas, o las unidades enemigas disponibles."[88]

China

La utilización de la inteligencia militar se dió en todas las civilizaciones antiguas, sin embargo en el Imperio chino se elaboró el primer tratado militar en el que se hace referencia al espionaje: El Arte de la Guerra, de Sun Tzu. Considerado tradicionalmente como un general que sirvió bajo el reinado de King Helu, hacia el año 512 a. C., las experiencias de Sun Tzu al servicio de su señor le sirvieron para componer su tratado.

[86] Ídem
[87] Zucher Anthony, Del imperio Romano a la NSA: la Historia del espionaje Internacional, BBC, 2013, disponible en línea: http: //www.bbc.com, Fecha de consulta: 19 de Abril de 2017.
[88] Jarabo Valdivieso, El espionaje-pasado y presente, 2015, disponible en línea: https://apavaldeluz.files.wordpress.com/2015/05/el-espionaje-pablo-jarabodef.pdf, Fecha de consulta: 19 de Abril de 2017.

"Sun Tzu parte de premisas realistas a la hora de establecer de dónde tiene que partir la información: no se puede obtener ni «de fantasmas ni espíritus», es decir, el teorizador chino rompe con la tradición militar de las civilizaciones mesopotámica y egipcia, cuyos ejércitos, antes de entrar en combate, consultaban la viabilidad o no de ir a la guerra. Sun Tzu fundamenta la obtención de información en el factor humano."[89]

"Sun Tzu habla sobre la importancia de utilizar espías para poder estar enterados de la intención del enemigo y la importancia de conocerse así mismo para ser invisible y obtener buenos resultados en las batallas; lo primero que explica Sun Tzu en El Arte de la Guerra son los tipos de espías, los clasifica en cinco tipos: espías nativos, espías internos, espías dobles, espías liquidables y espías sobrevivientes. Cuando están los cinco tipos funcionando al mismo tiempo y sus operaciones son clandestinas se denominan la "manipulación divina de los hilos" y es el tesoro de un soberano."[90]

El aspecto más valioso de El Arte de la Guerra de Sun Tzu es que ideo sus estrategias y tácticas a partir de las condiciones reales de la guerra basándose en el pleno conocimiento de los enemigos. Su idea de obtener inteligencia o dar importancia a los hombres que conocen la situación de los enemigos es material.

A lo largo de la historia se han utilizado varias técnicas para llevar a cabo el espionaje, pero las principales han sido por infiltración, una técnica usada para introducir individuos con el objetivo de investigar para conseguir información relativa a planes, actividades y proyectos, la otra técnica más utilizada es la penetración, para conseguir colaboración de los miembros de la organización o grupo contrario para suministrar información secreta.

El espionaje a lo largo de la historia empieza a producir grandes cambios en la manera de establecer sus redes de espionaje tanto de forma interna como

[89] Herrera Hermosillo Juan Carlos, Breve Historia del espionaje, Ed.Nowlitus, Madrid España, 2012, p. 25.
[90] Hanzhang Tao, Sabiduría aplicable a los negocios, Sun Tzu- El arte de la guerra, Ed. Profit, España, 2011, p. 81.

externa, al haber de manera directa operaciones secretas inmiscuidas en la política mundial, como fue el caso de la primera y segunda guerra mundial.

Los servicios de espionaje fueron evolucionando de acuerdo a los avances tecnológicos, desarrollando las actividades de espionaje de forma precisa, con la aparición de herramientas como fue el telégrafo y el teléfono proporcionando una mejora en la comunicación militar y facilitando la interceptación de mensajes enemigos.

Un ejemplo del método de espionaje norteamericano fue tras los atentados del 11 de septiembre de 2001, "se inició un tipo de espionaje que incluía operaciones encubiertas, como la que logró poner fin a la vida de Osama Bin Laden; Con la "Operación Gerónimo", surgió a partir de una alerta proveniente de agentes secretos paquistaníes al servicio de la CIA que situaba a uno de los mensajeros de Osama Bin Laden en la ciudad paquistaní de Peshawar"[91], el sistema de espionaje que utilizaron los servicios de inteligencia fue realizar por varios meses fotografías vía satélite para tener conocimiento de todos los movimientos que se producían en la guarida donde se encontraba Osama Bin Laden.

Aunque las técnicas del modelo tradicional de espionaje se han ido sofisticando con el tiempo para la obtención de información privada, clasificada y en varias ocasiones comprometedora de las instituciones gubernamentales y privadas, abriendo paso al espionaje informático o ciberespionaje como un arma poderosa en el espacio cibernético.

El ciberespionaje no es comparable al espionaje tradicional. Con anterioridad, el espionaje consistía en interceptar un teléfono del enemigo o en interceptar comunicaciones, o bien enviar un espía para que se infiltrara en las instituciones de otro país con el fin de apoderase de información clave y secreta. En cualquier caso, el objetivo de estas acciones era conseguir información, pero en ningún caso se trataba de manipularla ni destruirla.

[91] Ibídem, p. 14.

Para comprender mejor el concepto de ciberespionaje, se definiría como:

> "Una forma de cibercrimen en el que los hackers tienen como objetivo redes informáticas de trabajo para obtener acceso a información clasificada o de otro tipo que pueda producir beneficio o sea ventajosa para el hacker. El ciberespionaje es un proceso continuo que se produce con el tiempo a fin de obtener información confidencial. Puede dar lugar a todo, desde un desastre económico en la banca, bolsa de valores hasta actos terroristas."[92]

Con el ciberespionaje es muy normal que, después de obtener la información se manipule, se borre o la destruya, etc. Así, dentro del ciberespionaje se pueden incluir acciones como, por ejemplo, reconocer los sistemas (obtener información previa sobre las organizaciones y sus sistemas informáticos, para poder escanear sus puertos con el objetivo de determinar qué servicios se encuentran activos, etc.)

El ciberespionaje es un medio de ciberataque con la finalidad de conseguir información, secretos de Estado, propiedad industrial, propiedad intelectual, información comercial confidencial o datos de carácter personal. Este tipo de actos puede llevarse a cabo por el gobierno, centros de inteligencia, policía cibernética, empresas, hackers con un fin político, económico o social.

El ciberespionaje aparece con la creación del sistema Echelon, los orígenes de la red se remontan al final de la Segunda Guerra Mundial, cuando Estados Unidos y Gran Bretaña crearon un sistema conjunto de espionaje e intercambio de información denominado UKUSA, termino resultante de la unión de UK (United Kindom) y USA (United States of America); siendo hasta finales de los años 60´s del siglo pasado cuando se empezó a interceptar y espiar, telecomunicaciones espaciales por antenas satelitales que enviaban señales derivadas de diccionarios automáticos de filtrado.[93]

[92] Btzsercas, Ciberseguridad y ciberespionaje en las relaciones internacionales, Diplomacy Data, disponible en línea: http://diplomacydata.com/cyber-security-awareness-in-public-diplomacy/, Fecha de consulta: 28 de Julio de 2017.

[93] Villanueva López D. Christan, La red Echelon, Ed.Política de defensa y Fuerzas armadas, Revista digital de armamento, 28 de Agosto de 2016, disponible en línea: http://www.ejercitos.org/2016/08/23/la-red-echelon/, Fecha de consulta: 29 de Julio de 2017.

Este método de espionaje sirvió para captar señales y obtener información por medio de antenas satelitales, que eran un procedimiento avanzado en un inicio, con la interceptación de comunicaciones como método de vigilancia y seguridad al bloque de países que optaron por implementar este servicio de inteligencia.

Al convertirse la red de espionaje un proyecto a gran escala, los gobiernos empezaron a experimentar en los procesos de automatización en las estaciones de espionaje para reducir costos y que el sistema de espionaje fuera eficiente, convirtiendo al "[…] sistema Echelon en un sistema automatizado de interceptación global de transmisiones, operado por los servicios de inteligencia de cinco países: Estados Unidos, Gran Bretaña, Canadá, Australia y Nueva Zelanda. Su objetivo principal era controlar las comunicaciones militares y diplomáticas de la Unión Soviética y sus aliados durante la Guerra Fría."[94]

La Alianza conformada por Estados Unidos y Gran Bretaña en un principio llamada UKUSA buscaba el control de las comunicaciones militares y diplomáticas de la extinta Unión Soviética, con el ingreso de los países: Canadá, Australia y Nueva Zelanda denominados el grupo The Five Eyes, pareciera que han cambiado sus estrategias de espionaje enfocándola en la protección de información mediante la recopilación de datos para evitar "complots terroristas", por otra parte sus acciones de espionaje muestran todo lo contrario al ir enfocadas hacia intereses políticos y económicos mediante el dominio de la información.

Con el desarrollo de los sistemas de automatización en la interceptación global de las transmisiones del programa Echelon, fue el escalafón para que las redes de comunicaciones fuera un proyecto ambicioso ya que significó un gran avance en el desarrollo tecnológico al poner en marcha la primera conexión entre ordenadores mediante una red que facilitaría las actividades de espionaje.

[94] Medero Sánchez Gema, El ciberespionaje, Derecom, No. 13, Marzo-Mayo 2013, Ed. Nueva Época, España, p. 117, disponible en línea: http://s3.amazonaws.com/academia.edu.documents/34001413/DialnetElCiberespionaje4330467.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1499300065&Signature=TGvZW1RKw%2BJUMQXbQyLKGYmOEWQ%3D&responsecontentdisposition=inline%3B%20filename%3DEl_ciberespionaje.pdf, Fecha de consulta: 05 de Julio de 2017.

La manera en la que opera el programa Echelon consiste, entre otras cosas, de "palabras clave", las cuales son programadas desde grandes diccionarios y sirven como medio para limitar las búsquedas de sospechosos u objetivos peligrosos.

Sin embargo con el avance de la tecnología se han implementado mejoras en el programa Echelon, permitiendo operar sus bases de espionaje vía satélite por control remoto, operando a gran escala, al permitir monitorear la red e interceptar en todo el mundo millones de comunicaciones a cualquier hora del día. "Para esto se utiliza 120 satélites, potentes computadoras, estaciones de vigilancia en todo el mundo que reciben, analizan y ordenan la información capturada por los satélites de comunicaciones"[95]

En la actualidad se emplea para interceptar todo tipo de transmisiones con el objetivo de localizar actividades terroristas y de narcotráfico e implementar inteligencia política y diplomática. Su funcionamiento se basa en situar múltiples estaciones de interceptación electrónica en satélites y en otros puntos para capturar las telecomunicaciones establecidas por radio, satélite, microondas, teléfonos móviles y fibra óptica. Posteriormente, cada estación selecciona mediante una aplicación palabras clave que supongan un riesgo a la seguridad nacional y guarda toda la información con relación a la problemática que persigue el Sistema Echelon.

"La idea del sistema Echelon es detectar determinadas palabras consideradas "peligrosas" para la Seguridad Nacional de Estados Unidos y de los países participantes de este proyecto, el sistema Echelon intercepta cerca de 1,000 millones de mensajes que posteriormente son filtrados para extraer información que atente a la seguridad nacional de los países participantes."[96]

De acuerdo a la empresa Verizone el ciberespionaje; "supone el 22% de las violaciones de seguridad de los datos, con el 87% del espionaje electrónico

[95] Proponen un sistema de vigilancia en Internet, Nuestra América, 23 de Diciembre de 2002, disponible en línea: http://nuestramerica.info/article/proponen-un-sistema-de-vigilancia-en-internet/, Fecha de consulta: 16 de Julio de 2017.
[96] Ídem.

llevado a cabo por los gobiernos, el 11% por el crimen organizado, el 1 % por competidores y el restante 1% por un antiguo empleado"[97], con estas cifras podemos ver que los países tienen mayor actividad en cuestiones de ciberespionaje y el menor medida pero no menos importante el crimen organizado que ejecutan actividades de espionaje para cometer actos de índole criminal e ilegal.

De acuerdo a las cifras sobre Ciberespionaje, se muestra que "el 87% de espionaje es por la red"[98], permitiendo a los hackers hacer actividades de cualquier índole ya sea legal o ilegal de manera anónima y difícil de detectar por lo cual es complicado detectar las vulnerabilidades en el sistema de forma rápida.

2.3.1 Programas de espionaje y contraespionaje

Los programas de espionaje y contraespionaje en Estados Unidos se han utilizado para combatir actos terroristas que atentan contra la Seguridad Nacional estadounidense debido a que representa la principal amenaza del país; En este sentido las estrategias, acciones y políticas en materia de espionaje y contraespionaje tienen como finalidad preservar la capacidad del Estado para emprender acciones que permitan salvaguardar la Seguridad Nacional de actos que atenten a la seguridad, por medio de filtraciones en instituciones públicas o privadas que puedan manipular los procesos de toma de decisiones y sustraer información confidencial sobre las estrategias, metodologías y acciones orientadas a preservar la Seguridad Nacional.

Cuando se habla de espionaje y contraespionaje, el tema va encaminado a utilizar la información adquirida de acuerdo a los propios intereses de cada Estado para protegerse de ataques en el ciberespacio como es el uso de armas cibernéticas; "Las amenazas que enfrentan los sistemas de espionaje van desde la infiltración hasta el sabotaje de los programas informáticos por parte de individuos u organizaciones, que sean parte de un Estado enemigo o no. Para Estados Unidos,

[97] Ídem.
[98] Ídem.

la defensa contra estas amenazas es primordial para su seguridad y prosperidad ya que requiere que las redes sean seguras, confiables y resistentes. Su infraestructura digital, por lo tanto, se convierte en un bien estratégico, una prioridad de seguridad nacional."[99]

Desde la creación de la CIA, el FBI ha reducido su autoridad dentro de los Estados Unidos. Su función hoy en día es proteger y defender a los Estados Unidos de amenazas terroristas, armas de destrucción masiva o de inteligencia exterior, reforzar las leyes criminales y proveer liderazgo en los servicios de justicia tanto federal, estatal, municipal y a las diferentes agencias internacionales.[100]

Para llevar a cabo la defensa de los valores nacionales el FBI ha tenido que mejorarse en tres áreas fundamentales: la primera es la creación del National Security Branch (NSB), esta organización junta los sistemas de inteligencia, las operaciones de contraterrorismo y la contrainteligencia en una sola área. La misión de la NSB es:

> "Proteger a los Estados Unidos contra amenazas de seguridad nacional actuales y emergentes: armas de destrucción masiva, ataques terroristas, operaciones de inteligencia extranjera y espionaje mediante la integración de actividades de investigación y de inteligencia".[101]

La segunda área de transformación ha sido el sector tecnológico, por ello la *National Security Branch* ha desarrollado tecnología para monitorear e infiltrar información para investigar desde personajes inmiscuidos en la política, grupos ambientalistas, opositores de la guerra o posibles terroristas. Y la última área en la que se basa es el capital humano, mediante el reclutamiento de mejores analistas, lingüistas, programadores, científicos e ingenieros para afrontar posibles amenazas que atenten a la seguridad.

---

[99] Barack Obama, Remarks by the presiden ton securing our nation´s cyber infraestructure", Washington, D.C., 29 de Mayo de 2009, disponible en línea: http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infraestructure, Fecha de consulta: 08 de Mayo de 2017.

[100] Méndez de la Brema Dresna Emma, Biopoder como elemento de seguridad Nacional, Ed. Universidad de las Américas Puebla, Escuela de Ciencias Sociales, Artes y Humanidades, México, 2006, p. 32.

[101] Ídem.

Con la intención de enfrentar actos terroristas la *National Security Agency* brinda servicio al Departamento de Defensa, agencias gubernamentales, contratistas del sector privado que trabajen para el Estado y aliados de Estados Unidos su misión es:

"Prevenir que adversarios extranjeros adquieran acceso a información sensible o clasificada vinculada con la seguridad nacional, así como recolectar, procesar y diseminar información de inteligencia de fuentes externas para propósito de inteligencia y contrainteligencia y para respaldar operaciones militares"[102]

Sobre las medidas de inteligencia que se han utilizado por la NSA, es la que publicó el diario The New York Times en 2008 por medio de la plataforma Skype se puso en marcha un programa que permitiría a los servicios de inteligencia y a las fuerzas de seguridad estadounidenses acceder a las llamadas realizadas a través de esa compañía.

Otra de las medidas de inteligencia por la NSA y el cuartel General de Comunicaciones del Gobierno Británico, en 2007 utilizaron las aplicaciones móviles de Angry Birds y Google Maps principalmente para recabar información personal de usuarios; Por medio de estos sistemas, las agencias pudieron sustraer información proporcionada por el usuario como son los datos geográficos, listas de amigos, correos electrónicos, contraseñas y registros telefónicos de usuarios al enviarles mensajes para la confirmación del uso de las aplicaciones para versiones móviles de Facebook, Linkedin, Flickr y Twitter;[103] por medio de estas plataformas se pudo obtener información de datos geográficos, registros telefónicos, números de cuentas, listas de amigos, donde las redes sociales jugaron un papel importante al permitirle a las agencias de inteligencia formar un perfil de cada usuario y a través de esta forma tener una base de datos para saber si pueden ser los usuarios una amenaza o no.

---

[102] National Security Agency, Mission and Strategy, Mayo 2016, disponible el línea: https://www.nsa.gov/,Fecha de consulta: 8 de Mayo de 2017.

[103] Saiz Eva, La NSA usó aplicaciones como angry Birds o Google Maps para obtener datos, El país, 2014, disponible en línea: http://internacional.elpais.com/internacional/2014/01/27/actualidad/1390854460_566211.html,Fecha de consulta: 08 de junio de 2017.

Las medidas de inteligencia que son implementadas por la NSA y la agencia de inteligencia Británica justifican sus acciones sobre el combate al terrorismo, sin embargo deja entrever que las acciones de inteligencia están enfocadas a obtener una red de vigilancia internacional, mediante la obtención de contraseñas, registros, localizaciones, correos, listas de amigos, redes sociales, etc., de esta manera se pueden formular perfiles de cada usuario que se encuentra en la red para introducir ideas políticas, sociales, religiosas y culturales.

2.4 Amenazas emergentes a la seguridad Internacional en el ciberespacio

Los conflictos bélicos a lo largo de la historia han marcado la pauta al sistema internacional de acuerdo a los intereses de cada Estado; sin embargo, en la actualidad las guerras ya no soló se hacen en un campo de batalla, el uso de las tecnologías de la información y la comunicación juegan un papel importante en la interacción de las relaciones bilaterales de Estados Unidos con el resto del mundo por medio del ciberespacio, que es una red de información que ha traspasado fronteras con el uso de internet, correos electrónicos y redes sociales que son una herramienta indispensable para la vida cotidiana del ser humano para desarrollar sus actividades escolares, laborales y de entretenimiento.

Las amenazas cibernéticas adquieren gran relevancia, gracias a la globalización de las comunicaciones, así como las distorsiones de los medios de comunicación, que son influenciados por la información que circula en las redes sociales, las cuales se han convertido en un factor de penetración social.

Estados Unidos enfrenta un gran reto en su seguridad informática, debido a que la población no tiene una educación óptima sobre el uso de las nuevas tecnologías de la información y la comunicación (TIC) de cómo administrar el uso de la red, lo cual se vuelve en un factor que hace vulnerable al Estado, porque no se toman las medidas pertinentes para evitar ataques de hackers por medio del uso de virus, que permite espionajes desde cualquier punto del planeta en segundos.

Otra amenaza común es: "[…] el uso de las nuevas armas derivadas de las nuevas tecnologías, como los aviones no tripulados (drones) o los artefactos explosivos identificados (IED, por sus siglas en inglés) resultan ventajosas o peligrosas según en qué manos caigan y el uso que se haga de ellas, así como el punto desde donde se vean las cosas."[104]

"Derivado al perfeccionamiento de los ataques cibernéticos, en la administración de Barack Obama se presentó oficialmente la NCTC (*National Counter Terrorism Center* por sus siglas en inglés)"[105] para combatir ciberataques y ciberterrorismo, que puedan provocar un mal funcionamiento en el país por medio de un malware.

Los malware son una amenaza que incrementa apresuradamente en el espacio cibernético, su finalidad es dañar o modificar dispositivos electrónicos, en el siguiente cuadro se desglosan los tipos de malware:

Cuadro 2 Tipos de Malware

Adware	Es publicidad no solicitada, se presenta en forma de pop-ups que presentan algún tipo de publicidad.
Spyware	Es un software espía, en busca de claves, contraseñas e información.
Troyanos	Son programas o herramientas que al ser descargadas contraen virus.
Gusanos	Programa diseñado a replicarse y distribuirse de un equipo a otro rápidamente.
Keyloggers	Permite grabar el texto de la víctima en su teclado, para enviarlo después a una dirección de correo electrónico previamente configurada.

[104] Segura Serrano Antonio, Gordo García Fernando, Ciberseguridad global, oportunidades y compromisos en el uso del ciberespacio, Ed. Universidad de Granada, España, 2013, p. 22.
[105] Vázquez Medina Rubén, "Buenas prácticas para reducir los impactos de amenazas y riesgos de la información en el ciberespacio", Seguridad y Defensa en el Ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p. 258.

Rogge	Simuladores de herramientas de seguridad, pero al ser utilizados, descarga virus
Rootkits	Son aplicaciones que limitan, ocultan o deniegan acceso a los recursos del sistema.
Backdoors	Programas que permiten el acceso al sistema de manera no convencional, ignorando la autentificación.
Hoax	Son mensajes en cadena que se distribuyen con la finalidad de obtener correos.
Spam	Son mensajes no solicitados, que se envían de forma masiva, con el fin de perjudicar al receptor.
Phishing	Duplicación de páginas web con el fin de obtener información confidencial
Botnets	Redes de robots, que se distribuyen en miles y miles de máquinas y en un momento dado el creador puede ordenarles a realizar algo.
Virus informático	Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin permiso o conocimiento del usuario.

Fuente: Elaboración propia, con información tomada de Paloma Parra Luis Orlando, Op. Cit. pp. 36-41.

Debido a las amenazas antes mencionadas se han adoptado prácticas de seguridad, como es el uso del sistema SCADA (*Supervisory Control And Data Acquisition* por sus siglas en inglés) para proteger y establecer controles de seguridad en los dispositivos electrónicos.

2.5 Organismos Internacionales en pro de la ciberseguridad

Con la interdependencia de las operaciones en el ciberespacio, el autor David Moran menciona que las medidas de ciberseguridad se deben adoptar por parte de los Estados de manera multilateral (véase en anexo 1), tanto en el ámbito militar y político para el intercambio de información sobre incidentes cibernéticos que fueron detectados por organizaciones que tienen como principal función

resguardar la seguridad nacional e internacional como es el caso de la Organización del Tratado del Atlántico Norte (OTAN), que busca la seguridad colectiva entre sus miembros.

En la cumbre de Bucarest de 2008, se llegó a un acuerdo expresado en la sección 47 de la declaración de la cumbre:

> "La OTAN se mantiene comprometida con el fortalecimiento de los sistemas de información crítica de la Alianza contra ciberataques. Hemos adoptado recientemente una política de Ciberdefensa, y estamos desarrollando las estructuras y autoridades para llevarla a cabo. Nuestra política en materia de Ciberdefensa subraya la necesidad de la OTAN y de las naciones miembros de proteger los sistemas de información crítica conforme con sus respectivas responsabilidades; compartir las mejores prácticas y establecer una capacidad de apoyo a las naciones, bajo petición, para contrarrestar un ciberataque." [106]

En referencia a la cumbre de Bucarest, se hace énfasis en el fortalecimiento de la OTAN para mejorar la respuesta de acción ante ciberataques, después de lo sucedido en Estonia como se mencionó anteriormente, donde la OTAN no tuvo un plan de acción para la protección de ataques cibernéticos debido a que soló se concentraba en la protección de los sistemas de comunicación propios y los que eran operados por la Alianza.

A partir de la problemática en la cumbre de Bucarest, la OTAN adoptaría medidas de Ciberdefensa para proteger los sistemas de información y comunicaciones de importancia crítica para la alianza frente a los ciberataques, trabajando en conjunto con otros actores como es Naciones Unidas y la Unión Europea.

En 2004 se empieza a tomar medidas para la protección del ciberespacio por parte de la Unión Europea; "Por lo que la UE crea la Agencia de Seguridad de Redes y de la Información de la Unión Europea (ENISA); la creación de la ENISA marca un compromiso con la nueva realidad ya no solo porque se constituye como la agencia de ciberseguridad que asesora la Comisión y a los Estados

[106] Artiles Ganzúa Néstor, "La situación de la ciberseguridad en el ámbito internacional y en la Otan", ciberseguridad retos y amenazas a la seguridad nacional en el ciberespacio, Op cit. p. 203.

Miembros, sino porque impulso la creación del programa Europeo para la Protección de Infraestructuras Críticas en 2007."[107]

Teniendo en cuenta este precedente, "[…] en 2010 se aprueba la estrategia de Seguridad Interior, además de la creación de la "*Digital Agenda for Europe*", esta agenda establece la hojas de ciber-ruta de la Unión y opera en siete campos sobre los que sostiene su acción global: el mercado digital en todos sus espectros, la interoperabilidad y los estándares en tanto construyen la democracia digital, seguridad en el ciberespacio, la velocidad de los accesos a internet, la investigación y la innovación en la TIC, el acceso e inclusión para toda la población y lo digital como beneficio social de la propia UE"[108]

Como bien menciona el autor Gazapo M. Machín, la "Digital Agenda for Europe" sirvió como base para la Estrategia europea de Ciberseguridad teniendo como objetivo principal conseguir un ciberespacio abierto, protegido y seguro para los usuarios europeos, a continuación se mencionaran las cinco líneas de acción establecidas como prioridad en la Estrategia de Seguridad Europea:

- "Incrementar capacidad de ciberresilencia: Comprender que la mentalidad de fortaleza no funciona en el ciberespacio ya que ese se caracteriza por ser una dimensión de carácter abstracto, donde internet es un escenario de conflicto donde desaparece la posibilidad de protegerse mediante una línea ofensiva.
- Reducir el cibercrimen: Creación de un Centro de Cibercrimen Europeo, en colaboración con la EUROPOL, actuando como una plataforma de alerta permitiendo aumentar los canales de información para luchar y prevenir la delincuencia en la red.
- Política común de Ciberdefensa: Trabajar en una política de Ciberdefensa, en coordinación con la Política Común de Seguridad y Defensa (PCSD),

[107] Machín N. Gazapo M., La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea, revista UNISCI Norteamericana, España, 2016, p.59, disponible en línea: http://revistas.ucm.es/index.php/RUNI/article/view/53786/49258, Fecha de consulta: 15 de Noviembre de 2017.
[108] Ibídem, p.60.

mediante una serie de ejercicios de ciberseguridad, a modo de simulacro, que permitan comprobar la validez del sistema de defensa de la red.

- Adquirir un mercado digital único: Desarrollar recursos industriales y tecnológicos necesarios en materia de ciberseguridad mediante un mercado único que sea avalado por las instituciones europeas.
- Política común del ciberespacio: Establecimiento de una política internacional y coherente con la promoción de los llamados valores europeos, promoviendo la democracia e igualdad."[109]

A continuación se mencionaran diversos organismos internacionales que han mostrado actividad en proponer estrategias de seguridad y defensa en el ciberespacio:

La Organización de Naciones Unidas (ONU) como organismo Internacional a favor de la paz internacional se enfocó en la prevención y fortalecimiento de la seguridad: "La ONU en cumplimiento de la resolución 60/45 de la Asamblea General, el Secretario General estableció en 2009 un Grupo de Expertos Gubernamentales sobre los avances en la información y las Telecomunicaciones en el contexto de la seguridad Internacional, con el mandato de formular recomendaciones para fortalecer la seguridad para fortalecer la seguridad de los sistemas globales de información y telecomunicaciones" [110]

"En 2004, en la Organización de Estados Unidos Americanos (OEA) se aprobó la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética en la resolución AG/RES. 2004 (XXXIV-O/04)."[111]

"La Unión Internacional de Telecomunicaciones (UIT) elaboró una guía para los países en desarrollo sobre el ciberdelito, el entendimiento de las ciberamenazas y sus aspectos legales; así como las principales acciones que se han emprendido

[109] Ibídem, p. 61.
[110] Gutiérrez Diego Alonso, "La cultura de la Ciberseguridad. El ciberespacio y la sustentabilidad para conseguir los objetivos del desarrollo del milenio", Seguridad y Defensa en el Ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p.166.
[111] Organización de Estados Unidos Americanos (OEA), Seguridad cibernética, 2004, disponible en línea: https: //www.sites.oas.org/cyber/Es/Paginas/default.aspx, Fecha de consulta: 14 de Abril de 2017.

en cooperación internacional para el manejo de la ciberseguridad, y su entorno en el ciberespacio"[112]

La Organización para la Cooperación y el Desarrollo Económico (OCDE) en 2002 publicó una guía llamada "Hacia una cultura de seguridad" para resguardar la seguridad de la información, con el fin de promover una cultura de seguridad entre todos los participantes para evitar riesgos en los sistemas y redes de información, se establecen nueve principios los cuales deben ser adoptados por cada Estado[113]:

- Concienciación: Los participantes deberán de ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.
- Responsabilidad: Todos los participantes son responsables de la seguridad de los sistemas y las redes de la información.
- Respuesta: Los participantes deben de actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
- Ética: Los participantes deben respetar los intereses legítimos de terceros.
- Democracia: La seguridad de los sistemas y redes de información debe de ser compatible con los valores esenciales de una sociedad democrática.
- Evaluación de riesgo: Los participantes deben de llevar a cabo evaluaciones de riesgo.
- Diseño y realización de la seguridad: Los participantes deben de incorporar la seguridad como un elemento esencial de los sistemas y las redes de información.

[112] Ibídem, p.192.
[113] Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacía una cultura de seguridad, disponible en línea: https://www.oecd.org/sti/ieconomy/34912912.pdf, Fecha de consulta: 18 de Abril de 2017.

- Gestión de seguridad: Los participantes deben de adoptar una visión integral de la administración de la seguridad.
- Reevaluación: Los participantes deben revisar y revaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, practicas, medidas y procedimientos de seguridad.

Con estos principios la Organización para la Cooperación y el Desarrollo Económico (OCDE) busca la participación de los Estados, gobiernos, Instituciones y ONG´s para poder enfrentarse a riesgos y prevenir amenazas desde cualquier punto del espacio cibernético.

CAPÍTULO III: ESTADOS UNIDOS Y SUS ESTRATEGIAS DE CIBERSEGURIDAD A PARTIR DE ATAQUES CIBERNÉTICOS Y FILTRACIONES DE INFORMACIÓN CLASIFICADA.

La seguridad siempre ha existido entre los Estados: Sin embargo, la ciberseguridad era vista como una cuestión tecnológica donde los ingenieros eran los únicos que podían abordar la problemática, hoy en día la seguridad cibernética es un tema importante en la agenda de seguridad de Estados Unidos y de gran preocupación a escala internacional porque engloba la dimensión política interna y externa en cuestiones administrativas y legales referentes a las actividades del gobierno, diplomáticas y asuntos militares, con el fin de resguardar la seguridad nacional y la seguridad de los ciudadanos.

En el siguiente capítulo se explicarán los ataques que ha sufrido Estados Unidos tanto en el sector privado como en el sector público durante la primera administración de Barack Obama, además se detallará la Estrategia de Seguridad Nacional 2010 enfocada al tema de ciberseguridad y cómo combatir las ciberamenazas después del atentado del 11 de septiembre de 2001.

De la misma manera se mostrará las alianzas estratégicas que ha hecho el gobierno estadounidense con el sector privado para implementar herramientas de inteligencia para contrarrestar vulnerabilidades en los sistemas que atenten a la seguridad nacional.

Asimismo se hablará sobre las medidas de ciberseguridad en el ciberespacio, con la implementación de un Cibercomando para la protección de estructuras militares en el flujo y recolección de información, por parte de las medidas de ciberseguridad implementadas por el sector privado se detallara los pros y contra de la estandarización de la información en la red, como medida de ciberseguridad.

.

3.1 Estrategias de Seguridad Nacional frente a las ciberamenazas en Estados Unidos

Estados Unidos es una nación que ha invertido en ciberseguridad debido a las constantes amenazas que se han presentado en el ciberespacio por lo que al adquirir el poder como presidente Barack Obama se aceleraron iniciativas en materia de ciberseguridad que fueron propuestas por su antecesor George W. Bush, después del atentado del 11 de Septiembre de 2001, debido a las vulnerabilidades en la infraestructura informática se impulsó un cambio completamente en la Estrategia de Seguridad Nacional.

La Estrategia de Seguridad Nacional en el Ciberespacio de 2003, fue coordinada y estructurada durante el mandato de George W. Bush, la estrategia tenía como temática principal reorganizar al gobierno federal, estatal, sociedad civil y el sector privado para trabajar en conjunto y asignar un rol en cada área. Al percatarse que todavía había tropiezos en el funcionamiento de los sectores antes mencionados el presidente electo ordenó realizar una revisión exhaustiva sobre el uso del ciberespacio y los servicios de inteligencia.

"En Mayo de 2009 la Casa Blanca publicó la revisión política en el ciberespacio y como tema central era mejorar el funcionamiento de las agencias de inteligencia ante ciberataques y la reducción de amenazas mediante el desarrollo de mecanismos de coordinación entre las diferentes agencias y establecer las funciones de cada una, además se propuso una mayor implicación del gobierno de los Estados Unidos en la regulación internacional de la Ciberseguridad que permitiera una mayor colaboración internacional."[114]

Para conseguir los objetivos marcados, la estrategia de Seguridad Nacional se centró en tres pilares:

[114] Romero Candau Javier, Política y violencia: Comprensión teórica y desarrollo en la acción colectiva, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, España, 2014, p.275.

- Establecimiento y reordenación de las responsabilidades relativas a la seguridad del territorio (Entre las cuales se encuentran también las relacionadas con la ciberdefensa).
- El desarrollo de la legislación relativa a la Seguridad Nacional y la ciberdefensa.
- El desarrollo de planes y estrategias relativas a la Seguridad Nacional:
  - Seguridad del territorio
  - Seguridad del ciberespacio
  - Ejecución de ejercicios periódicos de ciberseguridad
  - Plan Nacional de protección de infraestructuras[115]

Del conjunto de estrategias antes mencionadas, se fijaron cinco prioridades nacionales en materia de seguridad en el ciberespacio:

- Sistema de respuesta Nacional de la seguridad en el Ciberespacio.
- Programa de formación y concientización de la seguridad en el Ciberespacio.
- Asegurar el ciberespacio gubernamental.
- Cooperación nacional e internacional para la Seguridad en el Ciberespacio[116].

El presidente Barack Obama, mostró su inquietud sobre la seguridad en la infraestructura digital norteamericana, considerándola como un activo nacional estratégico, por lo cual:

"En 2010 el pentágono nombró a Keith Alexander director de la National Security Agency (NSA) quien comando el nuevo cibercomando (Cybercom) que se encargaría de conducir operaciones de un amplio espectro para defender las redes militares estadounidenses, dirigir y realizar los ataques que fueran necesarios contra otros países".[117]

[115] Ibídem, p.69.
[116] Ídem.
[117] Aguilar Joyanes Luis, "Introducción Estado del arte de la ciberseguridad", Ciberseguridad Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, España, 2010, p. 30.

De las acciones que se tomaron en la administración de Barack Obama, fueron retomadas de la Iniciativa Integral Nacional de Ciberseguridad (CNCI por sus siglas en inglés) puesta en marcha por George W. Bush, de tal manera que en 2010 se restablecieron los nuevos lineamientos que rige hasta el momento a la ciberseguridad en Estados Unidos; a continuación se detallan los puntos prioritarios de la CNCI:

- Administración Federal Entreprise Network, se establece como una sola red para poder tener una conexión confiable en Internet (TIC por sus siglas en inglés Trusted Internet Connections) que dirige la Oficina de Administración y presupuesto y el Departamento de seguridad Nacional, con la finalidad de establecer capacidades en materia de seguridad y reducir accesos externos los cuales son fuente de inseguridad.
- Implementar un sistema de sensores de detección de intromisiones a través de la red Federal. Este sistema permitirá a las redes de defensa identificar cuando cualquier usuario sin autorización intente acceder a dichas redes en tiempo real e identificar cualquier actividad sospechosa o perjudicial en el tráfico de la red federal, logrando reducir vulnerabilidades y daños al gobierno o empresas que tengan implementado el servicio.
- Coordinar y redirigir los esfuerzos en investigación y desarrollo; Ninguna organización o individuo cuentan con un conocimiento solido en el uso de las herramientas tecnológicas relacionadas en el área cibernética, con esta iniciativa se establece una coordinación financiada por el sector público y privado para actividades en investigación y desarrollo, lo cual permitirá identificar prioridades y asegurar inversiones estratégicas.
- Crear nodos informáticos para conectar centros cibernéticos y prevenir amenazas.
- Desarrollar e implementar un plan de todo el gobierno de contrainteligencia cibernética para detectar, impedir y mitigar amenazas cibernéticas internas y externas, a través de la capacitación de personal en operaciones cibernéticas.

- Crear una cultura educativa en el uso de las nuevas tecnologías de la información y comunicación, no solo en empresas, sino también en las instituciones educativas.[118]

Con la estrategia de seguridad nacional que se siguió de la pasada administración, se agregó otra estrategia que "supuso un antes y un después en el diseño de las campañas electorales y una auténtica revolución comunicativa"[119], la estrategia fue llamada triple "O" (*Obama Online Operation*) la cual contemplo tres ejes básicos:

- Redes sociales, empleando además de su página web, blogs, Youtube, y por supuesto Facebook y Twitter, entre otras, redes sociales dirigidas a usuarios con pocos conocimientos de tecnología;
- Mensajería mediante telefonía móvil (SMS)
- Bases de datos alimentadas por las redes sociales y los SMS[120]

Como se observa en los 3 ejes de la estrategia triple "O", se proponía desarrollar organizaciones locales y descentralizadas que se encargaran de la seguridad en los medios de comunicación, como son las redes sociales y mensajería móvil, provocando descontento social al intervenir las redes de comunicación de manera arbitraria, postergando su implementación durante la primera administración de Barack Obama.

Otro rasgo importante dentro de las estrategias de Seguridad es el ámbito militar debido a la dependencia de las redes como medio de comunicación por lo que se

[118] The Comprehensive National Cybersecurity Iniciative, White House, 2010, disponible en línea: http://www.whitehouse.gov/Issues/foreign-policy/cybersecurity/national-Iniciative, Fecha de consulta: 31 de Mayo de 2017.
[119] Ponce de León y Marcos Enrique Carlos, "Las redes sociales en el ciberespacio como herramienta de la política", seguridad y defensa del ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p. 213.
[120] Ídem

busca “desarrollar alianzas militares entre la OTAN y estados miembros para desarrollar medios y métodos de defensa colectiva en el ciberespacio.”[121]

Entre las líneas de acción que implementa la OTAN entre las autoridades políticas, militares y técnicas en la mejora en sus capacidades de ciberdefensa es la creación de un centro de inteligencia:

“El Centro de Excelencia OTAN de Ciberdefensa Cooperativa (*Cooperative Cyber Defence Centre of Excellence- CCDCOE*), se encuentra ubicado en Tallinn, Estonia, este centro se encarga de la investigación y formación en ciberguerra con personal experto de los diez países que lo patrocinan (Estonia como país anfitrión, Alemania, Eslovaquia, España, EEUU, Hungría, Italia, Letonia, Lituania y Turquía), su finalidad es mejorar la capacidad y cooperación de la OTAN y sus Estados miembros en Ciberdefensa mediante el desarrollo de programas y proyectos que faciliten el análisis se casos reales.”[122]

Con las líneas de acción por parte de la OTAN y los Estados miembro, se planeó hacer un frente hacia amenazas en el ciberespacio, que no pusieran en riesgo a la sociedad y el desarrollo de los países se llevará de forma armónica, por lo cual la OTAN implementó métodos de defensa y contraataque para contrarrestar amenazas que pusierán en riesgo la seguridad internacional.

3.2.1 Alianza estratégica entre el sector público y privado en Seguridad Cibernética.

En los años 90´s del siglo pasado las agencias de inteligencia de Estados Unidos principalmente la NSA contaba con sus propios técnicos en computación, criptógrafos y analistas de información para manejar los sistemas de seguridad cibernética.

---

[121] Sánchez de Rojas Díaz Emilio, Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario, Ed. Ministerio de Defensa, Escuela de Altos Estudios de la Defensa, España, 2013, p. 295.

[122] Caro Bejarano J. María, Nuevo Concepto de Ciberdefensa de la OTAN, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 2011, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI092011ConceptoCiberdefensa OTAN.pdf,Fecha de consulta: 30 de Mayo de 2017.

Sin embargo en los últimos 10 años el sector privado se ha convertido en la piedra angular de la seguridad en el ciberespacio al ser el mayor distribuidor e innovador de herramientas y de capacitación para personal de las agencias de inteligencia estadounidenses.

La CIA y la NSA entre otras agencias reconocidas han recurrido a la subcontratación para el manejo de herramientas de inteligencia como es el uso de espionaje y recolección de datos de usuarios para realizar operaciones técnicas y de vigilancia.

De acuerdo al autor Tim Shorrock:

> *"Over de past ten years, the private sector has become a major supplier of tool and brainpower to the intelligence Community. The CIA, the NSA, and others agencies once renowned for their analysis of intelligence and for their technical prowess in covert operations, electronic surveillance, and overhead reconnaissance have outsourced"*[123]

Para proteger la infraestructura de la información se necesita en apoyo tanto del sector público como privado, durante la primera administración de Barack Obama, la Ciberseguridad ha sido un tema prioritario desde los inicios de su campaña, como es la importancia del uso de internet y los elementos asociados a la infraestructura de la información tanto económica como política de Estados Unidos.

Las empresas de tecnología han jugado un papel importante en la ciberseguridad de Estados Unidos, al proveer de herramientas a las agencias de inteligencia para la fácil detección y prevención de ataques en el ciberespacio, sin embargo con la subcontratación de servicios tecnológicos por parte de las agencias de inteligencia se puede convertir en una vulnerabilidad debido a que las empresas pueden vender sus servicios a cualquier Estado u empresa poniendo en riesgo las

[123] Shorrock Tim, spies for Hire: The secret world of intelligence Outsourcing, Ed. Simon & Schuster, Estados Unidos, 2008, p.11. (Traducción propia), A lo largo de los últimos diez años, el sector privado se ha convertido en un importante proveedor de recursos de inteligencia para la comunidad de inteligencia. La CIA y la NSA entre otras agencias, una vez reconocidas por su análisis de inteligencia y por sus proezas técnicas en operaciones encubiertas, vigilancia electrónica y reconocimiento aéreo, han subcontratado.

operaciones al facilitar la estructura de los software de seguridad y por medio de estos filtrarse.

“Con la finalidad de contrarrestar vulnerabilidades que atenten a la ciberseguridad, el gobierno de Estados Unidos estrecha lazos entre el sector privado y académico creando en conjunto “La Iniciativa Nacional para la Educación de la Ciberseguridad (por sus siglas en inglés NICE)”[124].

Con la finalidad de apoyar en la capacitación y desarrollo de personal para hacer frente a los retos presentes y futuros de la seguridad cibernética mejorando los estándares de calidad mediante mejores prácticas, con el fin de dinamizar y promover una educación cibernética.

Otro ejemplo es la empresa norteamericana CISCO, es líder en el mundo de las comunicaciones, y líder en las áreas de seguridad como: virtualización, investigación, desarrollo de tecnología y acceso a plataformas de almacenamiento llamada *cloud computing* que se empezó a utilizar desde los años 60 sin embargo la empresa CISCO volvió accesible la plataforma desde 2006.

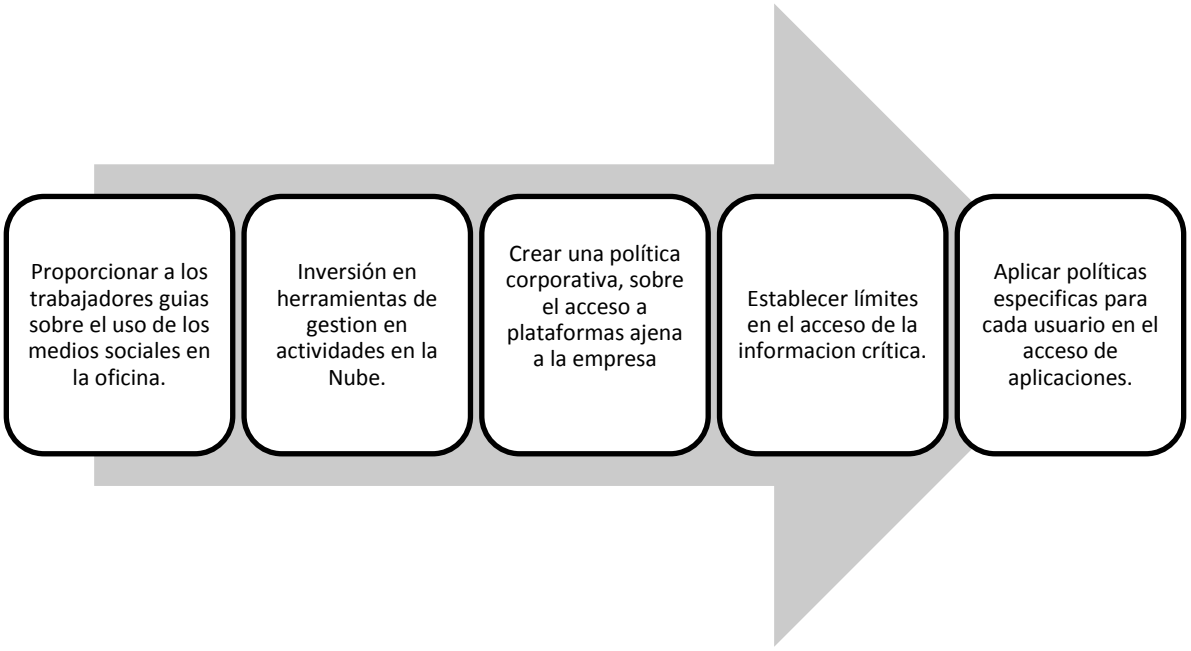
Esta empresa ofrece consultoría sobre los posibles riesgos y amenazas para la ciberseguridad y ofrece soluciones para que no se repliquen los incidentes con el uso creciente de redes sociales, que son utilizadas por grupos terroristas y se han convertido en un campo de batalla para los cibercriminales debido a que los trabajadores dedican la mayor cantidad de su horario laboral en acceder a juegos de redes sociales, lo que no solo produce una pérdida de productividad si no una amenaza latente en los servidores de las empresas, porque se pueden propagar malware a través de estas plataformas y lanzar amenazas que se propagaría en segundos en cualquier parte del mundo.

Debido a esto la empresa CISCO propone un diseño en la ingeniería social (redes sociales) con el uso de las tecnologías para evitar ataques multisectoriales, por

[124] Iniciativa Nacional para la Educación de la Ciberseguridad, 20 de Enero 2016, disponible en línea: https: //www.nist.gov/itl/applied-cybersecurity/nice/about, Fecha de consulta: 02 de Mayo de 2017.

medio de una educación tecnológica, para poder enfrentar los ataques cibernéticos de forma óptima como se muestra en la imagen 5:

Imagen 5 Prevención de Riesgos y amenazas a la Ciberseguridad



Fuente: Elaboración propia con información tomada de Aguilar Joyanes Luis, "Introducción Estado del arte de la ciberseguridad", Ciberseguridad Retos y amenazas a la seguridad Nacional en el Ciberespacio, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, España, 2010, p. 39.

Sin embargo, no todas las empresas tienen el compromiso de resguardar la seguridad informática en el ciberespacio, existen empresas que se dedican a comercializar con vulnerabilidades de los sistemas informáticos sin restricción, al comprar la información a investigadores de seguridad informática y después vender la investigación a entidades de dudosa procedencia o terroristas, para cometer ataques.

El mercado gris en un controvertido negocio en el mundo de la ciberseguridad, es un mercado conformado de manera ilegal, pero establecido de forma legal, volviéndose un problema para la ciberseguridad, al no llevar a cabo los métodos de gestión para tener un buen funcionamiento y evitar ataques.

En el mercado negro no hay ninguna contemplación las vulnerabilidades se venden al mejor postor como lo explica el hacker y experto Deloitte Deepak Daswani: “califica a estas empresas de mediadoras entre el investigador de seguridad y el que quiera comprar la vulnerabilidad. Son compañías que están constituidas legalmente y tienen una actividad declarada, “Es un mercado que existe y es ilícito”.[125]

3.2.2 Medidas de ciberseguridad

El ciberespacio es considerado el quinto dominio de la guerra junto a la tierra, mar, aire y espacio, debido a esto es de gran importancia proteger este espacio intangible, porque es donde se guarda y distribuyen información en la Nube considerada como una de las nuevas infraestructuras tecnológicas.

Por lo cual el ciberespacio es difícil de asegurar por la gran cantidad de actores maliciosos que operan desde pequeñas células en cualquier parte del mundo, un ejemplo de esto es el grupo de ciberactivistas Anonymous, que actúan en su mayor parte desde Estados Unidos, este grupo ha protagonizado ataques cibernéticos muy famosos que han llevado a destruir webs de asociaciones, empresas, corporaciones, y redes del gobierno estadounidenses, en consecuencia el departamento de Seguridad Nacional tiene como objetivo proteger las redes federales conjuntamente con empresas privadas para obtener mejores prácticas de seguridad en el ciberespacio.

De acuerdo a la página oficial del Departamento de Seguridad Nacional, “El Departamento de Seguridad Nacional Trabaja con cada departamento y agencia civil federal para promover la adopción de políticas y mejores prácticas comunes basadas en el riesgo y capaces de responder efectivamente al ritmo de las amenazas en constante cambio”[126]

---

[125] Bejarano G. Pablo, El mercado gris donde la CIA compra armas de ciberespionaje, el país, 14 de Marzo de 2017, disponible en línea: http://tecnologia.elpais.com/tecnologia/2017/03/13/actualidad/1489404727_131065.html,Fecha de consulta: 12 de Junio de 2017.

[126] Homland Security, Security National Network,United States, 16 de Marzo 2017, disponible en línea: https://www.dhs.gov/topic/cybersecurity, Fecha de consulta: 18 de Mayo de 2017.

Sin embargo, el presidente Barack Obama firmó una serie estrategias durante su mandato para usar de manera responsable el ciberespacio:

> "En 2011, se difunde un documento emitido por la casa Blanca firmado por el Presidente Barack Obama, conteniendo la estrategia internacional sobre el ciberespacio, las nuevas tecnologías, el mundo digital y sus aplicaciones. En la estrategia Internacional para el *Ciberespacio (United States of America. May 2011.International Strategy for Cyberspace.Prosperity,Security, and Openness in a Networked World),* se plantea el uso de internet en forma abierta, segura, confiable e interoperable y hace referencia al futuro del ciberespacio, así como a la necesidad de la cooperación internacional."[127]

Otra de las medidas de seguridad que aplicó en Estados Unidos, fue "[…] la prohibición en 2009 al personal del pentágono y a los marines utilizar redes sociales por internet, por ejemplo: twitter, Facebook y Myspace entre otras páginas debido al riesgo que generan en filtración y exposición de información, espionaje."[128]

En 2010 se creó el Cibercomando de Estados Unidos o mejor conocido como: USCYBERCOM, es un comando subalterno el cual entró en operación el 21 de Mayo del mismo año de su creación, está a cargo del general Keith B. Alexander de la Agencia de Seguridad Nacional.

> *"*USCYBERCOM planea, coordina, integra, sincroniza y realiza actividades para: Dirigir las operaciones y la defensa de las redes de información del Departamento de Defensa; Prepara y dirige operaciones militares ciberspaciales para permitir acciones en todos los dominios, garantizar la libertad de acción en el ciberespacio para los Estados Unidos y sus aliados y negar lo mismo a los adversarios.*"*[129]

La función de Uscybercom se centra en proteger exclusivamente las estructuras militares de ciberataques, este cibercomando surge como una medida que hace legítimos a los ciberataques a ejecutar para contraatacar posibles amenazas ya

[127] Seguridad y Defensa en el Ciberespacio, primera Edición, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p.197.
[128] BBC Mundo, Se acabó "Twittear" para los "Marines", 5 de Agosto de 2009, disponible en línea: http://www.bbc.com/mundo/cultura_sociedad/2009/08/090805, Fecha de consulta: 02 de Mayo de 2017.
[129] Fayerwayer, Texto cifrado en el logo de USCYBERCOM, 2016, disponible en línea: https://www.fayerwayer.com/2010/07/codigo-cifrado-en-el-logo-del-uscybercom/, Fecha de consulta: 31 de Mayo de 2017.

que valida el uso de armas en un conflicto o un ciberataque en contra de Estados Unidos que atente a su seguridad, intereses o sus aliados.

El cibercomando se enfoca en tres áreas:

“La primera se enfoca en proporcionar apoyo a los comandantes combatientes en la ejecución de misiones a través de la red por medio de esta función permite un acceso más seguro y confidencial evitando filtraciones sobre las estrategias de combate, la segunda función es fortalecer la capacidad de Estados Unidos para resistir y responder rápidamente a los ataques que cambian constantemente su modificación por lo que se tiene que responder a la amenaza en tiempo real y la tercera área y más importante se enfoca en la protección de la red de Información del Departamento de Defensa (Department of Defense Information Network-DoDIN).”[130]

Del mismo modo el sector privado ha implementado junto con algunos organismos internacionales como el *National Institute of standards and Technology* (NIST) una estandarización de Tecnologías de la Información y en particular con el servidor que concentra enormes cantidades de datos como es La Nube (The Cloud).

> “Con la medida de estandarización de la información, se busca en un futuro el almacenaje de información en internet que se encuentra en blogs, redes sociales, wikis, mashups, etc. y unificar toda la información que será alojada en la nube y se pueda acceder a través de la red.”[131]

El uso de la herramienta en la red llamada Nube, facilita el flujo y almacenamiento de información, estando al alcance de cualquier persona, aunque podría generar un riesgo y una ventaja para los hackers, los cuales podrían interceptar la plataforma por medio de una encriptación de datos para tener acceso y bajar la información de acuerdo a sus intereses.

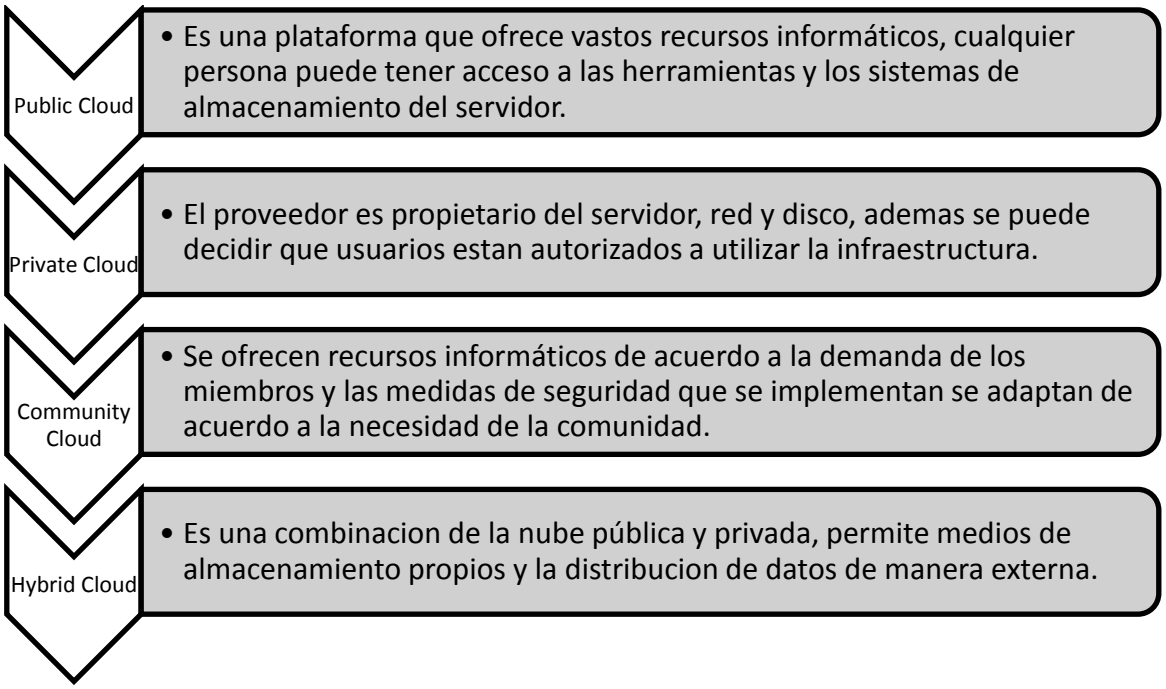
---

[130] U.S. *Strategic Command, U.S. Cyber Command* (USCYBERCOM), 30 de Septiembre 2016, disponible en línea: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/, Fecha de consulta: 01 de Junio de 2017.

[131] Mell Peter, Grance Tim, *Effectively and Securely Using the Cloud Computing Paradigm*, Octubre 2009, disponible en línea: http: //crsc.nist.gov/groups/SN/cloud-computing/cloud-computing-v25.ppt., Fecha de consulta: 08 de Mayo de 2017.

Con el uso de La Nube, cada usuario que se inscriba podrá escoger y configurar el servicio de acuerdo a su necesidad, como se muestra en el esquema 1.

Esquema 1 ***Cloud Computing Option***



Fuente: elaboración propia con información tomada del artículo Computación en la Nube, 2011, p. 50, disponible en línea: http://www.izt.uam.mx/newpage/contactos/anterior/n80ne/nube.pdf, Fecha de consulta: 08 de Mayo de 2017.

Los países miden su ciberseguridad de acuerdo a mayor almacenamiento de datos (Big data y Nube), lo que les permitirá concentrar información y almacenar armas cibernéticas al momento, para defenderse de un ciberataque.

No obstante guardar toda la información en una sola plataforma como es el caso de La Nube, se vuelve un foco rojo debido a que será más atractivo para los hackers filtrarse o generar un colapso a esta infraestructura informática lo que generaría una amenaza latente hacia la ciberseguridad y en particular a la protección de los datos.

3.2.3 Protección de Ciberataques a Infraestructuras críticas

De acuerdo al Departamento de Seguridad interior de Estados Unidos en 2012 creció el número de ataques a infraestructuras criticas; por lo que la legislación propuesta para regular los ataques cibernéticos se vio obstaculizada por los grupos empresariales que temían abusivas regulaciones federales, esto obligó al presidente Barack Obama a decretar medidas para sofocar el ciberespionaje contra las agencias del gobierno de Estados Unidos y empresas estadounidenses reforzando las defensas de la infraestructura critica vulnerables a los ataques cibernéticos.

"El 14 de Febrero de 2012, se presentó ante el Senado de los Estados Unidos un proyecto de Ley sobre Ciberseguridad, la iniciativa proponía aumentar los niveles de ciberseguridad sobre la infraestructura crítica y preparar a los Estados Unidos para soportar ciberataques internos y externos, con el proyecto de Ley se proponía un esquema de seguridad entre el gobierno Federal y el sector privado a fin de evitar un ataque que pudiera paralizar a la nación." [132]

Por otra parte los sectores estratégicos de Estados Unidos son supervisados continuamente, para poder supervisar y mantener el control sobre las infraestructuras críticas; se utiliza el sistema SCADA, el cual "sirve para monitorear y controlar en tiempo real los procesos industriales, redes eléctricas, centrales de generación eléctrica, industrias del petróleo y gas, tratamiento de agua y residuos e industrias farmacéuticas a distancia para reducir riesgos de seguridad; en 2008 empezaron a aparecer programas diseñados para vulnerar la seguridad del sistema SCADA (*Supervisory Control And Data Adquisicion* por sus siglas en inglés)."[133]

El riesgo principal es el desconocimiento del usuario al utilizar interconexiones en la red ajena a la interconexión del sistema SCADA lo que deriva en malas

[132] Nuevo Proyecto de Ley sobre Ciberseguridad en Estados Unidos, 22 de Febrero de 2012, disponible en línea: http://www.telam.com.ar/notas/201202/13568-nuevo-proyecto-de-ley-sobre-ciberseguridad-en-estados-unidos.html, Fecha de consulta: 30 de Mayo de 2017.
[133] Segura Serrano Antonio, Gordo García Fernando, Op. Cit., p. 219.

prácticas de seguridad porque al actualizar el sistema en la red se pueden filtrar varios errores lo que provocaría no tener control en los sistemas operativos.

Debido a las vulnerabilidades que tenía el sistema, se desarrolló una legislación para la protección de infraestructuras críticas, publicada en 2003 llamada Estrategia de Ciberseguridad.[134]

De acuerdo a los autores Segura Serrano Antonio y Gordo García Fernando, dentro de la Estrategia de seguridad, se debe de hacer una aproximación global al problema y tratarlo de forma conjunta entre los países, en la siguiente tabla se muestran los objetivos a desarrollar para el fortalecimiento de la Seguridad Internacional de los países y evitar posibles amenazas.

Cuadro 3 Estrategias de Ciberseguridad

Componente o política de la Estrategia	Objetivos e indicador de la Actividad
Consideración de la Ciberseguridad como un objetivo de Seguridad Nacional.	Resulta absolutamente prioritaria la formulación de políticas globales e integradas, que aglutinen a todas las áreas gubernamentales concernidas, designando la autoridad responsable de su coordinación al más alto nivel posible.
Arquitectura Institucional Formal	Creación y fortalecimiento de las organizaciones con responsabilidades en materia de ciberseguridad, definiendo y delimitando sus funciones y roles y asignando los recursos precisos: presupuestarios y humanos. Las instituciones clave incluirán:

[134] Ídem.

	1) Coordinador de la política de ciberseguridad, al más alto nivel 2) Centro de coordinación operacional y 3) Centro de respuesta a incidentes.
Desarrollo de Capacidades y conocimientos especializados	Necesidad de adoptar “nuevos” enfoques para la ciberseguridad, que deberán centrarse en el desarrollo y/o fomento de instituciones educativas y programas de formación que vengan a satisfacer la demanda de personal especializado, así como la determinación de los presupuestos precisos para fomentar la seguridad en del sector TIC nacional.
Dependencia especial de la comunidad de inteligencia	Tendencia significativa en la mayoría de los países para que las agencias de inteligencia o las unidades de inteligencia militar puedan, de facto, ganar influencia en la orientación general de la ciberseguridad.
Protección de infraestructuras criticas	Desarrollo o mejora de los esfuerzos para proteger los componentes TIC de infraestructura Critica nacionales, lo que implica la identificación y categorización de estas infraestructuras y la asignación de responsabilidad a una autoridad nacional de seguridad.

Coordinación público-privada	Incremento de las medidas para armonizar los esfuerzos del sector privado en materia de ciberseguridad con los planes gubernamentales de ciberdefensa, medidas que pueden ir desde la cooperación informal, a la institucionalización de la cooperación, a través de propuestas regulatorias y normativas.
Alcance Internacional	Incremento de los esfuerzos de muchos países con intereses comunes para establecer posiciones y prácticas de cooperación en materia de ciberseguridad.

Fuente: Ciberseguridad global, oportunidades y compromisos en el uso del ciberespacio, Ed. Universidad de Granada, España, 2013, p. 222.

3.2.4 Herramientas de seguridad que implementa el gobierno con relación a la Ciberseguridad.

Al hablar de ciberseguridad podemos ver que las guerras han cobrado otra dimensión que puede tener los mismos efectos que una batalla tradicional, las técnicas de ataque han ido evolucionando a lo largo del tiempo y sus armas también, en las primeras batallas el uso de arcos, flechas y escudos pasando por fusiles, ametralladoras y tanques hasta llegar a las guerras nucleares y bacteriológicas; Sin embargo la protección de las infraestructuras cibernéticas ha provocado otro tipo de batalla poco convencional llamada ciberguerra.

"Pero en el mundo en el que vivimos dominado por las nuevas tecnologías: hay un nuevo tipo de guerra que puede llegar a ser mucho más destructiva que todas

las demás: la ciberguerra, es decir, trasladar los conflictos bélicos del campo de batalla a internet y a las nuevas tecnologías de la información."[135]

Con la evolución de las amenazas y la proliferación de las ciberarmas con intenciones destructivas, han transformado los parámetros de defensa convencionales y provocando movimientos medulares en el comportamiento de los gobiernos, empresas, organizaciones y el sector militar de las naciones ante un enemigo invisible y difícil de detectar en la red.

Hoy en día Estados Unidos protege su infraestructura cibernética, mediante herramientas de seguridad que llevan a cabo protocolos de seguridad con los cuales se evita vulnerabilidades en el software de seguridad.

Las herramientas de ciberseguridad se crearon con la intención de prevenir, detectar, vigilar, responder de forma oportuna y recuperarse de ataques de forma exitosa; sin embargo no es posible evitar todos los ataques en el ciberespacio por lo cual debe de existir una planificación y preparación de las agencias de inteligencia para que implementen técnicas adecuadas para detectar ataques antes de que ya hayan ocasionado algún efecto además de aplicar de forma oportuna las herramientas de seguridad por medio de la identificación de objetivos sospechosos.

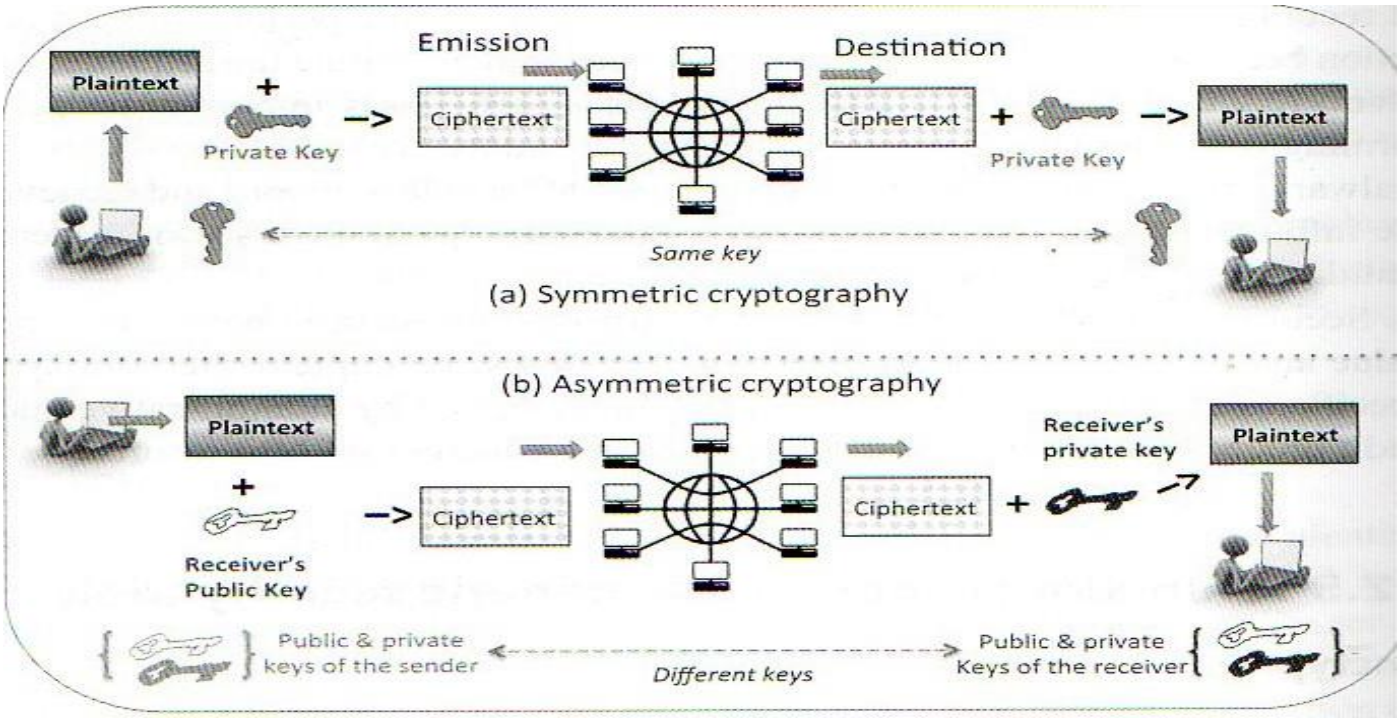
Debido a la dificultad de determinar de dónde proviene un ataque cibernético: El uso de armas cibernéticas, se vuelven esenciales para la supervivencia de cada Estado, la carrera armamentística empezó a cobrar gran importancia en 2006, al ver su gran éxito en 2007 el número de países que se sumaron a la creación y desarrollo de armas de destrucción cibernética fue aumentando rápidamente a 150 países, de los cuales 30 han incorporado unidades cibernéticas dentro de sus ejércitos.[136]

[135] Gutiérrez del Moral Leonardo, Curso de Ciberseguridad y hacking ético, Ed. Punto Rojo Libros, S.L., Sevilla España, 2014. p. 15.
[136] Coleman G. Kevin, Private sector- Military Collaboration Vital to Confront Cyber Threats ,19 de Marzo de 2010, disponible en línea: http://www.defensetech.org/1010/04/19/private-sector-military-colaboration-vital-to-confront-cyber-threats/, Fecha de consulta: 09 de Mayo de 2017.

Sin embargo, una forma de evitar vulnerabilidades en los servidores de la infraestructura cibernética nacional es utilizando como herramienta fundamental "el cifrado de datos también conocido como encriptación, "[…] es un conjunto de métodos para lograr que el mensaje original sea indescifrable, en su caso, difícil de encontrar por estar oculto, y con ello asegurar la confidencialidad del mismo ante los ojos de un interceptor que es capaz de ver el mensaje"[137]

Mediante este proceso permite la operación de servicios que garanticen la confidencialidad de los datos almacenados o transmitidos en los servidores por el medio de autentificación de entidades con el uso de una clave "secreta".[138] Es un método de defensa, alerta sobre posibles ataques de hackers que quieran romper candados de seguridad (contraseñas); en la siguiente imagen 6 se muestra cómo funciona el sistema de encriptación:

Imagen 6 Sistema de Encriptación



Fuente: Ghernaouti Solange, Cyberpower, crime, conflicto and security in cyberespace, Ed. CRC Press, EE.UU, 2006, p. 382.

[137] Arreola García Adolfo, Ciberespionaje: La puerta al mundo virtual de los Estados e Individuos: una revisión de los programas de espionaje digital de los Estados Unidos, Op cit., p. 38.
[138] Ghernaouti Solange, Cyberpower, crime, conflicto and security in cyberespace, Op. Cit., p.382.

Las agencias de inteligencia junto con el sector privado han creado diferentes herramientas de inteligencia para tener un mejor control del territorio y de la población, como es el sistema de video vigilancia que se utiliza para espacios urbanos, públicos y privados, este método se utiliza en tiempo real y se puede monitorear desde cualquier espacio, sin importar la distancia.

Por otra parte, el sistema de Biometrics: es una herramienta sofisticada, la cual toma características físicas o personales para identificar a un individuo, "principalmente se utiliza para controlar accesos en los aeropuertos, prevenir la suplantación de identidad así como también prevenir fraudes, robos de documentación o identificación de posibles terroristas, por medio de huellas digitales, rostro y voz."[139]

Entre las herramientas de vigilancia de la NSA, el programa secreto Xkeyscore que se utiliza en la web, hasta ahora es uno de los más eficaces, este programa permite vigilar en tiempo real en el mundo entero de los correos, la utilización de las redes sociales o cualquier otra acción que se efectúen internet, afín de poder, y luego llegar hasta cualquier internauta considerado un blanco.

"Xkeyscore permite que un agente de la NSA acceda a correos durante un determinado periodo, además este programa es capaz de encontrar criminales o terroristas hasta entonces desconocidos por los servicios de inteligencia, descubriendo en el tráfico de internet lo que los analistas llaman "anomalías""[140]; Xkeyscore a pesar de ser una herramienta utilizada además de ser eficaz para los servicios de inteligencia norteamericanos y evitar ataques terroristas, ha causado gran controversia por el uso indiscriminatorio en la red.

Otra herramienta que se ha creado para la protección en la infraestructura cibernética es Cybercity esta herramienta tiene como finalidad preparar a los piratas informáticos del gobierno para mantener su posición y contraatacar

[139] Woodward, John D., Super Bowl Surveillance. Facing up to Biometrics, Ed. RAND: arrollo center, Santa Mónica, Estados Unidos, 2001, p.4.
[140] Antoine Lefébure, El caso Snowden, así espía Estados Unidos al mundo, Primera edición, Ed.Le monde diplomatique, Argentina, 2014, p. 177.

simultáneamente hasta que a largo plazo se pueden encontrar soluciones a las vulnerabilidades en el sistema informático.

"Cybercity es un entorno virtual, que recrea una ciudad y su infraestructura critica, lanzando en los últimos años por los investigadores militares, empresariales y académicos para hacer frente a los increíbles retos de seguridad que plantea el ciberespacio."[141]

Con el programa Cybercity se podrá hacer una simulación de operaciones en el ciberespacio de manera virtual donde personal especializado podrá realizar operaciones de ciberseguridad en tiempo real lo que dará una mayor ventaja en las operaciones reales, debido a la preparación eficaz de personal informático de las diferentes agencias de inteligencia estadounidenses.

También otro sistema que está creando el "*National Cyber Range* (Cibercampo Nacional) es un simulador de ciberataques de potencias extranjeras y de piratas informáticos con base en Estados Unidos el cual es supervisado por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA), este simulador servirá como un campo de pruebas de tecnologías ofensivas y defensivas, tales como los sistemas de protección de redes."[142]

Con este prototipo, los investigadores de los centros de inteligencia podrán llevar a cabo experimentos continuamente, a diferencia del sistema de internet real, el modelo de este simulador se podrá reiniciar y podrá ser reconfigurado prueba tras prueba.

No solo se ha invertido en el desarrollo para asegurar la infraestructura cibernética, sino también se ha optado por la creación de dispositivos más eficaces y con mayor alcance como es el uso de artefactos aéreos no tripulados.

---

[141] Benedicto Soslana A. Miguel, EEUU ante el reto de los ciberataques,Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 2013, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO372013_Ciberataques_BenedictoSolsona.pdf, Fecha de consulta: 30 de Mayo de 2017.

[142] BBC Mundo, El nuevo campo de entrenamiento para las ciberguerras,18 de Junio de 2011, disponible en línea: http://www.bbc.com/mundo/noticias/2011/06/110617_eeuu_ejercito_ciberataque_ciberguerra_internet_jg.shtml, Fecha de consulta: 10 de Junio de 2017.

Un ejemplo de estos artefactos son los aviones no tripulados reafirmando la superioridad tecnológica de Estados Unidos comparada con Alemania, Francia, Inglaterra, por su renovación constante de su armamento, incluyendo aviones espía: “En 2009 se invirtió en el mayor avión espía no tripulado del mundo llamado Global Hawk, el cual tiene una envergadura de 35,2 metros y puede volar a 20,000 metros de altura durante 42 horas ininterrumpidas y sin piloto, permitiendo enviar imágenes de alta resolución en tiempo casi real”[143]

En años posteriores no se contaba con la tecnología que hoy en día está avanzando aceleradamente, como es el uso de drones, esta herramienta es de bajo costo, tamaño y difícil de detectar, lo que hace más seguras las operaciones de seguridad y militares, debido a que los drones se pueden manejar a larga distancia desde el ciberespacio donde se observa en tiempo real las operaciones desde cualquier ordenador.

La capacidad de un dron es impresionante, relativamente por su tamaño y bajo costo, siendo una herramienta para las operaciones de ciberseguridad, ejemplo de ello fue la operación contra el crimen organizado para atrapar a Osama Bin Laden, quien fue vigilado sobre sus movimientos durante varios meses.

“Los Drones son artefactos voladores no tripulados; de diferentes formas, dimensiones, capacidades y funciones; dotados de cámara de video, sensores y equipos informáticos hasta sistemas de armas avanzadas especiales; manipulados a control remoto, desde un perímetro relativamente corto o en dado caso muy larga distancia facilita su manipulación; son utilizados tanto en el campo de batalla como en espacios civiles nacionales y extranjeros; su operación consiste en la observación y el espionaje hasta la perpetración de ataques a puntos y blancos específicos, materiales y humanos.”[144]

---

[143] Sánchez Hernández Carlos, Las Nuevas Doctrinas Militares, El espionaje Aéreo y la Tecnología en la Guerra (2001-2008), De Hanoi a Bagdad, Vol. 19, No.3, Revista Critica de Ciencias Sociales y Jurídicas, Universidad Complutense de Madrid, España 2008, p.14.

[144] Rosas González María Cristina, La guerra de los Drones, Etcétera, 18 de Septiembre de 2013, disponible en línea: http://www.etcetera.com.mx/articulo.php?articulo=21586, Fecha de consulta: 09 de Mayo de 2017.

Dentro de las características de los drones son su alcance, interoperabilidad, imperceptibilidad, velocidad, equipamiento, flexibilidad, precisión, secrecía, potencia de fuego, funcionamiento prolongado sin reabastecimiento, capacidad de transmitir imágenes o videos en tiempo real, convirtiendo este vehículo no tripulado en una gran herramienta para obtener información y cambiar el rumbo de las batallas tanto físicas como virtuales.

El uso de los vehículos no tripulados es un proyecto que ha sido considerado por el Departamento de Defensa de los Estados Unidos como medida de ciberseguridad que se ha ido ampliando su uso para luchar en guerras futuras a larga distancia por medio de la infraestructura informática.

Los vehículos Aéreos No Tripulados (VANT) más utilizados por Estados Unidos son: "El *Predator* MQ-1B y el MQ-9 *Reaper*. Estos dispositivos se crearon con la finalidad de proporcionar información de inteligencia, vigilancia y reconocimiento combinado con la capacidad de asesinar.

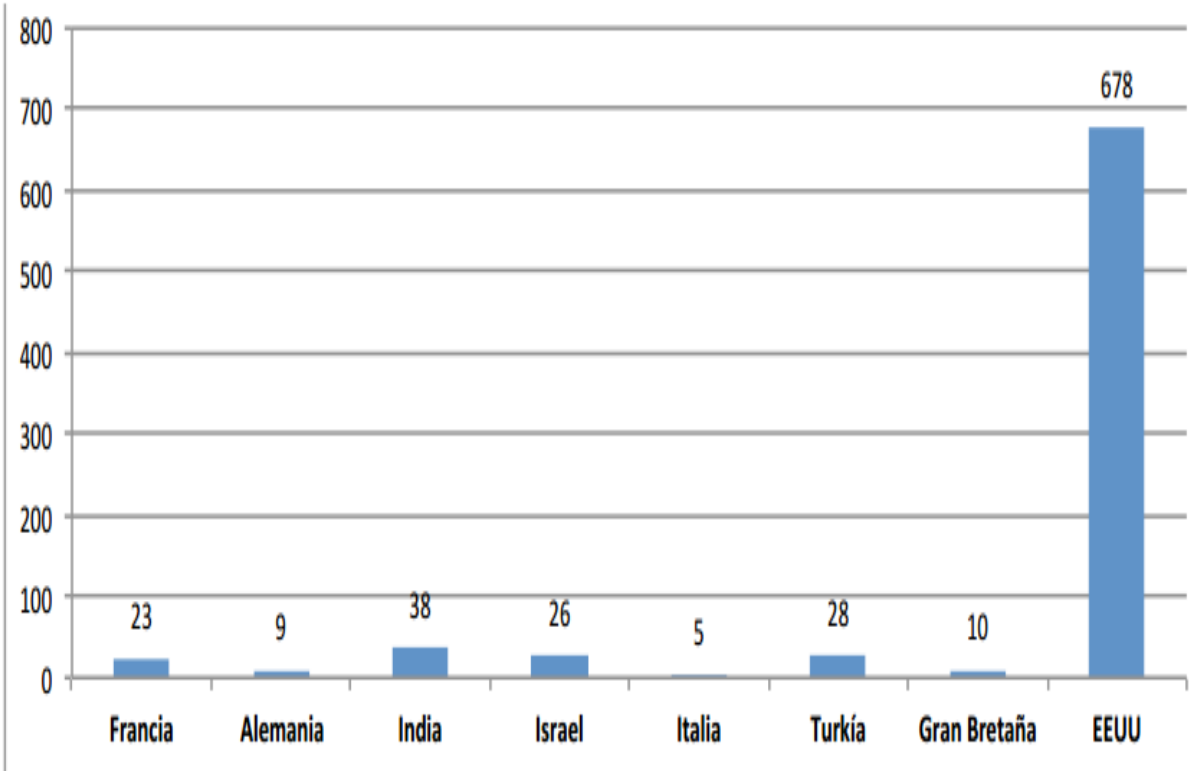
El dron *predator* MQ-1B fue el primer VANT armado del mundo y quizás su mejor cualidad es que puede estar veinticuatro horas en el aire, volando a una altura de hasta ocho kilómetros. El MQ-9 *Reaper* es más grande y más poderoso que el *predator* MQ-1 y está diseñado para procesar objetivos con persistencia y precisión".[145]

EE.UU ha articulado una red global de bases de drones que permiten un rápido despliegue de tales artefactos, contando para ello con un operativo para controlar el dron durante el vuelo que no se encuentra en la base desde donde se despliegan debido a que se cuenta con equipo especialmente para la supervisión de despegue y aterrizaje, además de un sistema de municiones y un sistema de mantenimiento rutinario del equipo.

[145] Calvo Jordi, Escoda Anna, Blanco Carlos, Serra Gabriela, Drones militares, la Guerra de videojuegos con victimas reales, Ed. Centre DeLàs D´Estudis Per La Pau, Barcelona, 2014, p. 8.

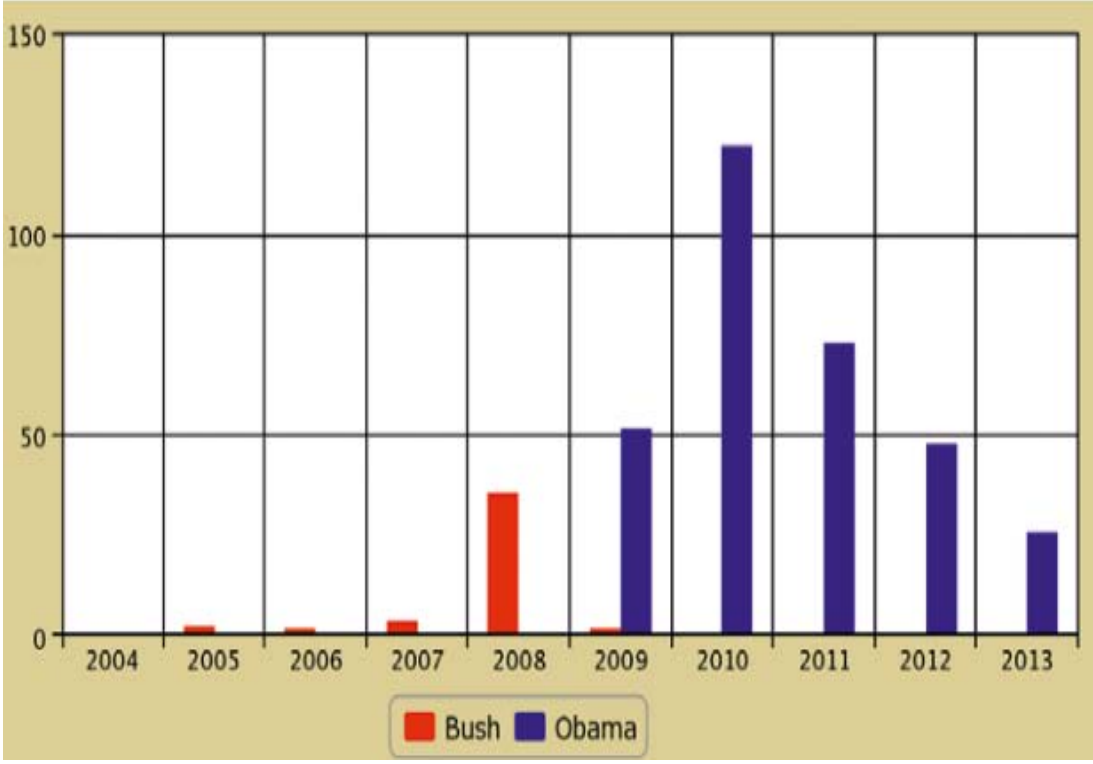
En la gráfica 1 se muestra el uso de drones como herramienta de vigilancia, espionaje y como medio de transporte de armas de largo alcance para operaciones militares, aunque varios países han introducido su uso, el mayor número de drones lo tiene Estados Unidos a comparación de países como Francia, Alemania, India, Italia, Turquía y Gran Bretaña.

Gráfica 1 Stock de Drones



Fuente: The Guardian, disponible en línea: http: //warlaws-pace.com/category/drones, Fecha de consulta: 05 de junio de 2017.

Gráfica 2 Ataques de drones de EE.UU. de Bush a Obama



Fuente: New American Foundation, The year of the Drone, 2007, disponible en línea: http://counterterrorism.newamerica.net/drones/2007, Fecha de consulta: 05 de junio de 2017.

Como se muestra en la gráfica número 2, el uso de drones fue en aumento a partir de 2008 con la administración de George W. Bush, sin embargo en 2009 se empieza a ver un aumento en el manejo de estos dispositivos de largo alcance como son los drones, causando gran controversia en el escenario internacional debido a las regulaciones internacionales que prohíben el uso de armas aéreas en órbita provocando incertidumbre sobre el mantenimiento de la paz y seguridad internacional.

"En abril de 2010 diversos medios de prensa informaron que un dron norteamericano se había lanzado al espacio exterior, el X37B. Posteriormente, se reportó que el 16 de junio de 2012 había concluido un segundo vuelo de un modelo X37B que duro 469 días en órbita y que en diciembre de 2012 se llevaría a

cabo un tercer vuelo. Esto supuso una nueva etapa en el concepto del alcance de los drones sobre una posible guerra armamentística en el espacio exterior"[146]

El uso de drones ha generado diferentes posturas en el entorno internacional, puesto que hay regulaciones sobre la utilización de armas en el espacio exterior ejemplo de ello es la Resolución de 1884 aprobada por la Asamblea General de las Naciones Unidas el 17 de Octubre de 1963:

> "Articulo IV: Los Estados parte en el tratado se comprometen a no colocar en órbita alrededor de la tierra ningún objeto portador de armas nucleares ni de ningún otro tipo de armas de destrucción de masa, a no emplazar tales armas en los cuerpos celestes y a no colocar tales armas en el espacio ultraterrestre en ninguna otra forma."[147]

Con esta regulación se busca una cooperación internacional para mantener la seguridad y paz internacional mediante medidas para regular el uso de armamento nuclear, bajo la jurisdicción del Derecho Internacional y la Carta de Naciones Unidas.

Desde el punto de vista de la ciberseguridad, estos dispositivos también están expuestos a riesgos de perdida de confidencialidad, integridad y disponibilidad. Sobre todo por el uso de tecnologías y sistemas informáticos, que pueden ser susceptibles a ser vulnerados en el ciberespacio al ser usados.

Otro punto que se toma en cuenta es la desmilitarización en el espacio exterior, lo que incluye la prohibición de colocar en órbita armas de destrucción masiva y de establecer bases militares en los cuerpos celestes, debido a que las actividades que desarrollen los Estados son de interés internacional sobre las repercusiones y afectaciones que puedan suceder.

---

[146] Villamizar Lamus Fernando, Drones: ¿Hacia una guerra sin regulación jurídica internacional, Revista de Relaciones exteriores, Estrategia y seguridad vol. 10, núm.2, Ed. Universidad Militar Nueva Granada, 2015, disponible en línea: http://www.redalyc.org, Fecha de consulta: 05 de Junio de 2017.
[147] Ídem.

3.3 Estrategias de seguridad ante filtraciones de cables diplomáticos Wikileaks

El sitio web WikiLeks fue fundado por su editor Julián Assange en 2006 y puesta en marcha oficialmente en 2007, se caracteriza por ser una página que filtra documentos de carácter confidencial de Estados Unidos; En la página se publica información relacionada con temas políticos, militares, religiosos y sociales. Sus revelaciones han impactado a nivel internacional poniendo en riesgo la seguridad nacional y las relaciones bilaterales de Estados Unidos.

De acuerdo a la página oficial "WikiLeaks se especializa en el análisis y publicación de grandes conjuntos de datos de materiales oficiales censurados o restringido de otro modo que implica la guerra, el espionaje y la corrupción. Se ha publicado más de 10 millones de documentos y análisis asociados."[148]

El nombre WikiLeaks proviene del prefijo Wiki que significa la posibilidad de editar el contenido de una página web por los usuarios que acceden a ella (no solo por el dueño de la misma), y el prefijo Leaks que significa filtraciones[149]; teniendo como propósito facilitar la publicación y difusión masiva de información restringida, sin embargo cabe aclarar que en el portal WikiLeaks, no es posible editar contenido debido a que es verificada la información y posteriormente se sube al portal los documentos para que sean consultados.

El objetivo de la creación de WikiLeaks, es el combate a la censura informativa, por lo que Julian Assange crea la plataforma como medio de información internacional, donde todo el usuario que acceda al portal pueda informarse y crear su propia opinión acerca de los documentos publicados.

Sin embargo como bien menciona el Mtro. Juan Daniel Garay Saldaña "la organización WikiLeaks a pesar de que se autodenomina como una organización

[148] Wikileaks, ¿Qué es Wikileaks?, Noviembre 2015, disponible en línea: https://wikileaks.org/What-is-Wikileaks.html, Fecha de consulta: 08 de Mayo de 2017.
[149] Salvador Carrasco de Luis, Internet, Filtraciones y Wikileaks, Diciembre 2010, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2010/DIEEEO25_2010Wikileaks.pdf, Fecha de consulta: 08 de Mayo de 2017.

activista que utiliza la web para dar a conocer de forma masiva millones de documentos que han sido filtrados de forma anónima y que son publicados en la página de la organización, lo cierto es que WikiLeaks no se trata como muchos creen de hackers es decir de expertos en informática que se infiltran en páginas de gobiernos o empresas para extraer información como si lo hace por ejemplo Anonymous"[150], más bien recopila documentos que son enviados de manera anónima mediante una herramienta llamada Whistleblowing con la cual se verifica la información.

Otro rasgo importante del portal WikiLeaks, es su funcionamiento implementando la medida Whistleblowing con lo cual se intenta romper barreras en el filtrado de información en el ciberespacio, su operación se basa mediante "esquemas de anonimato, protección de las fuentes, verificación de información, estudio de las consecuencias legales y difusión viral".[151]

En 2009 en la página web de WikiLeaks se publicó medio millón de cables informáticos, que segundo a segundo fueron emitidos y recibidos en los servidores, esta información causó controversia por la publicación de mensajes intercambiados durante el atentado del 11 de septiembre a las torres gemelas y en la sede del Pentágono, la mayoría de los mensajes fueron emitidos por el FBI y la policía de New York.

Varios de los cables filtrados han sido por analistas de inteligencia como es el caso del soldado Bradley Manning, que fue acusado de filtrar a una fuente no autorizada como es el portal wikiLeaks; "El soldado Bradley Manning fue asignado a una unidad del ejército en Bagdad (Irak), teniendo acceso directo a bases de datos usadas por el gobierno estadounidense para transmitir información clasificada, una de las primeras revelaciones fue el video llamado *Collateral Murder* donde se puede observar una matanza de varios civiles y dos trabajadores

[150] Garay Saldaña Juan Daniel, La Política de Seguridad en Norteamérica post 11-S: del Homeland Security a WikiLeaks, Tesis de Maestría en estudios México- Estados Unidos, Universidad Autónoma de México, Facultad de Estudios Superiores Acatlán, México, D.F., 2014, p. 173.
[151] Julián Assange, Jacob Apelbaum, Andy Muller-Maguhn y Jeremie Zimmermann, Cypherpunks: La libertad y el futuro de internet, Ed. Deusto, España, 2013, p.7.

de la agencia de Reuters en Irak de 2007 y el video del ataque aéreo en Granai (Afganistán) en 2009, además de filtrar 250,000 cables diplomáticos de Estados Unidos y 500,000 informes del ejército que llegaron a ser conocidos como registros de guerra en Irak y registros de guerra afganos."[152]

En el portal WikiLeaks se pueden ver el video clasificado por parte de los Estados Unidos sobre el asesinato indiscriminado en la guerra de Irak en dos versiones la original consta de 38 minutos (https://www.youtube.com/watch?v=fNQ0vaghu8g) y la versión corta que dura 17: 45 minutos y contiene un análisis inicial (https://www.youtube.com/watch?v=5rXPrfnU3G0), ambos videos constan con subtítulos.

Aunque el portal WikiLeaks tiene un sistema de anonimato llamado Whistleblowing, los datos del soldado Manning se dieron a conocer por un hacker informático llamado Adrián Lamo quien fue amigo del soldado Manning, coopero con el departamento de Defensa de Estados Unidos declarando que el soldado Bladley Manning había comentado en un chat en línea que había descargado material de las bases de datos estadounidenses y las había pasado al portal WikiLeaks de manera anónima para que fuera publicada la información.

Al darse a conocer la información el soldado Manning fue detenido el 26 de Mayo de 2010 en una base militar de Arifjan (Kuwait), "enfrenta una condena de 35 años de cárcel por la mayor filtración de documentos diplomáticos y militares secretos de la historia de Estados Unidos, el soldado Manning se enfrentaba a una sentencia de 90 años en prisión por los veinte delitos de los que fue encontrado culpable por la Juez, entre las acusaciones que enfrenta, son la violación de la Ley de Espionaje, robo y fraude informático."[153]

[152] Biography Bradley Manning, 2013, disponible en línea: http://.org/stealing-secrets/ss-bradley-manning.pdf, Fecha de consulta: 28 de Agosto de 2017.
[153] El país, El soldado Manning, condenado a 35 años por las filtraciones a Wikileaks, 22 de Agosto de 2013, disponible en línea: https://elpais.com/internacional/2013/08/21/actualidad/1377090640_718161.html, Fecha de consulta: 28 de Agosto de 2017.

Durante el juicio el ex soldado Manning se declaró culpable y pidió perdón por la filtración de documentos de las guerras de Irak, Afganistán y cables del Departamento de Estado, al ver los problemas de identidad a los cuales se enfrentaba debido a su cambio de sexo y sus intentos de suicidio en dos ocasiones en una cárcel de Kansas, la Casa Blanca reconoció la importancia del arrepentimiento del Bladley Manning para reiniciar su vida con su trasformación como mujer, por lo cual el presidente Barack Obama conmuto su condena de 35 años a 7 años.

"Barack Obama a finales de su mandato tomo la decisión de reducir la condena de 35 de cárcel a siete años a Chelsea Elizabeth Manning, por lo que fue liberada el 17 de Mayo de 2017 debido a sus muestras de arrepentimiento y de su reconocimiento que puso en peligro la seguridad de Estados Unidos."[154]

Dentro de las filtraciones que hizo el soldado Manning que han causado conmoción en el escenario internacional fueron las filtraciones de 2010 las cuales hizo llegar al portal WikiLeaks y posteriormente se publicaron los informes que fueron considerados como la mayor filtración de documentos que fueron sacados a la luz a lo largo de la historia, estos informes se volvieron controvertidos porque contenían información sobre abusos del ejército y el gobierno norteamericano en la guerra de Irak en cuanto a sus operaciones de ataque, a continuación se explicara las publicaciones que tuvieron mayor auge:

The war logs (Documentos de la guerra de Irak): El viernes 22 de Octubre de 2010 en el portal WikiLeaks publicó 391.832 informes militares de la guerra de Irak, donde se desprende detalladamente las muertes de civiles y tropas iraquíes.

Cablegate (Cables del Departamento de Estado Norteamericano): El 28 de noviembre de 2010 se filtró a la prensa internacional 251.187 cables diplomáticos del departamento de Estado estadounidense con sus embajadas en todo el mundo, así como representaciones en organismos internacionales.

[154] El país, Obama conmuta la pena de la soldado Chelsea Manning, 18 de Enero de 2017, disponible en línea: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245. html, Fecha de consulta: 17 de Noviembre de 2017.

“Dentro de estos cables se encuentran comunicaciones de la Administración Central estadounidense hacia sus diplomáticos y viceversa, comunicaciones de las diferentes embajadas de los Estados Unidos que abarcan un periodo de diciembre de 1966 hasta febrero de 2010, aunque se centran principalmente en los años 2008 y 2009; En estos cables diplomáticos se revela conflictos diplomáticos y se muestran evidencias de cómo operan las 274 embajadas estadounidenses en todo el mundo.”[155]

“De los 251.187 cables filtrados 15,652 están clasificados como “secretos” , 9,000 de los cables están identificados como “NOFORN” que es la abreviación para la identificación de información delicada para ser compartida a la sociedad o en algún Estado, 4,000 cables están en carácter de “secretos” y 101, 748 están clasificados como “Confidenciales” mientras que el resto de los informes, es decir, 133,887, se encuentran en la categoría de no clasificado y ninguno de ellos está marcado como “top secret””[156]

Los cables obtenidos por WikiLeaks son confidenciales, considerados por Estados Unidos, como un nivel de clasificación bajo que generaría un daño razonable a la seguridad internacional, a comparación de un cable con categoría *“top secret”* que sería considerado un daño grave a la seguridad nacional.

“La información exhibida por wikiLeaks es corroborada a través de un análisis forense de cada documento: se determina tipo de falsificación y los costos de difusión, medios, motivos de la filtración, se hacen preguntas detalladas sobre el contenido, al igual que se puede recurrir a una verificación externa de la información lo cual consiste en enviar un equipo de periodistas a entrevistar a las personas afectadas u observadores de ser posible, al igual que buscar otras

[155] El país, Preguntas y respuestas sobre los papeles del Departamento de Estado, 28 de Noviembre de 2010, disponible en línea: http://internacional.elpais.com/internacional/2010/11/28 /actualidad/1290898811_850215.html, Fecha de consulta: 17 de Noviembre de 2017.
[156] Shane Scott, Lehren W. Andrew, Leaked Cables Offer Raw Look at U.S. Diplomacy, New York Times, 28 de Noviembre de 2010, disponible en línea: http://www.nytimes.com/2010/11/29/world/29cables.html?_r=1&hp,&pagewanted=1&, Fecha de consulta: 11 de Mayo de 2017.

pruebas que corroboren la verdad de la historia, sin embargo, aceptan que puede haber errores en este proceso aunque hasta el momento no se han dado casos"[157]

El portal WikiLeaks, además de hacer análisis forenses a cada documento también tiene como prioridad mantener la confidencial de los informantes que facilitan sus investigaciones; por lo cual se creó un software de 256 bit llamado MediaWiki, el cual es un método muy avanzado en la encriptación similar a la que es utilizada por agencias de inteligencia y militares.[158]

Debido a estas publicaciones el gobierno de Estados Unidos inició una investigación criminal con todas las agencias de inteligencia, sobre Julián Assange y el personal de WikiLeaks por entrar en los servidores institucionales y extraer información confidencial.

WikiLeaks es una plataforma que ha tenido gran relevancia y diferentes posturas en el ciberespacio, de acuerdo con Valérie Guichaoua: La postura de wikiLeaks va más allá de "Izquierda o "derecha", su lucha es específicamente en contra del individualismo y de las instituciones corruptas, y su trabajo se orienta al establecimiento de gobiernos éticos y abiertos.

La plataforma WikiLeaks "basa su trabajo en la defensa de la libertad de expresión y de publicación de los medios de comunicación, afirma que cada persona tiene derecho a la libertad de opinión y de expresión; este derecho incluye la libertad de sostener opiniones sin interferencia y de buscar, recibir y difundir informaciones e ideas por cualquier medio y sin consideración de fronteras."[159]

El éxito de wikiLeaks se debe en gran medida a sus colaboradores, ya que gracias a ellos la plataforma ha logrado un alcance internacional sobre la información clasificada que se da a conocer en el portal.

---

[157] About Wikileaks, 2010, disponible en línea: http://wikileaks.org/about.html, Fecha de consulta: 11 de Mayo de 2017.
[158] Miller Jones, R. Edward, WikiLeaks, Removing the Top secret seal, Ed.Fastbookpublishing, Estados Unidos, 2010.
[159] About WikiLeaks, 2010, disponible en línea: https://wikileaks.org/About.html, Fecha de consulta: 17 de Noviembre de 2017.

A continuación, se muestra en el siguiente cuadro los colaboradores de wikiLeaks provenientes de todo el mundo, los cuales tienen amplios conocimientos en informática y han sido activistas de los medios de comunicación digitales.

Cuadro 4 Colaboradores Wikileaks

Julián Assange es editor jefe y fundador de WikiLeaks, es uno de los primeros colaboradores del portal; por medio de esta plataforma busca "forzar la transparencia y la responsabilidad de instituciones poderosas" Cabe señalar que el fundador Julián Assange a temprana edad tuvo problemas con la policía al acceder a documentos confidenciales en una Universidad de Australia, por lo cual fue multado por cometer 24 delitos informáticos a la institución.
Jacob Appebaum es otro de los miembros del portal WikiLeaks, es fundador de Noisebridge en San Francisco, miembro del club berlinés del Caos Informático y desarrollador, es uno de los principales defensores e investigadores del proyecto Tor, el cual es un sistema de anonimato virtual creado para que cualquier persona pueda evitar la vigilancia y la censura en internet.
Andy Müller- Maguhn es cofundador de la European Digital Rights(Derechos Digitales Europeos), está especializado en telecomunicaciones y otros sistemas de vigilancia, trabaja como periodista en la industria de la vigilancia con su proyecto Wiki, además tiene una empresa por la cual comercializa dispositivos seguros de comunicación de voz.
Jérémie Zimmerman es cofundador y portavoz del grupo civil de apoyo La Quadrature du Net, la organización europea más destacada en el ejercicio de la defensa del derecho al anonimato en la red y en la concientización sobre la existencia de ataques normativos a las libertades virtuales.

Fuente: Elaboración propia, con base en el libro Cyberpunks, La libertad y el Futuro de Internet, Ed. Deusto, España, 2013, pp. 21-24.

La misión principal de los wikiLeaks, en palabras de los cofundadores, es exponer los regímenes opresivos en Asia, el antiguo bloque soviético, el África subsahariana y el Oriente Medio, además de otras zonas del mundo en las que la gente desea revelar lo que los fundadores Consideran ser comportamiento "antiético" exhibido por sus gobiernos y corporaciones.[160]

En la administración de Barack Obama, se ordenó a las instancias Federales, que se mantuviera como clasificado el contenido filtrado por WikiLeaks, pese a que la información ya había sido publicada por agencias de noticias importantes internacionalmente, por ejemplo The New York Times y The Guardian.

“Además el gobierno de Estados Unidos presionó a los servidores de Internet para que dejaran de dar servicio a WikiLeaks.org, el 1 de Diciembre de 2010, Amazon elimino a WikiLeaks de sus servidores de almacenamiento y el 2 de Diciembre, el servidor DNS (Sistema de nombres de dominio) asignado al dominio wikiLeaks.org fue atacado, sin embargo el portal se mantuvo activo en la red durante el ataque debido a la creación de escudos llamados mirrors (espejos), por medio de los cuales miles de personas que visitaban el sitio copiaban la dirección del portal y alojaban en su computadora su propia versión y a través de esto distribuían la información por las redes sociales. ”[161]

Internacionalmente, las revelaciones en el portal han tenido gran impacto en la toma de decisiones internas y externas de Estados Unidos, debido a que se expone información al escrutinio público sobre las medidas que toma el Estado para llevar a cabo las relaciones diplomáticas y se expone las medidas de seguridad y su capacidad militar.

En el caso de las revelaciones que hace WikiLeaks, podemos encontrar “[…] 250,000 documentos que dan a conocer los métodos de espionaje de Estados

[160] Gragido Will, Piric John, Cybercrime and Espionage and Analysis of subversive Multivector Threats, Ed. Elsevier, Amsterdam, 2011, p. 191.
[161] The Guardian, Wikileaks lucha por seguir en la red tras la retirada de su dominio por parte de una compañía americana, 2010, disponible en línea: http://www.guardian.co.uk/media/blog/2010/dec/o3/ wikileaksknocked-off-net-dns-eveydns, Fecha de consulta: 14 de Mayo de 2017.

Unidos por medio de su equipo diplomático en Naciones Unidas para obtener información de representantes diplomáticos y altos funcionarios de la ONU, ejemplo de ello es en 2009 el departamento de Estado exigió detalles técnicos sobre los sistemas de comunicación utilizados por altos funcionarios de Naciones Unidas, entre los que se encontraban contraseñas y claves personales que utilizaban en las comunicaciones oficiales."[162]

De acuerdo a José Luis Serra, especialista en fuerzas armadas y seguridad Nacional: "Los cables que fueron revelados del portal wikiLeaks permite conocer algunas decisiones y procedimientos recientes en materia de inteligencia y contrainteligencia de Estados Unidos y sus efectos en una multitud de naciones investigadas".[163]

Ejemplo de las repercusiones de la filtración de cables en relación a los procedimientos militares y de inteligencia es el cable publicado el 25 de julio de 2010 llamado "Diarios de la Guerra en Afganistán", "contiene más de 91,000 informes que cubren la guerra de Afganistán de 2004 a 2010; Los informes describen la mayoría de las acciones militares letales que involucran al ejército de EE.UU., revela ubicaciones y operaciones clave."[164]

Debido a la filtración de este cablegate sobre operaciones militares, "Organizaciones de Derechos Humanos como Amnistía Internacional y el grupo *International Crisis Group* presentaron una queja al portal WikiLeaks, sobre la divulgación de información de las operaciones militares debido a que representaba

[162] Gómez Aguirre Gonzalo, WikiLeaks revela que EE usaba a sus embajadores para espiar en la ONU, 28 de noviembre de 2010, disponible en línea: http://www.elmundo.es/america/2010/11/28/estados_unidos/1290951375.html, Fecha de consulta: 17 de Noviembre de 2017.
[163] Santiago de Freda Manuel, Wikileaks, periodismo y transparencia: los filtros de las filtraciones, DERECOM, 2010, disponible en línea: www.derecom.com/blog/item/download/83_01316c1003f735e67fd8b9-a202710328, Fecha de consulta: 14 de Mayo de 2017.
[164] WikiLeaks, *Afghan War Diary*, 25 de julio de 2010, disponible en línea: https://wikileaks.org/afg/, Fecha de consulta: 17 de Noviembre de 2017.

un peligro a las personas involucradas en la operación además de poner en riesgo las operaciones militares por parte de Estados Unidos."[165]

3.4 Reacciones del Gobierno Estadounidense

Una de las bases de la política de seguridad nacional fue establecer una cooperación con aliados clave entre los países y empresas para intercambiar información trascendental en materia de ciberseguridad, generando un importante cuestionamiento sobre cuál es la información que puede ser compartida por parte de las empresas cuando se habla de seguridad nacional, pero también sobre las ganancias económicas por parte de las compañías inmersas en los dominios del ciberespacio al proporcionarle al gobierno información confidencial de los usuarios.

Aunque el gobierno de Estados Unidos reconoce la relevancia de la seguridad cibernética, las medidas implementadas no han logrado solucionar el conflicto dentro del ciberespacio debido a la constante innovación en las ciberarmas, teniendo un tiempo de caducidad muy corto las herramientas cibernéticas.

Después que la Casa Blanca ha sido víctima de diversos intentos de ataques originados en el extranjero, el Pentágono ha anunciado que los ataques cibernéticos pueden ser considerados como "Actos de Guerra"[166].

A través de los servicios de inteligencia y las redes de espionaje, se han logrado interceptar ataques a las infraestructuras críticas por grupos terroristas, un ejemplo de ello fue en 2011 "se interceptó los sistemas de comunicación del líder de Al-Qaeda en Pakistán donde se daban instrucciones para llevar a cabo un ataque terrorista en Nueva York o Washington, mediante un artefacto explosivo justo

[165] Zacarías López Daniela, Wikileaks y los efectos de la divulgación de información confidencial: análisis de las filtraciones de Estados Unidos, Colegio de San Luis, 2012, p. 73.
[166] BBC Mundo, El nuevo campo de entrenamiento para las ciberguerras, Op. Cit.

cuando se conmemora el décimo aniversario de los ataques terroristas del 11 de septiembre de 2001."[167]

Por otra parte, Barack Obama a finales de 2013 presentó una iniciativa para reformar las políticas de espionaje, la cual estableció el compromiso de analizar e intercambiar las políticas de inteligencia de manera anual de acuerdo a las funciones de los sistemas de inteligencia, además de transparentar las actividades realizadas en esta materia y establecer límites en la acumulación de registros telefónicos, direcciones electrónicas y datos personales explicando porque se cometieron actos de espionaje.

[167] CNN, EE.UU. interceptó una amenaza terrorista de Al-qaeda para el 11-S, 9 de Septiembre de 2011, disponible en línea: https://cnnespanol.cnn.com/2011/09/09/ee-uu-confirma-una-amenaza-creible-de-atentado-para-el-11-s/, Fecha de consulta: 12 de Junio de 2017.

CAPÍTULO IV: IMPACTO DE LAS MEDIDAS DE CIBERSEGURIDAD Y SUS REPERCUSIONES EN EL ESCENARIO INTERNACIONAL

Las acciones en materia de seguridad se han centrado en el intercambio de inteligencia, entrenamiento de personal calificado y protección a las redes en el ciberespacio; sin embargo, las filtraciones de cables diplomáticos en el portal WikiLeaks muestra la parte vulnerable sobre las medidas de seguridad cibernética que son implementadas por las agencias de inteligencia de Estados Unidos hacia el resto del mundo, lo cual ha provocado conflictos en las relaciones diplomáticas con el uso de espionaje y dispositivos no tripulados que son dirigidos desde larga distancia, vistas como un acto que atenta a la soberanía nacional de cada país.

En este capítulo se abordarán las medidas de ciberseguridad que se implementaron durante la primera administración de Barack Obama junto a empresas de seguridad informática para proteger la infraestructura crítica y cibernética y evitar posibles ataques que pusieran en riesgo el desarrollo de ese país.

Al mismo tiempo se mencionaran los sistemas de control de ciberespionaje implementados por la *National Security Agency* (NSA) y *la Central Intelligence Agency* (CIA); como es el sistema, Prism, Carnivore y Témpora, siendo estos sistemas capaces de infiltrarse en cualquier dispositivo y obtener información que sirva para evitar vulnerabilidades en el espacio cibernético.

También se comentará el proyecto de ley llamado Acta de Protección e Intercambio de Inteligencia Cibernética (CISPA), que es implementado con la finalidad de recopilar información por las agencias de inteligencia Federales y utilizarla como medio de intercambio entre empresas privadas para implementar medidas de ciberseguridad.

Siguiendo el orden de ideas, en este capítulo hará referencia sobre las filtraciones hechas por el ex empleado de la Central Intelligence Agency (CIA) y de la National Security Agency (NSA) Edward Snowden, sobre ciberespionaje y las reacciones diplomáticas entre los principales países aliados de Estados Unidos.

Para finalizar se abordara el tema de ciberterrorismo y el impacto que ha tenido en Estados Unidos así como las medidas que se han implementado para contrarrestar a los principales grupos terroristas.

4.1 Impacto de los sistemas de control de ciberespionaje

Estados Unidos de América ha implementado una red internacional de ciberespionaje que cubre la totalidad del globo terráqueo y que básicamente escucha todo lo que se dice en el mundo, el gobierno norteamericano busca la "cooperación voluntaria" de las agencias de servicio de comunicación más importantes internacionalmente debido a que concentran una gran fuente de información.

Los hackers han desarrollado formas de infiltrarse en las computadoras, correos electrónicos, comunicaciones electrónicas y telefonía por internet del gobierno norteamericano, lo que ha llevado a tomar medidas de vigilancia para monitorizar el tráfico de datos que se lleva a cabo en la red.

La Nacional Security Agency (NSA), ha utilizado y desarrollado varios métodos de espionaje, así como ha ido adaptando e innovando sus programas de inteligencia, de acuerdo a los requerimientos estratégicos actuales; sin embargo, no se han dejado de lado los programas de inteligencia, como es el sistema Echelon, Carnivere y el sistema de ciberespionaje Prism, siendo el programa más sofisticado que ha sido implementado por la NSA y la CIA como método de ciberespionaje.

Los sistemas para evitar ser objeto de espionaje que ha implementado la *National Security Agency* (NSA), se basan en programas y aplicaciones difíciles de detectar por el enemigo, con el fin de evitar ataques y obtener información sobre las actividades de hackers que quieran entrar a los sistemas operativos del gobierno.

Con el fin de evitar piratería y ataques cibernéticos, la National Security Agency (NSA) ha utilizado " *Access Network Technology* (ANT)"[168], estos cortafuegos o mejor conocidos como firewalls; es un software, funciona ocultándose a sí mismo en los dispositivos que tengan conexión a la red, ya que están instalados formatean el disco duro y reinstalan un nuevo sistema operativo, permitiendo identificar actividades maliciosas en la red, estos implantes ANT tienen acceso a la vida digital de cualquier usuario en la red, las unidades *Access Network Technology* (ANT) ha sido creada por los principales fabricantes de hardware y software de seguridad tecnológica como son las empresas Cisco, Juniper y Huawei.

Otro tipo de implante que ocupa la NSA, es el llamado "DEITYBOUNCE", este software se oculta dentro de los servidores Dell, se instala mediante el proceso de interdicción[169] el cual consiste en que los agentes de la NSA interceptan el equipo cuando lo compra el usuario, permitiendo manipular el hardware sin que se dé cuenta el comprador.

A continuación se explican los sistemas de ciberespionaje que han sido utilizados por las agencias de inteligencia estadounidenses como es la CIA, NSA y el FBI, para mantener monitorear la red y detectar a tiempo ataques terroristas a nivel internacional:

Sistema Carnivore

"El sistema Carnivore es la tercera generación de los sistemas de espionaje de redes del FBI. Un sistema que ha sido diseñado por el FBI para capturar aquellos mensajes de correo electrónico que sean sospechosos de contener información útil para la agencia."[170]

[168] Varonas Nico, Top secret: La tecnología con la que espía la NSA, NEOTEO, 6 de Enero de 2014, disponible en línea: http://www.neoteo.com/top-secret-la-tecnologia-con-la-que-espia-la-nsa/, Fecha de consulta: 03 de Agosto de 2017.
[169] Proceso de interdicción: Manipulación de hardware y software de manera oculta para el usuario.
[170] Ibídem, p. 120.

De acuerdo al FBI el sistema Carnivore es un sistema basado en ordenadores destinado a la colaboración entre proveedores de internet junto con la agencia de inteligencia para la recolección de datos y de información sobre un usuario que sea objeto de investigación.

También el sistema Carnivore es capaz de espiar cualquier disco duro de cualquier usuario que sea considerado como sospechoso, el sistema no deja rastro de actividad de espionaje en los equipos de cómputo. Para ello se coloca un chip en los dispositivos de los proveedores de servicio de Internet para controlar todas las comunicaciones electrónicas que tienen lugar a través de ellos.

El programa es suficientemente ligero para ser instalado en cualquier computadora, dentro de sus funciones se encuentra el rastreo o ubicación además de proporcionar un diagnóstico sobre las redes que son utilizadas cotidianamente en proveedores de servicios de internet y que funcionan con las aplicaciones convencionales como es el uso de las redes sociales y correo electrónico.

Tempora

Es un programa clandestino de vigilancia de seguridad electrónica que fue puesto a prueba en 2008, y establecido en 2011 para ser operado por el Government Communications Headquarters (GCHQ) del gobierno británico junto con la colaboración de la NSA.

“La forma en la cual se apodera de la información es interceptándola directamente en los cables de fibra óptica que confluyen en territorio inglés o en las centrales que conforman internet. Agregando que a los puntos de intercepción no solo se encuentran en territorio británico sino también en otras partes del mundo, aparentemente las compañías prestadoras del servicio tienen pleno conocimiento de la situación.”[171]

[171] Arreola García Adolfo, Ciberespionaje: La puerta al mundo virtual de los Estados e Individuos: una revisión de los programas de espionaje digital de los Estados Unidos, primera edición, Ed. Siglo XXI, México, 2015, p. 119.

El programa tempora, intercepta y absorbe comunicaciones por medio de los cables de fibra óptica, teniendo acceso total a los datos de los usuarios que circulan por este medio.

El programa Tempora cuenta con dos componentes principales:

- Mastering the Internet (Dominando el internet).
- Global Telecoms Exploitation (Explotación global de las telecomunicaciones).[172]

Los componentes en los que se basa el programa Témpora es en el acceso a los dominios de internet mediante los cables de fibra óptica trasatlánticos que aterrizan desde las costas británicas hacia Europa Occidental desde las centrales telefónicas y los servidores de internet de Estados Unidos y posteriormente se procesa la información en instalaciones de almacenamiento de datos del GCHQ en Reino Unido.

"Tempora es parte de los acuerdos de colaboración suscritos bajo la alianza del grupo denominado The Five Eyes que está conformada por diferentes agencias de seguridad de los Estados miembros (Estados Unidos, Reino Unido Australia, Canadá y Nueva Zelanda), que buscan una completa integración para el acceso total de los datos en internet"[173]; desde otro punto de vista el programa Tempora absorbe todas las formas de comunicación que circula por los cables de fibra óptica alrededor del mundo, explotando las telecomunicaciones globales con el objetivo de captar todo el tráfico de datos sin importar de donde proviene la información.

"Para los 2 millones de usuarios de la World Wide Web, Témpora representa una ventana a su vida cotidiana, absorbiendo todas las formas de comunicación con los cables de fibra óptica que dan la vuelta al mundo."[174]

[172] Ídem.
[173] Ibídem, p. 121.
[174] The Guardian, GCHQ utiliza cables de fibra óptica para obtener acceso secreto a las comunicaciones del mundo, 21 de Junio de 2013, disponible en línea:

Como se mencionó con anterioridad, Estados Unidos no solo busca alianzas estratégicas con empresas, sino también con Estados justificando sus métodos de protección con leyes que responden a las demandas de la cobertura legal que necesitan las agencias de inteligencia para justificar sus acciones de inteligencia como es el uso de la Pratriot Act y la Ley de Vigilancia de Inteligencia Extranjera (FISA) (véase en anexo 5).

4.2 Acta de protección e intercambio de Inteligencia cibernética (CISPA)

El proyecto de ley denominado *Cyber Intelligence Sharing and Protection Act* (por sus siglas en inglés CISPA) o también conocida como Acta de Protección e Intercambio de Inteligencia Cibernética, busca facilitar el intercambio de información con diferentes Agencias Federales de Estados Unidos, el monitoreo de contenido entre los distintos actores de internet con la finalidad de prevenir las posibles infracciones a los derechos de propiedad intelectual y mitigar los crímenes y ciberamenazas que ocurren en la Red.

"Los representantes estadounidenses Mike Rogers y Charles Albert Ruppersberger, pertenecientes tanto al partido republicano y demócrata en 2010 promovieron el proyecto de Ley CISPA con la finalidad de regular las relaciones entre el gobierno y las empresas, permitiendo que estas compartan información privada de sus usuarios para combatir "ciberamenazas", quedando las empresas libres de cualquier responsabilidad legal."[175]

Bajo los lineamientos de la *Cyber Intelligence Sharing And Protection Act of* 2011 (CISPA), permitirá el intercambio de información del tráfico de internet entre el gobierno estadounidense y las empresas fabricantes y prestadoras del servicio, con la intención de ayudar a Estados Unidos a investigar amenazas cibernéticas y

---

https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, Fecha de consulta: 19 de Noviembre de 2017.

[175] Granados Omar, CISPA, un nuevo intento por controlar internet, animal político, 10 de Abril de 2012, disponible en línea: http://www.animalpolitico.com/2012/04/cispa-un-nuevo-intento-de-controlar-internet/, Fecha de consulta: 03 de Julio de 2017.

garantizar la seguridad de las redes contra ataques generados desde el interior o exterior de su territorio.

“Básicamente lo que pretende hacer el proyecto de CISPA es adicionar un acápite de inteligencia contra ciberamenazas e información dentro del título XL del *National Security Act of* 1947 (50 U.S.C. 442 et seq.) y de esta manera, mediante la Dirección Nacional de Inteligencia se pretende establecer pautas y guías por medio de las cuales se procura otorgar seguridad a los empleados de determinadas entidades (Sección 1104 del Proyecto precipitado); dejando por sentado que este esquema de seguridad no puede ser entendido de ninguna forma como un beneficio real o provisional para las entidades del sector privado, sino por el contrario, se pretende aumentar el grado de protección en lo que a la seguridad de la información se trata.”[176]

Para que el sector privado enfoque las operaciones seguridad en detectar ciberamenazas la ley CISPA restringe y limita el monitoreo de información de carácter personal como: archivos médicos, educativos, devolución de impuestos, etc.

Las entidades del sector privado, por medio del proyecto CISPA, son certificadas para que puedan seguir haciendo actividades de manera segura tomando en cuenta los protocolos de seguridad y se puedan proteger de filtraciones en sus sistemas operativos, también se implementan medidas para usar sistemas de ciberseguridad para identificar y obtener información acerca de posibles amenazas en el ciberespacio, además de intercambiar información con otras empresas y el gobierno Federal para evitar que se reproduzcan amenazas. El proyecto de Ley CISPA permite ejercer acciones de monitoreo de la información que circula en la red y efectuar acciones de restricción.

“El proyecto de ley CISPA delimita las potestades en cuanto al manejo de la información relacionada con entidades privadas y públicas por parte de agentes

[176] Aristizabal Velásquez David, Luces y sombras de las nuevas tendencias de la regulación de contenidos informáticos en los Estados Unidos de Norteamérica, Revista CES, No.1, Medellín Colombia, p.80.

militares, sentando la pauta consistente en que no se constituirá una autoridad adicional o se modificará la autoridad de que están investidos el departamento de Defensa o las Agencias de Seguridad Nacional."[177]

La Ley CISPA es una muestra de que internet se concentra en la operación e infraestructura de Estados Unidos, para tener el control de las diferentes redes tomando en cuenta los nombres de dominios y los servidores DNS que están bajo la jurisdicción norteamericana.

Sin embargo el proyecto de Ley CISPA ha generado gran controversia al permitir el intercambio de información en el tráfico de internet entre el gobierno de EEUU y cierta tecnología entre las empresas especializadas en la creación e innovación de tecnologías de la información. "El objetivo declarado del proyecto es ayudar al gobierno estadounidense a investigar las amenazas cibernéticas y garantizar la seguridad de las redes contra los ataques cibernéticos."[178] El proyecto permite al poder ejecutivo la capacidad de acceder a los sistemas tanto de las autoridades como de compañías privadas espiar las comunicaciones. La razón principal, es la defensa contra el terrorismo, así como asegurar las patentes y derechos de autor debido a que la tecnología es la principal industria de Estados Unidos.

También se reconoce que el intercambio de información pública y privada para poder proteger la infraestructura cibernética y evitar que se propaguen malware que se puedan filtrar en los dispositivos que se encuentre conectado a la red, tomando en cuenta los protocolos de seguridad y privacidad. "en el marco de amenazas de ciberseguridad" tendrá que garantizar la privacidad y confidencialidad de datos.

[177] Ídem.
[178] De Tomas Morales Susana, Retos del Derecho ante las Nuevas Amenazas, Ed. Dykenson S.L., España, 2015, p.143.

4.3 Vigilancia en Estados Unidos por la Agencia de Seguridad Nacional (NSA)

El poder de inteligencia de la NSA se extiende por todo el mundo, la misión de esta agencia de inteligencia es recolectar, procesar y diseminar información de inteligencia por medio de alianzas, asociaciones y acuerdos políticos de cooperación entablados por los países aliados de Estados Unidos.

"La NSA ha desarrollado múltiples programas de espionaje para adaptar sus capacidades a la evolución tecnológica y a los requerimientos estratégicos, a consecuencia de los atentados del 11 de septiembre de 2001, se inicia la lucha contra el terrorismo y se crea una nueva legislación antiterrorista"[179]; con las operaciones que se pusieron en marcha se utilizaron varios programas de vigilancia capaces de monitorizar y vigilar el tráfico de internet, las cuentas de correo electrónico, los datos multimedia, las comunicaciones telefónicas y la telefonía por internet, por el programa PRISM.

Con el avance de la tecnología los métodos de espionaje son más sofisticados, en el caso de la NSA basa su predominio en el desarrollo tecnológico para tener control en la información que fluye en los sistemas digitales, que posteriormente es resguardada en servidores de almacenamiento en una central de operaciones.

La *National Security Agency* (NSA) ha tomado gran relevancia tras las actividades de espionaje internacional que fueron filtradas por un ex agente de la Agencia Central de inteligencia (CIA) y de la NSA llamado Edward Joseph Snowden.

"Edward Snowden a los 20 años de edad se había alistado en el ejército para luchar en la guerra de Irak, sin embargo se vio obligado a dejar el ejército al

[179] La agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EEUU, Real Instituto Elcano, 11 de Noviembre de 2013, disponible en línea: http://www.realinstitutoelcano.org/wps/wcm/connect/7366288041c9aefda642ae709b5c3216/ARI41-2013-THIBER-NSA-espionajepublicoprivadaSnowden.pdf?MOD=AJPERES&CACHEID=7366288041c9aefda642ae709b5c3216, Fecha de consulta: 05 de Agosto de 2017.

romperse las dos piernas en un accidente y retomo su talento tecnológico convirtiéndose en 2005 en experto técnico de la CIA."[180]

En 2006, paso a trabajar para una empresa contratista de la CIA a ser miembro de la plantilla a tiempo completo, en 2007 es mandado a trabajar en los sistemas informáticos de la CIA en Suiza, a partir de ahí, se empieza a dar cuenta de las operaciones que se utilizaban para sacar información .

A finales de 2009, Snowden, deja la CIA en Ginebra y es cuando empieza a contemplar la posibilidad de filtrar documentos secretos considerados delitos graves, sin embargo decidió esperar que pasaran las elecciones de Estados Unidos que provocaran un cambio, donde el discurso de Barack Obama ofrecía acabar con los abusos de seguridad nacional que habían estado justificados por la guerra contra el terrorismo.

Al ver que en la administración de Barack Obama no había un cambio en los abusos de poder por las agencias de inteligencia y por temor de los daños colaterales que provocaría si daba a conocer información sensible, "Edward Snowden decide incorporarse a la NSA por medio de la compañía Dell Corporation y en 2010 fue destinado a Japón concediéndole un nivel de acceso a secretos de vigilancia mucho mayor al que había tenido antes."[181]

Durante toda su labor tanto para la CIA como para la NSA, recibió cada vez más información para llegar a ser agente cibernético cualificado, con la capacidad de hackear sistemas civiles y militares de otros países para robar información o perpetrar ataques sin dejar huella, convirtiéndose en un experto de ciberseguridad para la NSA.

El 9 de Julio de 2013 se dan a conocer las filtraciones reveladas por Edward Snowden quien contacto a Gleen Greenwald en 2012 sin poder establecer un método de comunicación seguro, después de un mes Snowden trata de retomar la comunicación mediante correos electrónicos cifrados; otra pieza importante para

[180] Gleen Greenwald, Snowden. Sin un lugar donde esconderse, Ed. Metropolitan Books, Barcelona España, 2014, p.124.
[181] Ídem.

hacer llegar la información a la opinión pública fue Laura Poitras con quien estableció comunicación en febrero de 2013, después de meses de comunicarse de forma anónima, el 3 de junio de 2013 se reunieron con Edward Snowden en un hotel de Hong Kong para entrevistarlo.

Durante la entrevista Gleen Greenwald le pregunta a Edward Snowden ¿Por qué tomo la decisión de filtrar la información y sacarla a la luz?, por lo que Edward Snowden contesto lo siguiente:

> "Todo se reduce al poder del Estado contra la capacidad del pueblo para oponerse significativamente a ese poder, sabiendo que recibo un pago por diseñar métodos para la amplificar ese poder del Estado y me doy cuenta que las políticas cambian, siendo las únicas que pueden restringir al Estado, cambian a tal grado que ni siquiera las personas brillantes podrían oponerse al poder del Estado, y como vi en las promesas de la administración Obama traicionar y evaporarse, en lugar de avanzar en las cosas que había prometido se volvió a una especie de olvido, reducción y retroceso."[182]

Después de ser publicada la información por el periódico The Guardian y The Washington Post, por temor a represalias legales debido a las filtraciones Snowden se trasladó a Moscú para viajar posteriormente a Cuba, sin embargo no pudo abordar al avión debido a que el gobierno estadounidense le anula su pasaporte quedando varado en el aeropuerto de Rusia.

"A causa de quedar varado Snowden, el gobierno Ruso le ofreció asilo político por un año y en 2014 se le concede una extensión de tres años para permanecer en Rusia, recientemente se le otorgó el permiso de residencia hasta 2020."[183]

Dentro de las revelaciones que filtró Edward Snowden, a los periódicos The guardian y The Wasnhington Post son las siguientes:

---

[182] Poitras Laura, Citizenfour, 10 de Octubre de 2014, disponible en línea: https://www.youtube.com/watch?v=4EgTXEn15ls&t=328s, Fecha de consulta: 19 de Noviembre de 2017.

[183] El Mundo, Rusia no sabe qué hacer con Edward Snowden, 11 de Febrero de 2017, disponible enlínea:http://www.google.com.mx/amp/s/.amp.elmundo.es/.internacional/.2017/02/11/589f345ce2704e156a8b467c.html, Fecha de consulta: 26 de Noviembre de 2017.

- The Guardian publicó una orden secreta de un tribunal que exigía a la empresa de telecomunicaciones Verizon a entregar todos sus datos telefónicos a la NSA diariamente para su almacenamiento.
- El periódico The Guardian reporto que la agencia de espionaje británica estaba "pinchando" cables de fibra óptica que transportan comunicaciones globales y que estaba compartiendo grandes cantidades de datos con su contraparte la NSA.
- También se reveló que los servicios de inteligencia han intervenido las sedes diplomáticas en Washington y Nueva York, siendo los países afectados: Francia, Italia y Grecia, así como países aliados no europeos como Japón, Corea del Sur e India, detallando en los documentos los métodos de espionaje e interceptación de mensajes en dispositivos electrónicos y llamadas telefónicas.[184]

Después de las filtraciones que hizo Edward Snowden, ponen en tela de juicio la discrecionalidad y secretismo con el que se administran las polémicas leyes que aprobaron durante la primera administración de Barack Obama sobre vigilancia a los usuarios que fueran sospechosos de cometer actividades extremistas, por lo que se autorizó la obtención masiva de datos telefónicos de la empresa Verizon por medio de operaciones de vigilancia estatal que tienen el poder de contener información de grandes segmentos de la población sobre lo que no hay evidencia de actividad legal.

El sistema especial de vigilancia de la NSA, fue llevado a cabo bajo una orden secreta emitida bajo la llamada Ley de Vigilancia de Inteligencia Extranjera (FISA):

> "El tribunal de Vigilancia de Inteligencia Extranjera puede autorizar a las compañías a proporcionar información, servicios o asistencia necesaria, en

[184] Márquez William, Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU., 2 de Julio de 2013, disponible en línea: http://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm, Fecha de consulta: 07 de Agosto de 2017.

> contrapartida al cumplimiento, la compañía es compensada por su trabajo y recibe inmunidad frente a posibles demandas."[185]

La Ley FISA fue creada para darle certeza jurídica a sus acciones, y ofrecer la protección de la ley a las compañías que cooperan con el gobierno estadounidense en la recolección de información, sin embargo esta ley es utilizada con otra finalidad, ya que sirve como escudo jurídico para justificar las acciones de ciberespionaje en todo el mundo por parte del gobierno norteamericano.

El programa PRISM fue revelado por Edward Snowden en junio de 2013 al periodista Glenn Greenwald[186] y a Laura Poitras[187] documentalista estadounidense esté programa fue utilizado entre diciembre de 2007 y octubre de 2012 cuya matrícula es US-984XN, el programa PRISM fue utilizado de manera conjunta con los sistemas Upstream[188], permitiendo que la NSA dispusiera de un acceso privilegiado a los servidores y a los datos de empresas prestadoras del servicio de internet.

El programa PRISM es un programa secreto de vigilancia e investigación de datos electrónicos con el que Estados Unidos opera a través de la Agencia de Seguridad Nacional (NSA) desde el año 2007. "Por medio del programa el gobierno de Estados Unidos podía acceder a cuentas de correo electrónico, chats, fotografías, videos, documentos e incluso datos de tarjeta de crédito, almacenadas en internet por medio de las compañías Microsoft, Yahoo, Google, Facebook, Pal Talk,

[185] FORBES, Ninguna tecnológica se salva de la inteligencia de EU, 10 de Junio de 2013, disponible en línea: https://www.forbes.com.mx/pocas-opciones-para-que-firmas-desafien-a-inteligencia-de-eu/, Fecha de consulta: 20 de Junio de 2017.

[186] Glenn Greenwald es un abogado constitucionalista estadounidense, columnista, bloguero, escritor y periodista, ha recibido numerosos premios por su trabajo entre los que destacan el premio Pulitzer en 2014 y en 2013 el premio George Polk.

[187] Laura Poitras es una documentalista y productora estadounidense, ha recibido numerosos premios por su trabajo Citizenfour ganó el Óscar al mejor documental largo de 2014, también ganó el premio Pulitzer en 2014 y en 2013 ganó el premio George Polk a la información sobre seguridad nacional.

[188] Los sistemas Upstream son direcciones de internet que permiten transferencia y descarga de datos de servidor a usuario.

Youtube, Skype y Apple, el programa PRISM podía direccionarse directamente a los servidores de las compañías para obtener datos"[189].

Como su nombre lo indica, PRISM actúa, pues, como un prisma que descompone un rayo de luz de los colores del arcoíris. Lo que lo vuelve terrible es su increíble eficacia, dado que el sistema está en gran parte automatizado y ofrece una navegación simple.

Pese a que el programa PRISM es de carácter privado, la obtención de datos por parte de la National Security Agency (NSA) se hacía mediante el tribunal secreto de la Foreing Intelligence Surveillance Court (FISA) el cual permitía la operación de las agencias de inteligencia por medio del programa PRISM recolectar información que posteriormente seria almacenada en una base de datos que serviría como detección de terroristas.

Por medio de la Ley FISA se obligaba a cooperar a las empresas de tecnología a brindar información a las agencias de inteligencia como la CIA y la NSA datos como números de teléfono, correos electrónicos, etc, al gobierno de Estados Unidos para las operaciones de inteligencia, como es interceptación de llamadas a cualquier persona.

El programa PRISM opera bajo la supervisión del Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos de América (El tribunal FISA o FISC) bajo la sección 702 de la Ley de Enmiendas de la FISA 2008:

> "La Ley de Enmiendas de FISA 2008: Permite una amplia vigilancia sin la debida autorización de los estadounidenses en los Estados Unidos, siempre que el llamado telefónico o el correo electrónico sea considerado internacional."[190]

La ley de enmiendas FISA cobro gran impacto al ser aprobada por el congreso como marco legal para la vigilancia internacional, después de los ataques del 11

[189] Castaño Sencianes Albert, Periodismo de Filtración: El caso PRISM, Ed. Universitat Autònoma de Barcelona, España, 2014, p. 33.
[190] Gregory Anthony, El Estado de vigilancia bipartidista, 11 de Junio de 2008, disponible en línea: http://www.elindependent.org/articulos/article.asp?id=2263, Fecha de consulta: 11 de Junio de 2017.

de septiembre de 2001; La ley FISA determina las condiciones en las cuales las agencias de inteligencia estadounidense pueden interceptar llamadas y correos electrónicos internacionales sin restricción alguna, mediante programas de espionaje, claro ejemplo de ello es la utilización del programa PRISM.

El sistema PRISM, se encuentra bajo responsabilidad de una unidad de elite, el servicio especial Source Operations (SSO) de la National Security Agency (NSA), Prism es el sistema de vigilancia de las telecomunicaciones electrónicas más usados por la NSA: En 2012, 24,005 informes de la agencia lo citaban como fuente principal.

Sin embargo a partir de los atentados del 11 de septiembre de 2001 y con el crecimiento de las instancias gubernamentales a cargo de la seguridad, la cantidad de personas habilitadas en Estados Unidos para consultar los documentos secretos abarco alrededor de 5 millones en 2013.

“La National Security Agency (NSA) estima que en 2007, más del 80 % de las cuentas de correo de terroristas conocidos utilizaba Yahoo o Hotmail, entonces, con toda lógica, el Source Operation (SSO), el servicio especial de la Agencia de Seguridad Nacional que se encarga con el vínculo con las empresas privadas, suele ser calificado como la “joya” de la corona de la NSA”[191]

Debido al crecimiento acelerado del uso de las tecnologías por grupos terroristas a partir de 2007, el gobierno norteamericano empezó a poner medidas precautorias para vigilar las redes que fluctúan en el ciberespacio por medio de su interceptación, recolección y almacenamiento.

El programa PRISM, ayuda a detectar rápidamente cualquier acto ilícito en el ciberespacio, sin embargo ha sido cuestionado internacionalmente por su aplicación indiscriminatoria por su vigilancia ya que se recopila información de cualquier usuario sin importar si tiene antecedentes terroristas o no.

[191] Antoine Lefébure, El caso Snowden, así espía Estados Unidos al mundo, Primera edición, Ed.Le monde diplomatique, Argentina, 2014, p. 167.

Las revelaciones provocaron indignación por los grupos de defensa de derechos civiles, sobre la nueva normatividad estadounidense, por lo que el director Nacional de Inteligencia James Clapper dio declaraciones sobre los sistemas de vigilancia, así como el uso del programa PRISM para la adquisición de información extranjera:

> "El sistema PRISM, no puede ser usado para intencionalmente convertir en blanco a cualquier ciudadano estadounidense o cualquier otro estadounidense o cualquiera localizado dentro de los Estados Unidos, la información recogida bajo este programa está entre la más importante y valiosa información de inteligencia exterior que recogemos, y se usa para proteger a nuestra nación de una amplia variedad de amenazas"[192]

El programa PRISM recurre a las compañías prestadoras de servicios de comunicación, para la obtención de inteligencia que permita salvaguardar la seguridad nacional, aunque en la búsqueda transgredan los derechos de otros individuos o Estados.

No solo el programa PRISM se ha utilizado como medio de espionaje por la NSA; Las agencias de inteligencia de Estados Unidos han implementado programas con otras agencias de inteligencia de diversos Estados, ejemplo de ello es Gran Bretaña para monitorear la información que fluye en internet y poder detener amenazas en el hackeo de información.

En el siguiente cuadro se muestran los programas que ha implementado la NSA de manera conjunta con Government Communications Headquarters (GCHQ) como medida de vigilancia a nivel internacional:

[192] BBC Mundo, Crece el escándalo de Espionaje en EE.UU, 7 de jJnio de 2013, disponible en línea:http://www.bbc.com/mundo/noticias/2013/06/130606_eeuu_verizon_internet_metadata_vigilancia_cch, Fecha de consulta: 20 de Junio de 2017.

Cuadro 5 Programas utilizados por la NSA

PROGRAMA	CARACTERÍSTICAS
Turbine	Este programa representa un medio eficaz para infectar computadoras a través de la red, conocido también como Deep Packet Infection (infección de paquete profundo), permite a la NSA utilizar líneas de comunicación ultra rápidas cerrando un circulo de monitoreo de las acciones en internet, este programa funciona interrumpiendo las actividades de los enemigos por medio de un virus informático, provocando que la velocidad de internet en la computadora infectada no funcione de manera normal.
Muscular	El programa cuenta con una capacidad para almacenar 20 gigabytes de información de tráfico ya procesada, pero tiene por objetivo final alcanzar una capacidad de 100 gigabytes diarios. Su principal Característica radica en la no necesidad, por parte de la NSA, de contar con una orden judicial para llevar a cabo la interceptación de las comunicaciones privadas, por que dichas acciones se realizan en territorio ajeno (Gran Bretaña).
Olympia	Este programa es de participación conjunta entre los servicios de inteligencia de EEUU y Canadá para espiar las actividades dentro del Ministerio de Energía de Brasil, funciona al romper códigos e infiltrarse en las comunicaciones al interior y al exterior por medio de llamadas telefónicas y correos electrónicos.
Whitetamale	Este programa se utiliza para un objetivo en particular de una agencia "amiga", la cual es espiada al capturar correo electrónicos de funcionarios designados como objetivos y a partir de ahí infiltrarse en toda la red e iniciar con la captura de información.

The clipper Chip	Consiste en una implantación física de un chip en la tarjeta madre de una computadora, especialmente en los sistemas de comunicación seguros, con el fin de dar libre acceso remoto a las agencias gubernamentales de Estados Unidos.
Blarney	Tiene capacidad de interceptar y analizar tráfico de internet tanto nacional como internacional en grandes escalas a través de los cables de fibra óptica utilizando un sistema de imagen para no interrumpir el flujo de información.
Pinwale	Es una base de datos para analizar las actividades de internet, el programa Pinwale incorpora en su software información de diversos medios de comunicación digital.
Mainway	Es una base de datos totalmente controlada por el gobierno estadounidense, en las instalaciones de la National Security Agency (NSA), la información contenida es sobre millones de llamadas telefónicas realizadas a través de la infraestructura de las cuatro compañías telefónicas más importantes de los Estados Unidos (AT&T, SBC, Bellsouth y Verizon).
Bullrun	Está orientado a manejar la intrusión en las actividades de comercio internacional, su propósito es la intercepción de correos electrónicos, la vigilancia de los buscadores de la red, el monitoreo de las conversaciones a través de la red en tiempo real y las llamadas electrónicas, su principal herramienta la constituyen las llamadas supercomputadoras “rompe códigos”.

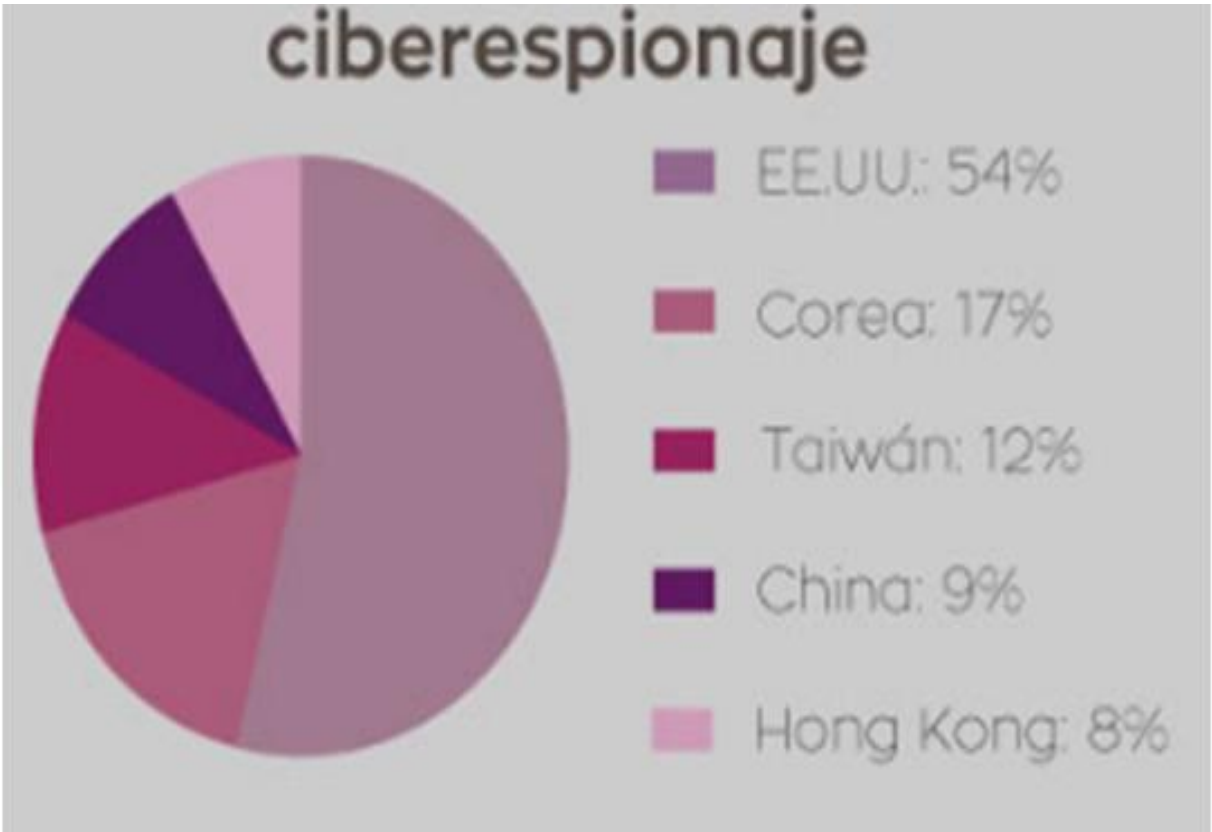
Fuente: elaboración propia, con base en el libro: Arreola García Adolfo, Ciberespionaje: La puerta al mundo virtual de los Estados e Individuos: una revisión de los programas de espionaje digital de los Estados Unidos, primera edición, Ed. Siglo XXI, 2015, p.p.121-133.

Como se observa en el cuadro número 5, Estados Unidos mediante la National Security Agency y por medio de las compañías de tecnología y

telecomunicaciones más poderosas del país permiten total acceso al gobierno estadounidense para obtener datos de los usuarios de telefonía y tener un control en el flujo de información mediante la intercepción de llamadas, correos electrónicos, monitoreo e interceptación de datos con la finalidad de proteger su seguridad nacional.

Para tener un parámetro claro de lo que representa para Estados Unidos obtener la mayor información posible y tener un control de diversos sectores tanto nacionales como internacionales, se muestra un estudio que fue hecho por las empresas Dell EMC y RSA FirstWatch, donde se da un panorama global sobre las direcciones o también conocidas como International Protocol (IP) maliciosas que fueron detectadas de diversos países, como se puede observar en la gráfica 3 Estados Unidos tiene mayor actividad de ciberespionaje al ocupar el 54%.

Gráfica 3 Ciberespionaje



Fuente: Russinovich Mark, Time Wavefront, Real Instituto Elcano, disponible en línea: www.diplomacydata.com, Fecha de consulta: 16 de Julio de 2017.

En la anterior gráfica se observa los países y regiones que tienen mayor actividad en actividades de ciberespionaje, donde Estados Unidos ocupa el primer lugar con el 54% está por encima de Corea con el 17% y China que tiene el 9% mientras las regiones como Taiwán su actividad de ciberespionaje es del 12% y Hong Kong en menor grado con el 8% basando sus acciones de ciberespionaje principalmente en el espionaje industrial.

4.3.1 Reacciones diplomáticas sobre los sistemas de ciberespionaje

Tras las filtraciones que hizo Edward Snowden y las revelaciones posteriores obligaron a muchos gobiernos a estimar el valor estratégico del ciberespacio y la ciberseguridad para resguardar sus intereses nacionales. Antes el ciberespacio era considerado como un bien abierto y seguro, sin embargo con el progreso de la tecnología que se está desarrollando aceleradamente, los Estados han desarrollado métodos para usar en el ciberespacio como un medio de obtención de información para ejercer presión en el sistema internacional. También se ha dejado al descubierto la interdependencia asimétrica entre EEUU y sus aliados en materia de inteligencia y el precio que hay que pagar por información que comparten y la inteligencia que reciben.

Las revelaciones sobre el plan de ciberespionaje de la NSA ha suscitado un debate internacional sobre los métodos que usa la inteligencia estadounidense para vigilar su territorio. “Mientras unos países mostraron su molestia argumentando que el plan de ciberespionaje viola la privacidad de los ciudadanos, no requiere autorización judicial y traspasa cualquier tipo de código moral, por parte de Estados Unidos el presidente Barack Obama defiende los métodos de inteligencia argumentando que se necesita salvaguardar la seguridad del país y que no expone a la privacidad de los usuarios de internet”[193]

Los países que más mostraron su molestia por las acciones de vigilancia fue Alemania y Brasil, con una postura más pacífica México, se abstuvo en tomar

[193] BBC Mundo, La poderosa herramienta de EE.UU. para vigilarlo todo en internet, 1 de Agosto de 2013, disponible en línea: http://www.bbc.com/mundo/noticias/2013/08/130801_tecnologia_snowden_nsa_xkeyscore_dp, Fecha de consulta: 24 de Julio de 2017.

medidas contra las acciones de espionaje hechas por la National Security Agency (NSA).

Alemania

En relación con las filtraciones que hizo Edward Snowden en junio de 2013, se dio a conocer el espionaje a los jefes de Estado, en el caso de Alemania la Canciller Ángela Merkel, fue interceptado su teléfono móvil, por lo que se hizo una investigación por parte de la agencia de inteligencia alemana para corroborar los hechos, encontrándose evidencia sobre el espionaje por parte de la NSA.

A causa de los acontecimientos de espionaje "la Canciller Ángela Merkel recrimino a Obama y expreso su exasperación por la lentitud de los estadounidenses para responder preguntas detalladas sobre los escándalos de la NSA desde que aparecieron las primeras revelaciones de Snowden en The Guardian."[194]

La vigilancia estadounidense aparenta buscar la seguridad por medio de espionaje siendo contradictorias las prácticas de inteligencia ya que no solo están enfocadas en la búsqueda de grupos terroristas, pareciera que buscan el control de los Estados mediante la información obtenida haciendo una fragmentación del ciberespacio al no tomar las medidas de seguridad entre los demás países.

Además de los hechos de espionaje a Ángela Merkel, el diario Der Spiegel reveló que los espías de la Agencia de Seguridad Nacional (NSA) y la Agencia Central de Inteligencia (CIA) espiaron instalaciones en el interior de la embajada en Berlín.

> De acuerdo con un documento de la NSA, en la Embajada estadounidense trabajaba un exclusivo grupo de espías que tienen por nombre de *Special Connection Service* (SCS) y que coopera con la NSA y la CIA. El exclusivo "ejercito electrónico" actúa en 80 lugares repartidos por el mundo, entre ellos 19 en Europa. Las herramientas de trabajo de este grupo de elite, que tiene cobertura diplomática en embajadas y consulados, le permiten captar todo tipo

[194] The Guardian, Llamada de Ángela Merkel a Obama: ¿Estás molestando a mi teléfono móvil?, 24 de octubre de 2013, disponible en línea: https://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german, Fecha de consulta: 20 de Noviembre de 2017.

de comunicaciones, tanto telefonía móvil, correos electrónicos, comunicaciones en internet inalámbricas y comunicaciones de satélite"[195]

Tras las filtraciones de espionaje por parte de Estados Unidos, las relaciones diplomáticas entre Alemania y Estados Unidos estuvieron tensas, el gobierno alemán ordenó a sus servicios de inteligencia que limitaran la cooperación de inteligencia y pidió la expulsión del Jefe de la CIA en Alemania.

"Tras la molestia por parte del gobierno alemán, buscó un acuerdo bilateral por escrito, en el cual se excluya explícitamente el espionaje por parte del gobierno norteamericano a la administración alemana y a las embajadas por parte de los servicios secretos, en segundo término se habló de regular y restringir las actividades de vigilancia sobre los ciudadanos alemanes, entre otro de los temas que se abordaron fue el espionaje industrial y financiero, debido a que las filtraciones que se revelaron sobre las medidas de vigilancia por parte de los medios internacionales que fueron dadas a conocer por el ex empleado de la NSA Edward Snowden."[196]

Las medidas que sugirió la canciller Ángela Merkel para evitar casos de espionaje "[…] fue la creación de una red de datos europea que evite el paso de las informaciones mediante el espionaje masivo a las comunicaciones por parte de las agencias de espionaje a los servicios digitales por servidores informáticos estadounidenses"[197]

Con la propuesta que promueve la Canciller Ángela Merkel en la Unión Europea, es un paso importante para resguardar la seguridad de los ciudadanos Europeos con el robo de datos, aunque al crear una red de datos solo de la Unión Europea podría causar una polarización del ciberespacio dejando de ser este un espacio universal; impactando en la globalización que busca una homogenización de los

[195] El país, Espías con vistas al Reichstag, 28 de Octubre de 2013, disponible en línea: http://internacional.elpais.com/internacional/2013/10/28/actualidad/1382993121_383527.html, Fecha de consulta: 20 de Junio de 2017.
[196] Ídem.
[197] Calderón Canales Rebeca, Chiquillo Benítez Vilma, Rodríguez Peña Yasmin, Espionaje como instrumento de la política exterior de estados Unidos de América y las consecuencias en sus relaciones exteriores. Casos: República Federal de Alemania y República Federativa de Brasil, Ed. Universidad de el Salvador, El Salvador, 2015, p. 126.

Estados, donde puedan interactuar sin restricción de fronteras y de forma fluida a cualquier parte del mundo.

Brasil

Las relaciones diplomáticas entre Estados Unidos y Brasil se vieron tensionadas debido al escándalo sobre espionaje el cual fue dirigido a la presidenta Dilma Rousseff como también a empresas nacionales y a la población en general, creando cierto nivel de desconfianza sobre las medidas de seguridad.

El gobierno estadounidense interceptó llamadas y mensajes de texto de empresas y ciudadanos brasileños de forma masiva, pidiendo al gobierno una aclaración al embajador de Estados Unidos en Brasilia, Thomas Shannon y en Washington a través de su embajada.

El Canciller brasileño Luis Fuigueiredo anunció que el gobierno se reuniría con países del BRIC para tomar medidas contra el espionaje en llamadas y correos electrónicos por parte de Estados Unidos, calificando el tema como un hecho alarmante para la soberanía del Estado.

"Por otra parte, la presidenta Dilma Rousseff emitió determinadas reacciones, principalmente políticas frente al espionaje estadounidense, expresando un total rechazo a ello, así como implementando medidas para frenar las filtraciones e interceptación de los dispositivos u ordenadores con valor estratégico y económico del país."[198]

Dentro de las medidas que se tomaron en las políticas internas relacionadas con los servicios de telecomunicaciones utilizados por el ministerio público brasileño, con el fin de proteger la información del mismo y así no exponerla a ser espiada.

México

[198] Calderón Canales Rebeca, Chiquillo Benítez Vilma, Rodríguez Peña Yasmin, Espionaje como instrumento de la política exterior de Estados Unidos de América y las consecuencias en sus relaciones exteriores. Casos: República Federal de Alemania y República Federativa de Brasil, op.cit. p. 130.

De acuerdo a los documentos filtrados por Edward Snowden, "[…] se dió a conocer que fueron hackeados correos electrónicos de Felipe Calderón por la NSA cuando todavía ejercía el poder, por lo que la cancillería de México expuso su molestia sobre las actividades de espionaje, tachándolas como inaceptables, ilegales y contraria a las buenas relaciones entre los dos países."[199]

"La National Security Agency (NSA) hackeo cuentas de correo electrónico de la Presidencia de México por años, obteniendo información interna a través de su división especializada en espionaje denominada Operaciones de Acceso Personalizado (Tailored Access Operations, TAO, por sus siglas en inglés, con sede en una vieja fábrica de electrónicos Sony, en San Antonio, Texas) espió a la Secretaría de Seguridad Publica, hoy Comisión Nacional de Seguridad. La TAO filtró cuentas de correo electrónico de funcionarios y luego de toda la red de cómputo, ingresando a los servidores de la secretaría se obtuvieron las direcciones de IP y diagramas de las estructuras de la institución."[200]

La postura que tomó México ante el problema de espionaje fue pasivo, "[…] la Secretaría de Relaciones Exteriores publicó un comunicado en el cual se indicaba que las prácticas de espionaje eran contrarias a la Carta de las Naciones Unidas y a la jurisprudencia de la Corte Internacional de Justicia; por su parte el presidente Enrique Peña Nieto comunicó sobre un posible acercamiento de manera informal con el presidente Barack Obama para aclarar los actos y conductas de espionaje."[201]

Debido al malestar y desconfianza que provocó entre los aliados de Estados Unidos, el uso del programa PRISM de ciberespionaje masivo, el Presidente Barack Obama compareció públicamente desde el Departamento de Justicia para

---

[199] BBC, México condena supuesto espionaje de EE.UU. a Calderón, 21 de Octubre de 2013, disponible en línea: http://www.bbc.com/mundo/ultimas_noticias/2013/10/131020_ultnot_mexico_snowden_nsa_espionaje_cch, Fecha de consulta: 21 de Junio de 2017.

[200] La Jornada, La NSA espiaba a la Secretaría de Seguridad Pública, 30 de Diciembre de 2013, disponible en línea: http://wikileaks.jornada.com.mx/notas/la-nsa-espiaba-a-la-secretaría-de-seguridad-publica, Fecha de consulta: 21 de Junio de2017.

[201] Molina Javier, Polémica en México por el espionaje de Estados Unidos, El país, 04 de Septiembre de 2013, disponible en línea: http://internacional.elpais.com/internacional/2013/09/05/actualidad/1378341578_816433.html, Fecha de consulta: 21 de Junio de 2017.

enumerar y explicar a los conciudadanos, y al resto de la comunidad internacional, las medidas que su administración adoptó para controlar las actividades "SIGINT"[202] también conocidas como inteligencia de señales del sistema nacional de inteligencia de los Estados Unidos.

> "Aun defendiendo la legitimidad y legalidad de sus programas, el presidente Obama se comprometió a ejecutar un conjunto de reformas en los próximos meses; recogidas estas en la Directiva Política Presidencial 28 (Presidential Policy Directive 28- Signals Intelligence Activities, PPD-28), Obama anuncio que dejara de espiar a los líderes de países aliados y pondrá limites a los procesos de obtención de información de los servicios de inteligencia del país haciéndolos compatibles con los derechos civiles y la privacidad de los ciudadanos estadounidenses y del resto del mundo."[203]

En la reunión del G20 de 2013, el Presidente Barack Obama justificó las acciones realizadas por su gobierno en contra de países como México y Brasil, a fin de obtener información de sus respectivos presidentes y de algunas empresas públicas, y las catalogó como actos de inteligencia, para resguardar su seguridad nacional.

Tomando en cuenta los actos de ciberespionaje por parte de la *National Security Strategy Agency* (NSA) hacia México y Brasil, Barack Obama justificó las técnicas de inteligencia, debido a que la tecnología cambia rápidamente, por lo que se deben de tomar en cuenta medidas que generen beneficios y se pueda proteger los intereses de Estados Unidos, aunque genere fricciones entre los demás países por violar su privacidad y las libertades civiles de los ciudadanos.

El Presidente Barack Obama al ser cuestionado sobre las filtraciones de la NSA referente a sus principales aliados y socios comerciales (México y Brasil), habló sobre las reuniones bilaterales que tuvo con la Presidenta de Brasil Dilma Rousseff y el Presidente Enrique Peña Nieto para explicar los actos de inteligencia para resguardar la seguridad nacional.

---

[202] Es la obtención de información mediante la intercepción de señales entre personas mediante señales electrónicas entre los medios de comunicación, en la inteligencia de señales se utiliza criptoanálisis para la recolección de información delicada.

[203] Hernández Lorente Adolfo, Vigilados por defecto, Ed. Ministerio de Defensa, 4 de Abril de 2014, p.5, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2014porDefecto_Hdez-Colom-Fojon.pdf, Fecha de consulta: 18 de Julio de 2017.

> "Presidente Barack Obama: Me reuní con la presidenta Rousseff y con el presidente Enrique Peña Nieto, de Brasil y México, respectivamente, para discutir estos alegatos que se hicieron en la prensa sobre la NSA, lo que les dije fue consistente con lo que he dicho públicamente. Estados Unidos tiene una agencia de inteligencia, y el trabajo de nuestra agencia de inteligencia es recolectar información que no está disponible a través de fuentes públicas, entonces no sería una agencia de inteligencia. En este sentido, lo que hacemos es similar a lo que hacen los países de todo el mundo con sus servicios de inteligencia."[204]

Con referencia a lo que dijo Barack Obama en el foro del G20 en 2013 sobre sus métodos de recolección de información, son utilizados como un método de monitoreo entre sus principales aliados y socios comerciales para resguardar la seguridad internacional, debido a que no existe una ley que regule los actos de ciberespionaje no se puede aplicar un castigo, por lo que se deben de aplicar medidas para proteger la seguridad en el ciberespacio y los intereses de los países aliados como es México y Brasil.

4.4 Análisis de las medidas de ciberseguridad

Las acciones emprendidas en la primera administración de Barack Obama por la *National Security Agency* (NSA) se enfocaron en el espionaje telefónico, la intercepción de todo tipo de datos de los servidores centrales de las compañías estadounidenses más poderosas de internet y tecnología, y creaciones de programas de ciberespionaje que actúan fuera de territorio(véase en anexo 4).

A continuación se detallan las medidas de ciberseguridad implementadas para la protección de Estados Unidos:

El 12 de febrero del 2013, el presidente Barack Obama firmó un decreto de ciberseguridad que, proponía entre otras cosas permitirle al gobierno intercambiar con empresas privadas las "ciberamenazas" que fueran consideradas como un riesgo para el país. Mediante este decreto se facilitaría el flujo de información entre el gobierno y las compañías de tecnología.

[204] The White House, Remarcks by President Obama in a Press Conference at the G20, 06 de Septiembre de 2013, disponible en línea: https://obamawhitehouse.archives.gov/the-press-office/2013/09/06/remarks-president-obama-press-conference-g20, Fecha de consulta: 09 de Agosto de 2017.

En este decreto el presidente Obama señala la importancia de Estados Unidos frente a las amenazas que representan los ciberataques; el propósito de este decreto consistía en permitir una cooperación más fluida entre el sector privado y público, incluyendo al sector empresarial que sea ajeno al ámbito de defensa.

Otra de las medidas que se pusieron en marcha durante la primera administración de Barack Obama fue el: *Cybersecurity National Action Plan* (Plan de acción Nacional de Ciberseguridad), para llevar acciones a un corto plazo y poner en marcha una estrategia a largo plazo, para asegurar una triangulación entre el gobierno, las empresas y los ciudadanos estadounidenses con el fin de tener un mejor control de la seguridad informática.

Los objetivos que se fijaron en el *Cybersecurity Nacional Action Plan*, fueron los siguientes:

- Establecer una Comisión nacional para la modernización de la Ciberseguridad traerá consigo personal calificado para implementar estrategias de alto nivel, de negocio así como técnicos fuera del gobierno para hacer recomendaciones criticas de cómo se pueden utilizar de manera óptima las nuevas soluciones técnicas y las mejores prácticas para proteger datos y el acceso seguro en la red de los usuarios y la seguridad pública.
- Convertir la manera en que el gobierno se encargue de la ciberseguridad a través de la gestión de un Fondo de Modernización de Tecnologías de la información de $ 3.1 mil millones de USD y la implementación de un Jefe de Información Oficial Federal de Seguridad que ayudara a retirar, sustituir y modernizar la infraestructura de las TIC´s en el gobierno.
- Capacitar a la población norteamericana, para asegurar sus cuentas en línea mediante el uso de herramientas de seguridad adicionales, como múltiples factores de autentificación, cambios de contraseñas periódicamente y otros pasos de procesamiento de identidad, además trabajar con las empresas Google, Facebook, Dropbox, Microsoft, empresas financieras como Visa, Pay Pal, y Venmo para proteger las cuentas en línea y las transacciones financieras.

- Invertir más de $19 mil millones de dólares para la seguridad informática como parte del presupuesto del presidente, además de un aumento de más del 35% a comparación del año posterior y con ello asegurar el futuro de la Nación.[205]

Otra de las medidas de ciberseguridad que se tomó durante la presidencia de Barack Obama fue restablecer las relaciones diplomáticas con China, por lo que ambos países pactaron trabajar de manera conjunta en las agendas en materia de seguridad de Washington y Beijing, después de los ataques cibernéticos hacia empresas estadounidenses.

Ambos gobiernos acordaron el 25 de septiembre de 2015, medidas de ciberseguridad para evitar problemas de ciberespionaje:

- Intercambiar información sobre investigaciones relacionadas con actividades maliciosas en el ciberespacio.
- No apoyar actividades de ciberespionaje que puedan menoscabar los intereses comerciales e industriales de ambos países.
- Identificar y promover normas de buena conducta en el uso del ciberespacio por parte de los Estados.[206]

Con las medidas de ciberseguridad que acordaron implementar el gobierno de China y Estados Unidos a fin de contrarrestar el ciberespionaje, es un paso importante en las acciones de seguridad que se necesita tomar en el ciberespacio, para proporcionar una respuesta oportuna a los problemas de espionaje.

Otro punto importante de resaltar sobre el acuerdo es si ambos países acataran las reglas establecidas en materia de ciberseguridad, para promover el uso del

[205] Hoja de Datos: Plan Acción Nacional de Ciberseguridad, The White House, Office of the Press secretary, 09 de Febrero 2016, disponible en línea: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan, Fecha de consulta: 19 de Junio de 2017.
[206] Forjón Chamorro Enrique, ¿Diplomacia para luchar contra el ciberespionaje?, Ed. Real Instituto el cano Royal Institute, 02 de Octubre de 2015, disponible en línea: http://www.blog.rielcano.org/diplomacia-para-luchar-contra-el ciberespionaje/, Fecha de consulta: 19 de Julio de 2017.

ciberespacio de forma correcta en el sistema internacional y evitar las actividades maliciosas como es el robo cibernético y los actos de ciberespionaje.

Sin embargo las acciones que se implementaran no representan una seguridad impenetrable debido a que los ataques cibernéticos se pueden realizar desde cualquier punto del planeta, aunque cabe destacar que el acuerdo entre las dos potencias internacionales constituye una iniciativa importante a nivel mundial.

4.5 Impacto de las medidas de ciberseguridad contra el Ciberterrorismo

"Para entender que es y cómo funciona el ciberterrorismo, se debe de partir desde su origen: El terrorismo se puede definir como redes operativas que usan de manera ilegal la fuerza y la violencia contra personas y objetivos, para intimidar o presionar a los gobiernos, pueblos y/o sectores específicos como pueden ser políticos y sociales"[207]

De acuerdo al autor Santiago Acurio, define al ciberterrorismo o terrorismo informático como: "el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados o poco convencionales provocando sabotaje al funcionamiento de la infraestructura informática."[208]

En los últimos años se ha detectado que las alteraciones cibernéticas en la red y en ordenadores gubernamentales se han producido tanto de la mano de actores conocidos o no conocidos, destacando grupos terroristas, el terrorismo ha estado inmerso en las redes tecnológicas en cualquier parte del mundo, los grupos terroristas ocupan internet para planear y coordinar acciones para obtener y compartir información para reclutar seguidores y expandirse en cualquier parte del planeta para obtener fondos, hacer propaganda y llevar a cabo guerras desde el ciberespacio.

[207] J. Gebhardt J. Bruce, Ciberterrorismo: Nefasta evolución, 07 de Febrero de 2014, disponible en línea: https://es.scribd.com/document/205282600/ciberterrorismo-pdf, Fecha de consulta: 07 de Julio de 2017.
[208] Del Pino Acurio Santiago, Delitos informáticos: Generalidades, Ed. PUCE, Ecuador, 2013, p. 27.

El uso de redes sociales virtuales ha aumentado de forma exponencial en Medio Oriente, por lo que ha sido aprovechada esta plataforma por grupos terroristas que ya no solo utilizan internet para buscar medios de financiación, propaganda o reclutar nuevos militantes sino cometer ciberataques evitando ser rastreados en la red y tener una presencia en este medio de comunicación para seguir cometiendo atentados.

Uno de los principales blancos de los ciberterroristas son las redes computacionales que proveen servicios públicos, tales como los sistemas de control de energía eléctrica, aeropuertos, redes de trenes, redes satelitales, sistemas financieros y de emergencia, mediante varias técnicas, pero la que más han empleado es el uso de robots informáticos mejor conocidos como *botnets,* los cuales son controlados por los hackers y por medio de este virus enviar ataques desde cualquier punto del planeta.

Principalmente los grupos ciberterroristas direccionan sus operaciones por medio de mensajes encriptados a través del correo electrónico, impidiendo a los expertos de seguridad entrar en los servidores.

Los ataques terroristas no solo afectan a las redes y sistemas informáticos de Estados Unidos, también a sistemas de control de tráfico aéreo, redes de suministro energético, sistemas financieros, así como redes de inteligencia y militares.

Grupos terroristas que atentan a la ciberseguridad de Estados Unidos.

Los países como China, Irán, y Rusia tienen un interés estratégico en el ciberespacio como vehículo para alcanzar posiciones de liderazgo económico y político en sus áreas geográficas de influencia, y lo están logrando en la implementación de políticas internas, por lo que han invertido en la ejecución recursos de las TIC y en la formación de recursos humanos, con el objetivo de establecer “una defensa beligerante” en el ciberespacio y por ende en estos países se ha mostrado mayor auge de grupos terroristas para cometer

ciberataques y ciberespionaje principalmente a Estados Unidos con el fin de lograr una desestabilización en el desarrollo de sus actividades políticas y económicas.

Al Qaeda

El grupo terrorista Al Qaeda tiene presencia en el ciberespacio desde 2011, es uno de los principales grupos terroristas que inicio ataques por medio del espacio cibernético, "opera con la asistencia de extensas bases de datos que contienen potenciales objetivos americanos; esta célula terrorista utiliza internet para recoger información principalmente en el ámbito económico, y tecnológico para poder analizar deficiencias estructurales en la infraestructura critica americana y provocar daños colaterales."[209]

En cuanto a planificación y coordinación, AL Qaeda controla sus operaciones en internet por medio de plataformas en la *deep web* para coordinar ataques de manera simultánea desde cualquier parte del mundo mediante el uso de chats rooms en la red oscura para enviar instrucciones sobre cómo, cuándo, y donde realizar ataques terroristas.

Islamic Revolutionary Guard Corps

Islamic Revolucionary Guard Corps, es un ejército que depende de las fuerzas armadas de Irán, su objetivo es la protección del sistema de la República Islámica, evitando la interferencia extranjera, por lo que han sido acusados de varios delitos y ataques que atentan contra los intereses y la seguridad nacional de Estados Unidos llevados a cabo "entre 2011 y 2013, este grupo extremista comete sus ataques por la red, el *Islamic Revolutionary Guards Corps* trabaja para dos compañías tecnológicas iraníes (ITSec Team y Mersad) contratadas por el

[209] Carlini Agnese, ISIS: Una nueva amenaza en la era digital, Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 1 de Diciembre de 2017, p.5, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO1292015_ISIS_AmenazaEraDigital_AgneseCarlini.pdf, Fecha de consulta: 21 de Noviembre de 2017.

departamento de Justicia y por el gobierno iraní para llevar a cabo ciberataques."[210]

"De acuerdo al Fiscal General de Estados Unidos, los ciberterrorista de la *Islamic Revolucionary Guard Corps* tuvieron acceso al sistema de control de una presa situada al norte de Nueva York, donde accedieron a toda la información de su operación, sin embargo, se pudo evitar el ciberataque por el mantenimiento que le estaban dando en su momento a los sistemas operativos de la presa, evitando una catástrofe."[211]

Otro ejemplo de los ciberataques que ha hecho este grupo terrorista a las infraestructuras criticas estadounidenses, fueron las entidades financieras norteamericanas, que sufrieron alrededor de 187 ataques de denegación de servicios(DDoS), con el que saturaron varios servidores y los sistemas de la red infectándolos con un virus desconocido en su momento, impidiendo el acceso a los mismos.

Hezbollah

El grupo terrorista hezbollah surge a comienzos de los años 80 del siglo pasado, durante la ocupación del Líbano por Israel, para el Departamento de Estado de Estados Unidos, esta organización está incluida en su lista de organizaciones terroristas extranjeras desde el 8 de Octubre de 1997.

Hezbollah se retrata así mismo como un defensor de los oprimidos y los débiles frente a lo que valora como la injusticia de los poderosos, especialmente Estados Unidos e Israel. Los líderes del grupo terrorista consideran que la política exterior norteamericana está impulsada por la necesidad de consolidar la hegemonía política y económica de Estados Unidos bajo el pretexto de combatir el terrorismo.

---

[210] Buendía José, La justicia americana sigue su lucha contra el ciberterrorismo, mCpromuycomputer, 28 de Junio de 2016, disponible en línea: http://www.muycomputerpro.com/2016/03/28/la-justicia-americana-sigue-su-lucha-contra-el-ciberterrorismo, Fecha de consulta: 31 de Julio de 2017.

[211] Ídem.

En 2010, el gobierno del Presidente Barack Obama describió al grupo terrorista hezbollah como: “El grupo terrorista con más capacidad técnica del mundo, al mostrar gran actividad terrorista, infringiendo amenazas a aliados norteamericanos como es el caso de Israel.”[212]

Dentro de las actividades de este grupo extremista llamado Hezbollah, tiene una importante presencia institucional a través de un sitio web propio con el cual obtienen seguidores en todo el mundo, la forma en la que opera su portal es mediante tres “mirrors” (www.hizbollah.org, www.hizballah.org y www.hizbollah.tv).[213]

La actividad de Hezbollah en el ciberespacio, ha posicionado a la organización en el sistema internacional para cometer actos ilícitos a gran escala, gran parte de este acontecimiento se debe a su financiamiento, el cual se hace a través de donaciones en sus páginas web por sus seguidores.

Cabe mencionar que esta organización terrorista además de tener presencia en la red, también cuenta con armamento sofisticado, el cual se puede manipular a larga distancia por medio de ordenadores, cuenta con arsenal para infringir daños a otro Estados, dentro del armamento con en que cuenta esta organización, “es con 100 misiles de larga distancia llamados Fajr-3, Fajr-5 y Zelzal un misil con alcance de 150 km, dispone de misiles anti-carro, AT-3 Sagger, de fabricación rusa, AT-4 Spigot, AT-5 Spandrel, AT-13 Saxhorn-2, Metis-M, AT-14 Sprigan KOrnet, aviones no tripulados Mahajer-4 de fabricación iraní y un amplio arsenal de artillería ligera.”[214]

[212] Blanco Navarro José María, Hezbollah, el partido de Dios, 2015, Ed. Ministerio de Defensa, Grupo español de estudios Estratégicos, España, p.12, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_investig/2015/DIEEEINV012015_Hezbollahx_El_partido_de_Dios_JMBlanco.pdf, Fecha de consulta: 09 de Julio de 2017

[213] Los mirrors, son espejos en un sitio web que tiene una réplica exacta de otro; Estas replicas u espejos se suelen crear para facilitar descargas grandes y facilitar el acceso a la información aun cuando haya fallos en el servidor principal.

[214] Ibídem, p. 15.

Hamas

El grupo islámico Hamas es uno de los más poderosos en Palestina, en 2005 cobró más poder al participar activamente dentro del proceso político palestino; En 2006, Hamas alcanzó el poder tras lograr ganar las elecciones para el consejo Legislativo Palestino, debido a su actividad terrorista contra Israel, Estados Unidos ha tomado medidas de seguridad nacional para evitar cualquier atentado que provenga de este grupo islámico.

Los ataques terroristas de Hamas se han ido sofisticando con el tiempo, al utilizar bombas, misiles, explosivos de largo alcance, los cuales son manipulados desde cualquier lugar; Dentro de los ataques perpetrados por esta organización desde 2008, podemos ver una cronología de los ataques con mayor catástrofe en el siguiente cuadro número 6:

Cuadro 6 Ataques por el grupo Hamas

8 de Febrero de 2008	Hamas adjudica responsabilidad por los misiles dirigidos hacia la estación energética en Ashkelon, que provee a la Franja de Gaza con electricidad.
28 de Febrero de 2008	Misiles aterrizan en Sdert y sus alrededores.
2 de Marzo de 2008	Hamas dispara misiles Grad de gran alcance- importados de Irán hacia Ashkelon
12 de Junio 2008	Hamas lanza tres misiles Grand, 18 misiles Kassam y 22 morteros hacia Israel.
Diciembre 2008	Decenas de misiles impactan sobre Israel, provocando que se lance una operación defensiva contra Hamas en Gaza.

1 de Marzo 2009	Doce misiles Kassam explotan hacia Sderot desde Gaza causando daños a propiedades.

Fuente: Elaboración propia, con información tomada del documento Ataques terroristas perpetrados por Hamas, Madrid, 2005, pp.2-3, disponible en línea: http://embassies.gov.il/madrid/AboutIsrael/AboutIsraelInfo/Documents/Ataques_terroristas_perpetrados_por_Hamas.pdf, Fecha de consulta: 25 de Julio de 2017.

Debido a que los constantes ataques terroristas tenían gran alcance, el Presidente Barack Obama y el Primer Ministro Israelí Benjamín Netanyahu tuvieron una reunión bilateral el 1 de septiembre de 2011 para garantizar la seguridad de Israel.

El Presidente Barack Obama en su discurso menciono lo siguiente: "Quiero que quede muy claro: EE.UU. se va a mantener inquebrantable en su apoyo a la seguridad de Israel y vamos a hacer retroceder esa clase de actividades terroristas. Y en este sentido, el mensaje debería de ir más allá de Hamas y a todo aquel que de crédito a esos crímenes atroces, que esto no va a detenernos, no solo en el hecho de garantizar la seguridad de Israel sino en asegurar una paz duradera en la que los pueblos de toda la región puedan tomar un rumbo diferente."[215]

De acuerdo a Jehrom Chacón Vega: "todos los sistemas informáticos dependen del factor humano y por ende, este es el eslabón débil de la cadena de seguridad. Una de las Leyes de seguridad Informática establece que la tecnología no es 100% segura, convirtiéndose en una vía fácil para cometer actos terroristas."[216]

Debido al temor de ataques terroristas, las medidas de ciberseguridad que se han implementado en Estados Unidos han sido la piedra angular para contrarrestar las sofisticadas redes de delincuentes y terroristas que operan en el ciberespacio, poniendo en marcha el Mando Cibernético de EE.UU. mejor conocido por su acrónimo CYBERCOM.

[215] Ibídem, p.1.
[216] Chacón Vega Jehron, Seguridad informática: factor humano- principios, Revista digital En-Toas, disponible en línea: http://revistaentoas.com/seguridad-informatica-factor-humano-principios/, Fecha de consulta: 08 de Julio de 2017.

> "La legislación Federal de Estados Unidos del 15 de Abril de 2002, establece penas para el acceso no autorizado de sistemas informáticos, previendo específicamente el acceso a sistemas del gobierno relacionados con la seguridad del Estado, por lo que se encuentra castigada la comunicación, la entrega, transmisión e incluso el solo intento de realizar actos que atenten a la seguridad nacional."[217]

El ejército CYBERCOM está al mando del Comando Estratégico USSTRATCOM de los Estados Unidos, considerado uno de los nueve comandos unificados bajo el Departamento de Defensa (DoD) Con sede en la Base de la Fuerza Aérea de Offutt, Nebraska, proporciona apoyo a comandos combatientes como es la defensa, vigilancia, control, comunicaciones, computadoras, inteligencia y reconocimiento.

El comando CYBERCOM se centra en aplicar medidas defensivas en el ciberespacio, sin dejar de lado la protección del ciberespacio mediante estrategias de ataque a enemigos en el ciberespacio.

Frente al terrorismo, se busca mejorar la seguridad interna del país a través de "esfuerzos comunes para prevenir y disuadir los ataques mediante la identificación y la interdicción de las amenazas, negando a los actores hostiles la capacidad de operar dentro de las fronteras norteamericanas, además de proteger la infraestructura crítica de la nación y sus principales recursos, y asegurar el ciberespacio."[218]

Dentro de las medidas de seguridad para contrarrestar en Ciberterrorismo es la implementación de un programa llamado Dark Web, "el cual se centra en actividades terroristas, fue creado por la Universidad de Arizona, el programa utiliza técnicas como el uso de arañas y análisis de enlaces, contenidos, autoría,

[217] Orta Martínez Raymond, Ciberterrorismo, conferencia dictada en la Facultad de Ciencias Jurídicas y Políticas de la Universidad de Carabobo, disponible en línea: http://servicio.bc.uc.edu.ve/derecho/revista/relcrim21/art06.pdf, Fecha de consulta: 08 de Julio de 2017.

[218] Herrera Yopo Boris, La nueva estrategia de Seguridad Nacional de Estados Unidos: sus implicancias regionales, Academia Nacional de Estudios Políticos y Estratégicos, Boletín de investigación No.6, Diciembre de 2013, disponible en línea: https://anepe.cl/wp-content/uploads/boris_yopo_bolet%C3%ADnN%C2%BA-6.pdf, Fecha de consulta: 10 de Julio de 2017.

opiniones y multimedia para poder encontrar, catalogar y analizar actividades de extremistas en la red"[219]

El programa Dark Web cuenta con la herramienta Writeprint, la cual extrae automaticamente características multibilingues, estructurales y semánticas para determinar quien esta creando contenido anónimo en la red, con este programa se puede lograr un seguimiento de actividades terroristas que se esten llevando a cabo en páginas de dudosa procedencia o información que se reproduce en foros para conseguir mayor número de seguidores.

Otra medida de seguridad muy utilizada en Estados Unidos es el sistema llamado *Supervisory Control and Data Acqisition* (SCADA), permite el control y manipulacion de cualquier sistema local o remoto sin la necesidad que sea manipulado por un factor humano, este software esta principalmente diseñado para el control y protección de infraestructuras críticas que son resguardadas mediante instrumentos digitales como es el uso de una "interfaz gráfica"[220]

En Estados Unidos el sistema SCADA, es utilizado para mantener el control de oleoductos, sistemas de transmisión de energía eléctrica, yacimientos de gas y petróleo, redes de distribución de gas natural y generación energética, debido a la estructura del software es difícil que los hackers tengan acceso al sistema debido a que se configura en un lapso de tiempo corto.

La importancia de una legislación para contrarestar el terrorismo cibernético se centra en aumentar el intercambio entre el sector privado y el gobierno para informar de posibles amenazas en tiempo real al Departamento de Seguridad Nacional (DHS por sus siglas en inglés), el cual enviará los datos obtenidos por las empresas a otras agencias federales de información.

[219] Sánchez Madero Gema, Los Estados y la Ciberguerra, Ed.Universidad complutense de Madrid, 2010, p. 69, disponible en línea: dialnet.unirioja.es, Fecha de consulta: 14 de Julio de 2017.
[220] Una interfaz gráfica es un conjunto de imágenes y objetos gráficos que son utilizados para representar información y controlar en tiempo real ordenadores por medio de una interfaz que se conectan a los sistemas de comunicación.

El Presidente Barack Obama presentó en Febrero de 2013 una orden ejecutiva para mejorar la defensa nacional contra ataques cibernéticos, con la finalidad de proteger los sectores más vulnerables a los ciberataques, por medio de una alianza estratégica entre el sector privado y público, para actuar de forma rápida y eficaz en la detección y protección de la infraestructura informática.

"El Departamento de Seguridad Nacional será el encargado de proteger las principales infraestructuras y establecer un flujo de comunicación con las instituciones privadas para que puedan reportar posibles amenazas; con esta orden ejecutiva las empresas privadas podrán trabajar de forma conjunta con el Instituto Nacional de Estándares y Tecnología para que de esta manera los estándares de seguridad cibernética se puedan unificar."[221]

Con la Orden ejecutiva que pronunció el presidente Barack Obama en 2013, servirá como herramienta de apoyo para realizar trabajo en equipo con las empresas privadas para la detección y protección en el ciberespacio de ataques terroristas, aunque en primera estancia las empresas de tecnología no están obligadas a ejecutar las normas de protección para la ciberseguridad debido a que su infraestructura cibernética es débil en comparación de las grandes empresas que son pioneras en la innovación tecnológica, por lo que se debería de poner mayor énfasis sobre los lineamientos en los protocolos de seguridad para que se puedan seguir de manera óptima.

"Tras las revelaciones de Edward Snowden sobre la vigilancia masiva por parte de Estados Unidos y agencias de espionaje Británicos, las relaciones con la industria de la tecnología quedaron dañadas; Empresas como Google y Apple están bajo enorme presión para convencer a sus clientes de que sus comunicaciones son

[221] Zazo Lara, ¿Toma medidas mañana Obama sobre ciberterrorismo?, Computer Hoy, 12 de Febrero de 2013, disponible en línea: http://computerhoy.com/noticias/software/tomara-medidas-manana-obama-ciberterrorismo-3078, Fecha de consulta: 12 de Septiembre de 2017.

totalmente seguras y privadas, en el caso de Apple, por ejemplo, ha cambiado su infraestructura para que sea imposible entregar datos del servicio IMessagge."[222]

Con las medidas de seguridad y protección de datos que están llevando a cabo las empresas con mayor proyección internacional (Google, Apple), dificulta llevar a cabo las operaciones de ciberseguridad entre el sector público y privado haciendo más difícil las operaciones de vigilancia.

Conclusiones

A través del tiempo la protección de comunicaciones ha sido un factor importante para el desarrollo y funcionamiento de los países en el sistema internacional, ejemplo de ello fue el lanzamiento del primer satélite soviético llamado Spunik con el cual se inició una etapa que trajo consigo toda una serie de adelantos tecnológicos pero que también trajo una serie de problemáticas como guerras asimétricas.

Los medios tecnológicos y el internet han sido elementos que han experimentado un mayor desarrollo a lo largo del tiempo, desde la primera computadora, hasta el avanzado uso que hoy en día se le da a los dispositivos electrónicos y el uso de internet como medio de interacción y comunicación al alcance de cualquier ser humano que tenga un dispositivo electrónico.

De esta investigación podemos concluir que las Relaciones Internacionales a partir de la globalización, se ha reconfigurado un orden en la dinámica mundial, mediante el uso del ciberespacio que ha cobrado mayor relevancia al permitir interrelacionarse sin el impedimento del lugar, tiempo y espacio, tomando en cuenta que los riesgos aumentan y cambian constantemente por lo cual la ciberseguridad es primordial para establecer medidas que regulen y protejan la seguridad , sin interferir en la soberanía de la Estados, como lo ha venido haciendo Estados Unidos con los programas de ciberespionaje.

[222] Benedicto Solsona Miguel A., El discurso del Estado de la Unión: Obama se niega a condescender, Instituto Español de estudios Estratégicos, 3 de Febrero 2015, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO152015_DiscursoNacionUS_MABenedicto.pdf, Fecha de consulta: 12 de Septiembre de 2017.

Con la globalización los medios tecnológicos han tenido un papel importante como medios de comunicación no solo de los Estados sino también de la sociedad, que han utilizado internet como un componente de información alrededor del mundo, aunque esta revolución del uso del ciberespacio y las telecomunicaciones ha sido benéfico también ha afectado a Estados y organizaciones, que por medio de programas de ciberespionaje y armas de ataque destructivas se han obtenido determinadas ventajas sobre otros actores internacionales, como es la desestabilización de los países por medio de filtraciones en los sistemas que controlan las infraestructuras críticas. Como fue el caso de Irán que fueron paralizadas totalmente sus plantas nucleares por un virus stuxnet que se filtró al sistema de seguridad SCADA.

Debido a las vulnerabilidades en la infraestructura cibernética, Estados Unidos ha implementado medidas de ciberseguridad más eficaces, después de la creación de ARPANET que fue en 1969, como es la creación de un ejército cibernético llamado USCYBERCOM, capaz de detectar amenazas y contrarrestarlas en tiempo real o el caso de armas cibernéticas como es el uso de implantes en dispositivos electrónicos que permiten a las agencias de inteligencia interceptar dispositivos desde su base de operaciones.

El proyecto ARPANET tuvo varias modificaciones en sus protocolos de conexión para utilizarse en operaciones militares, aunque debido a la poca seguridad que tenía el proyecto ARPANET, se comenzó a desarrollar y utilizar lo que hoy en día conocemos como internet, por lo cual no es un tema reciente sino que ya lleva varios años que el uso de la red en el ciberespacio sirve como un medio intangible de interacción que si no se utiliza adecuadamente representa un peligro para la seguridad nacional.

Las operaciones que se hacen en el ciberespacio por lo regular se hacen de forma anónima de acuerdo a la clasificación de internet que el usuario utilice, en el caso del internet profundo es de difícil acceso con los motores de búsqueda convencionales, en esta parte de internet se puede encontrar bases de datos y

hacer transacciones de forma ilegal, siendo un espacio propicio para los hackers que cometen actos ilícitos.

Con la primera administración de Barack Obama el tema de ciberseguridad cobró mayor relevancia tras sufrir ciberespionaje en su campaña presidencial de 2008, en 2009 se establecieron estrategias de ciberseguridad más agresivas que las de su antecesor George W. Bush en las cuales se especificaba que el ciberespacio se debería de tomar en cuenta como cualquier campo de batalla convencional, además de aplicarse medidas defensivas ante posibles amenazas.

También se establecerían alianzas estratégicas entre los países aliados de Estados Unidos para apoyarse mediante ciberdefensas y mejorar la industria tecnológica con la innovación y adquisición constante de equipo y programas de seguridad.

Las estrategias nacionales de ciberseguridad deben de servir como un instrumento que guie, organice y gestione a los sectores inmiscuidos en la seguridad cibernética, involucrando a las organizaciones tanto públicas como privadas y a la sociedad en general, fomentar la participación tanto de asociaciones, universidades, expertos en tecnología para contribuir en la defensa del ciberespacio mediante la capacitación del uso responsable de la tecnología como medio de comunicación e interacción entre el ser humano para trabajar de forma coordinada ante posibles ataques o proliferaciones de virus informáticos que puedan causar daños a las infraestructuras criticas nacionales y provocar caos en el desarrollo del país.

Con las estrategias de ciberseguridad que se han implementado por parte de las agencias de inteligencia como la CIA y la NSA, las medidas de seguridad han estado encaminadas hacia un trabajo en equipo no solo con los países aliados, sino también de empresas tecnológicas del sector privado para la obtención de información de cualquier usuario con la finalidad de prevenir actos terroristas aunque pareciera que la actividad de recopilación de datos está enfocada a un mayor control en las redes de comunicación mundiales.

Como bien se menciona en la hipótesis que sustenta la investigación, Estados Unidos utiliza las estrategias de ciberseguridad para coordinar al sector público y privado, para hacer frente a las ciberamenazas principalmente por grupos terroristas, por lo que implementa programas de vigilancia que violan la soberanía de los Estados por la gran cantidad de información que recopilan.

Para Estados Unidos tener en sus manos información precisa, veraz y oportuna representa un medio de poder con la finalidad de preservar u obtener predominancia sobre el resto del mundo, no escatiman esfuerzos para recopilar la mayor cantidad de información sobre los gustos, intereses, fortalezas, debilidades, hábitos, vicios, y todo aquello que permita un conocimiento anticipado y profundo de las contrapartes, permitiendo detectar amenazas y neutralizarlas a tiempo.

Con el uso de la ciberinteligencia se puede interferir la información que pasa en la red a nivel internacional, con el fin de controlar y prevenir acontecimientos que puedan entorpecer el desarrollo de Estados Unidos, por lo que la ciberinteligencia es una parte fundamental para la ciberseguridad porque a partir de la información obtenida se pueden establecer estrategias de inteligencia de acuerdo a las amenazas que se presenten.

Actualmente se vive en un mundo conectado digitalmente, donde la información sensible fluye en la red, las infraestructuras críticas son susceptibles a las amenazas cibernéticas desde ataques patrocinados por grupos terroristas a delincuencia cibernética en menor grado, tanto gobiernos como individuos de cualquier edad son vulnerables en el ciberespacio, por lo cual los proveedores de servicios de internet, telecomunicaciones, software y servicios financieros se ven obligadas bajo la Ley de FISA a dar información de sus clientes al gobierno norteamericano para identificar posibles amenazas.

El desarrollo tecnológico actual, ha revolucionado en muchos campos la forma de producción y socialización de la vida común y la individualidad e intimidad de las personas con el uso de internet, debido a que se han transformado las actividades de socialización e interacción del ser humano mediante el uso de redes sociales

en el ciberespacio en tiempo real por personas en diferentes partes del mundo, donde los datos personales se procesan y se guardan en segundos.

Por lo que la seguridad cibernética afecta a todos, incluso a personas que no se encuentran familiarizadas con dispositivos electrónicos que se conecten a la red, tanto los Estados, empresas y organizaciones no gubernamentales que mantienen en sus sistemas datos personales como puede ser correos electrónicos, redes sociales, banca en línea, convirtiendo el acceso a la tecnología en una actividad cotidiana del ser humano, el cual no cuenta con una educación óptima sobre el uso de la tecnología de manera responsable provocando la exposición a amenazas potenciales en los servidores conectados a la red y provocando que las medidas de seguridad que se implementan fracasen en su ejecución.

En internet no hay fronteras, por lo que no hay un control en el uso de las tecnologías de la información y comunicación (TIC), debido a que en internet no existe una gobernabilidad los medios de comunicación y el ciberterrorismo tienen un campo abierto para cometer actos ilegales, derivado a esto los países deben de comprometerse a cumplir regularizaciones en el ciberespacio de manera conjunta tomando en cuenta la cultura de cada Estado porque a partir de la cultura se van a delimitar las legislaciones políticas y legales para que pueda haber un mejor control en el sistema informático.

En el caso del uso de internet, se originó una nueva forma de combate en el cual el mundo virtual es otro espacio para la disputa de intereses debido a que las comunicaciones se hacen en tiempo real; las fronteras y distancia entre países se ven diluidas e inexistentes en el ciberespacio, por lo que Estados Unidos establece sus reglas en el ciberespacio debido a su mayor dominio tecnológico.

Sin embargo, el uso de armas cibernéticas no solo pueden presentar daños en el espacio virtual, también pueden ocasionar daños en el mundo físico con el uso de aviones no tripulados conocidos como drones, siendo estos una arma de destrucción ventajosa por su tamaño, costo y fácil manipulación que puede ser a larga distancia.

En el caso de Estados Unidos hay iniciativas que se han impulsado como fue en 2008 con la iniciativa Amendments Comprehensive National Cybersecurity Iniciative y la International Strategy for Cyberspace en 2010, con estas iniciativas se busca establecer una diplomacia pública de ciberseguridad cibernética entre los Estados para crear conciencia de las amenazas cibernéticas y el gran alcance que pueden tener al propagarse desde cualquier ordenador.

Con las actividades de apoyo entre los demás países, Estados Unidos busca reforzar la protección de la seguridad ante ciberataques provenientes de grupos terroristas con el uso de actividades secretas de las agencias de inteligencia como es la interceptación de llamadas, comunicaciones y dispositivos móviles, con la finalidad de “garantizar un mayor control judicial” en el ciberespacio, mediante el uso del ciberespionaje.

Dentro de los efectos de espionaje y ciberespionaje, la soberanía de los Estados se ve afectada por las acciones de inteligencia que utiliza Estados Unidos para obtener información y evitar vulnerabilidades que provoquen un mal funcionamiento en la infraestructura critica del país, mediante intervenciones que se realizan a los medios de comunicación electrónicos, provocando que se incline la balanza de poder hacia un solo lado.

Hoy en día , la capacidad de memoria para el procesamiento de datos y de los dispositivos de almacenamiento es insuficiente debido a la inmensa cantidad de información que requiere ser procesada o al menos resguardada, convirtiéndose en una de las principales debilidades de los sistemas digitales; ya que con el surgimiento de un espacio virtual las medidas de ciberseguridad van a ser efectivas de acuerdo a la capacidad de almacenamiento en el ciberespacio para tener mayor control en la información que fluye en la red y la capacidad de almacenamiento de armas virtuales para proteger la infraestructura cibernética.

Un segundo desafío para la National Security Agency (NSA) es la preservación de la seguridad de los datos propios y ajenos que han sido recopilados por la comunidad de inteligencia, ya que las recientes filtraciones realizadas por

miembros de su personal sobre las actividades de espionaje que lleva a cabo dicha institución, ponen de manifiesto que, tal y como se ve en cualquier otro sistema de inteligencia, hay vulnerabilidades que no pasan desapercibidas y pueden ocasionar problemas con la filtración de información.

Debido a los desafíos que se presentan con los avances en las tecnologías de la comunicación e información, las estrategias de ciberseguridad se deben de ir enfocando de acuerdo a los desafíos actuales en la red, las estrategias de seguridad que se establecen entre el sector privado y público se ha convertido en una parte importante para la protección de la infraestructura de la información por lo que en la Iniciativa Nacional para la Educación de la Ciberseguridad (NICE por sus siglas en inglés), se precisan lineamientos para trabajar de manera conjunta para la protección de la infraestructura informática estadounidense mediante la capacitación de personal que ayude en la detección de vulnerabilidades en los sistemas de las empresas mediante consultorías sobre el uso de herramientas de protección como antivirus y respaldo de información como es el uso de la plataforma Cloud computing para evitar riesgos y amenazas a sus sistemas operativos.

Sin embargo al dejar en manos de empresas privadas las operaciones de seguridad de forma parcial podría resultar problemático, por la gran cantidad de actores que tienen interferencia en los sistemas provocando que las legislaciones se vean afectadas por los intereses de particulares, poniendo en riesgo la seguridad nacional estadounidense.

En las estrategias de ciberseguridad se deben de tomar en cuenta todos los actores involucrados para fortalecer las medidas de seguridad, estableciendo políticas internacionales que todos los países se comprometan a cumplir, así como también crear instituciones especializadas que coordinen las estrategias de ciberseguridad para proteger las infraestructuras críticas mediante la cooperación internacional y por parte del sector privado imponer medidas precautorias como es la capacitación de su personal a fin de prevenir vulnerabilidades.

Por otra parte las herramientas de seguridad que implementa el gobierno de Estados Unidos por medio de sus agencias de inteligencia y empresas de tecnología para la protección de la infraestructura cibernética, como es la encriptación de los sistemas de seguridad ha sido fundamental para evitar filtraciones de enemigos en los sectores estratégicos nacionales, y en el caso de los sistemas de espionaje y contraespionaje, como es el uso de aviones no tripulados, drones y los programas de espionaje que han causado controversia por las operaciones para la detección de ciberterroristas, en el caso del programa PRISM que opera bajo la Ley FISA (Foreing Intelligence Surveillance Court), la cual permite los procedimientos de vigilancia y recolección de datos de los ciudadanos norteamericanos mediante la interceptación de información obligando a las grandes empresas de tecnología a brindar información personal de los usuarios.

A pesar de los sistemas de encriptación de datos, los actos de espionaje y contraespionaje siguen vigentes ejemplo de ello es el caso de wikileaks , a pesar de implementar medidas de ciberseguridad, personal que tenía acceso a información confidencial sobre las operaciones de las agencias de inteligencia, filtraron información sobre las operaciones militares, espionaje y los métodos de vigilancia, poniendo en tela de juicio las actividades de espionaje y vigilancia de Estados por los temas de violación a los derechos humanos y violación a la soberanía de los Estados.

Una de las filtraciones que causo indignación en el mundo fueron los documentos y videos de las operaciones militares en la guerra de Iraq, las cuales fueron adquiridas por el soldado Bradley Manning cuando aún era analista militar, a pesar de haberse considerado culpable de los cargos de espionaje y ayuda al enemigo, fue exonerado por el gobierno de Barack Obama de sus cargos argumentando que solo quería generar un debate público; en comparación con el caso de Edward Snowden ex analista de la CIA y la NSA, filtró información clasificada sobre los programas de espionaje como es el programa PRISM que recaba información de cualquier persona tenga o no antecedentes penales por medio de

las empresas de comunicación, sin embargo en el caso de Edward Snowden se generó una persecución del gobierno de Estados Unidos más agresiva a comparación del caso del soldado Manning.

Un ejemplo claro de las vulnerabilidades a las que se encuentra las agencias de inteligencia es la filtración de información, como fue el caso Edward Snowden y el soldado Manning, quienes lograron entrar a información clasificada, dejando ver que a pesar de las medidas de seguridad que se implementan existen aún vulnerabilidades en los sistema de inteligencia de la NSA y la CIA por medio del personal autorizado que tiene acceso a bases de datos confidenciales.

Como ya se mencionó anteriormente, todos los sistemas informáticos dependen del factor humano y por ende, este es el eslabón débil de la cadena de seguridad, por lo que se debe de poner mayor énfasis en el capital humano para evitar vulnerabilidades que entorpezcan la operación de las medidas de seguridad, otro factor importante de destacar es la cooperación de empresas privadas con el gobierno para fortalecer las capacidades de ciberseguridad en el ciberespacio, se debe de poner atención a la información a la cual tienen acceso las empresas privadas como son los códigos de protección de seguridad en la infraestructura cibernética para evitar fines de lucro que ponga en riesgo la seguridad nacional estadounidense.

Bibliografía

- Aguilar Joyanes Luis, “Introducción Estado del arte de la ciberseguridad”, Ciberseguridad Retos y amenazas a la seguridad Nacional en el Ciberespacio, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, España, 2010, p. 29.
- Alfredo A. Reyes Krafft, “Ciberespacio y sociedad”, Seguridad y defensa en el ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p.11.
- Antoine Lefébure, El caso Snowden, así espía Estados Unidos al mundo, Primera edición, Ed.Le monde diplomatique, Argentina, 2014, p. 177.
- Aristizabal Velásquez David, Luces y sombras de las nuevas tendencias de la regulación de contenidos informáticos en los Estados Unidos de Norteamérica, Revista CES, No.1, Medellín Colombia, p.80.
- Arreola García Adolfo, Ciberespionaje: La puerta al mundo virtual de los Estados e Individuos: una revisión de los programas de espionaje digital de los Estados Unidos, primera edición, Ed. Siglo XXI, México, 2015, p. 119.
- Artiles Ganzúa Néstor, “La situación de la ciberseguridad en el ámbito internacional y en la Otan”, ciberseguridad retos y amenazas a la seguridad nacional en el ciberespacio, Ed. Ministerio de defensa, Instituto Español de Estudios Estratégicos, España, 2010, p. 175.
- Calderón Canales Rebeca, Chiquillo Benítez Vilma, Rodríguez Peña Yasmin, Espionaje como instrumento de la política exterior de estados Unidos de América y las consecuencias en sus relaciones exteriores. Casos: República Federal de Alemania y República Federativa de Brasil, Ed. Universidad de el Salvador, El Salvador, 2015, p. 126.
- Calvo Jordi, Escoda Anna, Blanco Carlos, Serra Gabriela, Drones militares, la Guerra de videojuegos con victimas reales, Ed. Centre DeLàs D´Estudis Per La Pau, Barcelona, 2014, p. 8.
- Canay Pazos J. Raúl, El uso de entornos virtuales de aprendizaje en las universidades presenciales: Un análisis empírico sobre la experiencia del

campus virtual de la USC, Ed. Universidad de Santiago de Compostela, España, 2008, p.49.

- Caro Bejarano María José, Alcance y ámbito de la seguridad en el ciberespacio, en ciberseguridad. Retos y Amenazas a la seguridad nacional del ciberespacio,Ed. Ministerio de defensa, Instituto Español de Estudios Estratégicos, España, 2011, p. 55.
- Castaño Sencianes Albert, Periodismo de Filtración: El caso PRISM, Ed. Universitat Autònoma de Barcelona, España, 2014, p. 33.
- De Tomas Morales Susana, Retos del Derecho ante las Nuevas Amenazas, Ed. Dykenson S.L., España, 2015, p.143.
- Del Pino Acurio Santiago, Delitos informáticos: Generalidades, Ed. PUCE, Ecuador, 2013, p. 27.
- Diáz del Rio Duran José Juan, “La ciberseguridad en el ámbito militar”, Ciberseguridad retos y amenazas a la seguridad nacional en el ciberespacio, Ed. Ministerio de defensa, Instituto español de Estudios Estrategicos, España, 2010, p. 235.
- E. Reyes Giovanni, Teoría de la globalización: Bases fundamentales, Revista de la Facultad de ciencias Económicas y administrativas, Vol. II, No.1, Universidad de Nariño, Colombia, 2001, p. 46.
- Ezquer Matallana Fermín, Castellano D. José Manuel, Big to small: Las estrategias de las grandes corporaciones al alcance de la mediana empresa, Ed. Caixagalicia, España, 2010, p.18.
- Gambrill Mónica, La globalización y sus manifestaciones en América del Norte, Ed. Centro de Investigaciones sobre América del Norte, México, 2002, p.29.
- Garay Saldaña Juan Daniel, La Política de Seguridad en Norteamérica post 11-S: del Homeland Security a WikiLeaks, Tesis de Maestría en estudios México- Estados Unidos, Universidad Autónoma de México, Facultad de Estudios Superiores Acatlán, México, D.F., 2014, p. 173.

- García Hernández Arturo, “Una visión del poder económico en la Ciberseguridad”, Seguridad y Defensa en el Ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p.40.
- Ghernaouti Solange, Cyberpower, crime, conflicto and security in cyberespace, Ed. CRC Press, EE.UU, 2006, p. 335.
- Gleen Greenwald, Snowden. Sin un lugar donde esconderse, Ed. Metropolitan Books, Barcelona España, 2014, p.124.
- Gragido Will, Piric John, Cybercrime and Espionage and Analysis of subversive Multivector Threats, Ed. Elsevier, Amsterdam, 2011, p. 191.
- Gregory J. Rattray, Strategic Warefare in Cyberspace. Defining the problem, Ed. MIT Press, Washington D.C., 2009, pp.26-27.
- Gutiérrez del Moral Leonardo, Curso de Ciberseguridad y hacking ético, Ed. Punto Rojo Libros, S.L., Sevilla España, 2014. p. 15.
- Gutiérrez Diego Alonso, “La cultura de la Ciberseguridad. El ciberespacio y la sustentabilidad para conseguir los objetivos del desarrollo del milenio”, Seguridad y Defensa en el Ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p.166.
- Hanzhang Tao, Sabiduría aplicable a los negocios, Sun Tzu- El arte de la guerra, Ed. Profit, España, 2011, p. 81.
- Held D. y McGrew A., Globalización/Antiglobalización. Sobre la reconstrucción del orden mundial, Ed. Paidós, Barcelona, 2003, p.13.
- Hernández-Vela Salgado Edmundo, Diccionario de política Internacional, Tomo ll, Letras J-Z, sexta edición, Editorial Porrúa, México, 2002, p.935.
- Herrera Hermosillo Juan Carlos, Breve Historia del espionaje, Ed.Nowlitus, Madrid España, 2012, p. 25.
- Ianni Octavio, La era del globalismo, Ed. Siglo Veintiuno Editores, s.a. de c.v. , España, 1999, p.27.
- Jeannetti Dávila Elena, “Ciberdefensa Activa: Mejorando la Ciberseguridad”, Seguridad y Defensa en el Ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p. 193.

- Julián Assange, Jacob Apelbaum, Andy Muller-Maguhn y Jeremie Zimmermann, Cypherpunks: La libertad y el futuro de internet, Ed. Deusto, España, 2013, p.7.
- K. Kostopoulos George, Cyberspace and Cybersecurity, Ed. CRC Press Taylor Francis Group editor, United States, 2013, p.159.
- Kendall, Willmoore, The function of intelligence, World politics, vol.1, n°4, Ed. Cambridge University Press, England, 2011, p. 552.
- Luján Mora Sergio, Programación de aplicaciones web: historia, principios básicos y clientes web, Ed. Club Universitario, España, 2002, p.53.
- Maroto, Juan Puime. El ciberespionaje y la ciberseguridad, En La violencia del siglo XXI. Nuevas dimensiones de la guerra, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, España, 2009, p. 50.
- Medina Manel, Molist Mercé, Cibercrimen ¡Protégete del Bit-Bang!, Los ataques en el ciberespacio a: Tu ordenados, tu móvil, tu empresa, Ed. Tibidabo, Barcelona, 2015, p.88.
- Méndez de la Brema Dresna Emma, Biopoder como elemento de seguridad Nacional, Ed. Universidad de las Américas Puebla, Escuela de Ciencias Sociales, Artes y Humanidades, México, 2006, p. 32.
- Miller Jones, R. Edward, WikiLeaks, Removing the Top secret seal, Ed.Fastbookpublishing, Estados Unidos, 2010.
- Ortega Monjaraz Víctor, Nueva Inteligencia y Ciberseguridad, Ed. Secretaría de Marina, Revista del Centro de Estudios Superiores Navales, Volumen 37, México, 1 de Marzo de 2016, p. 64.
- Paloma Parra Luis Orlando, Delitos Informáticos (en el ciberespacio), Ed. Ediciones Jurídicas Andrés Morales, Bogotá, Colombia; Ciudad de Panamá, Panamá, 2012, p. 65.
- R. Linosay John, Cheung Ming Tai, S. ReveronDerek, China and cybersecurity espionaje, strategy, and politics in the Digital Domain, Ed.Oxfort University, England , 2015, p.127.
- Restrepo Vélez, Juan Camilo., La Globalización en las Relaciones Internacionales: Actores internacionales y sistema internacional

contemporáneo, Facultad de Derecho y Ciencias Políticas, Medellín Colombia, 2013, p.635.

- Romero Candau Javier, Política y violencia: Comprensión teórica y desarrollo en la acción colectiva, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, España, 2014, p.275.
- S. Gal Cecilia, B. Kantor Paul, Brancha Shapira, Security Informatics and Terrorism: Patrolling the web, Ed. IOS Press, Amsterdam, 2008, p.11.
- Sánchez de Rojas Díaz Emilio, Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario, Ed. Ministerio de Defensa, Escuela de Altos Estudios de la Defensa, España, 2013, p. 295.
- Sánchez Hernández Carlos, Las Nuevas Doctrinas Militares, El espionaje Aéreo y la Tecnología en la Guerra (2001-2008), De Hanoi a Bagdad, Vol. 19, No.3, Revista Critica de Ciencias Sociales y Jurídicas, Universidad Complutense de Madrid, España 2008, p.14.
- Segura Serrano Antonio, Gordo García Fernando, Ciberseguridad global, oportunidades y compromisos en el uso del ciberespacio, Ed. Universidad de Granada, España, 2013, p. 22.
- Seguridad y Defensa en el Ciberespacio, primera Edición, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p.197.
- Vázquez Medina Rubén, “Buenas prácticas para reducir los impactos de amenazas y riesgos de la información en el ciberespacio”, Seguridad y Defensa en el Ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p. 258.
- Vizarreta Gonzales Emilio, Nueva Inteligencia y Ciberseguridad, Ed. Secretaría de Marina, Revista del Centro de Estudios Superiores Navales, Volumen 37, México, 1 de Marzo de 2016, p. 54.
- Woodward, John D., Super Bowl Surveillance. Facing up to Biometrics, Ed. RAND: arrollo center, Santa Mónica, Estados Unidos, 2001, p.4.
- Yañez María Rebeca, S. Villatoro Pablo, Las nuevas tecnologías de la información y de la comunicación (TIC) y l institucionalidad social. Hacia

una gestión basada en el conocimiento, Ed. CEPAL, Santiago de Chile, 2005, p.7.

- Zacarías López Daniela, Wikileaks y los efectos de la divulgación de información confidencial: análisis de las filtraciones de Estados Unidos, Colegio de San Luis, 2012, p. 73.

Hemerografía

- Aristizabal Velásquez David, *Luces y sombras de las nuevas tendencias de la regulación de contenidos informáticos en los Estados Unidos de Norteamérica, Revista CES,* No.1, p.80.
- Canay Pazos J. Raúl, *El uso de entornos virtuales de aprendizaje en las universidades presenciales: Un análisis empírico sobre la experiencia del campus virtual de la USC,* Universidad de Santiago de Compostela, España, 2008.
- E. Reyes Giovanni, *Teoría de la globalización: Bases fundamentales,* Revista de la Facultad de ciencias Económicas y administrativas, Vol. II, No.1, Universidad de Nariño, 2001, p. 46.
- Gambrill Mónica, La globalización y sus manifestaciones en América del Norte, México, Ed. Centro de Investigaciones sobre América del Norte México, 2002.
- Gregory J. Rattray, *Strategic Warefare in Cyberspace. Defining the problema, Franklin D. Kramer, Stuart H. Starr y Larry K. Wentz, Washington D.C., 2009.*
- Guazmayán R. Carlos, *Internet y la Investigación científica, El uso de los medios y las nuevas tecnologías en la educación,* Alma Mater, Colombia, 2004.
- Kendall, Willmoore, *The function of intelligence, World politics,* vol.1, n°4, Cambridge University Press, England, 1 de Julio 2011.
- Maroto, Juan Puime. *El ciberespionaje y la ciberseguridad, En La violencia del siglo XXI. Nuevas dimensiones de la guerra*, Instituto Español de Estudios Estratégicos, 2009.
- Ponce de León y Marcos Enrique Carlos*, "Las Redes sociales en el ciberespacio como herramienta de la política",* seguridad y defensa del

ciberespacio, Ed. Secretaria de marina, Centro de Estudios Superiores Navales, México, 2015, p. 213.

- Sánchez Hernández Carlos, *Las Nuevas Doctrinas Militares, El espionaje Aéreo y la Tecnología en la Guerra (2001-2008), De Hanoi a Bagdad, Vol. 19, No.3, Revista Critica de Ciencias Sociales y Jurídicas, Universidad Complutense de Madrid, España 2008.*
- Vizarreta Gonzales Emilio, *Nueva Inteligencia y Ciberseguridad*, Revista del Centro de Estudios Superiores Navales, Volumen 37, 1 de Marzo de 2016, p. 64.
- Yañez María Rebeca, S. Villatoro Pablo, *Las nuevas tecnologías de la información y de la comunicación (TIC) y l institucionalidad social. Hacia una gestión basada en el conocimiento, CEPAL, Santiago de Chile, 2005.*

Mesografía

- About Wikileaks, 2010, disponible en línea: http://wikileaks.org/about.html, Fecha de consulta: 11 de Mayo de 2017.
- About WikiLeaks, 2010, disponible en línea: https://wikileaks.org/About.html, Fecha de consulta: 17 de Noviembre de 2017.
- Aranda, T. Vicente, Historia y evolución de Internet. 2004, Manual formativo de ACTA, disponible en línea: https://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf, España 2004, p.2, Fecha de consulta 10 de Abril de 2017.
- Associated Press, Obama Asks For Review Of Online Security, 10 de Febrero de 2009, The Washington Post, disponible en línea en: http: //www.washingtonpost.com, Fecha de consulta: 17 de marzo de 2017.
- Barack Obama, Remarks by the presiden ton securing our nation´s cyber infraestructure", Washington, D.C., 29 de Mayo de 2009, disponible en línea: http://www.whitehouse.gov/the-press-office/remarks-president-

securing-our-nations-cyber-infraestructure, Fecha de consulta: 08 de Mayo de 2017.

- BBC Mundo, Crece el escándalo de Espionaje en EE.UU, 7 de jJnio de 2013, disponible en línea:http://www.bbc.com/mundo/noticias/2013/06/130606_eeuu_verizon_internet_metadata_vigilancia_cch, Fecha de consulta: 20 de Junio de 2017.
- BBC Mundo, El nuevo campo de entrenamiento para las ciberguerras,18 de Junio de 2011, disponible en línea: http://www.bbc.com/mundo/noticias/2011/06/110617_eeuu_ejercito_ciberataque_ciberguerra_internet_jg.shtml, Fecha de consulta: 10 de Junio de 2017.
- BBC Mundo, La poderosa herramienta de EE.UU. para vigilarlo todo en internet, 1 de Agosto de 2013, disponible en línea: http://www.bbc.com/mundo/noticias/2013/08/130801_tecnologia_snowden_nsa_xkeyscore_dp,Fecha de consulta: 24 de Julio de 2017.
- BBC Mundo, Se acabó “Twittear” para los “Marines”, 5 de Agosto de 2009, disponible en línea: http://www.bbc.com/mundo/cultura_sociedad/2009/08/090805, Fecha de consulta: 02 de Mayo de 2017.
- BBC, Ciberespacio: el nuevo ámbito de la guarra para el pentágono, 27 de julio de 2011, disponible en línea: http://www.bbc.com/mundo/movil/noticias/2011/07/110722_eeuu_pentagono_ciberespacio_estrategia_wbm.shtml, Fecha de consulta: 20 de Mayo de 2017.
- BBC, México condena supuesto espionaje de EE.UU. a Calderón, 21 de Octubre de 2013, disponible en línea: http://www.bbc.com/mundo/ultimas_noticias/2013/10/131020_ultnot_mexico_snowden_nsa_espionaje_cch, Fecha de consulta: 21 de Junio de 2017.
- Bejarano G. Pablo, El mercado gris donde la CIA compra armas de ciberespionaje, el país, 14 de Marzo de 2017, disponible en línea:

http://tecnologia.elpais.com/tecnologia/2017/03/13/actualidad/1489404727_131065.html,Fecha de consulta: 12 de Junio de 2017.

- Benedicto Solsona Miguel A., El discurso del Estado de la Unión: Obama se niega a condescender, Instituto Español de estudios Estratégicos, 3 de Febrero 2015, disponible enlínea:http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO152015_DiscursoNacionUS_MABenedicto.pdf, Fecha de consulta: 12 de Septiembre de 2017.
- Benedicto Soslana A. Miguel, EEUU ante el reto de los ciberataques,Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 2013, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO372013_Ciberataques_BenedictoSolsona.pdf, Fecha de consulta: 30 de Mayo de 2017.
- Biography Bradley Manning, 2013, disponible en línea: http://.org/stealing-secrets/ss-bradley-manning.pdf, Fecha de consulta: 28 de Agosto de 2017.
- Blanco Navarro José María, Hezbollah, el partido de Dios, 2015, Ed. Ministerio de Defensa, Grupo español de estudios Estratégicos, España, p.12, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_investig/2015/DIEEEINV012015_Hezbollahx_El_partido_de_Dios_JMBlanco.pdf, Fecha de consulta: 09 de Julio de 2017
- Btzsercas, Ciberseguridad y ciberespionaje en las relaciones internacionales, Diplomacy Data, disponible en línea: http://diplomacydata.com/cyber-security-awareness-in-public-diplomacy/, Fecha de consulta: 28 de Julio de 2017.
- Buendía José, La justicia americana sigue su lucha contra el ciberterrorismo, mCpromuycomputer, 28 de Junio de 2016, disponible en línea: http://www.muycomputerpro.com/2016/03/28/la-justicia-americana-sigue-su-lucha-contra-el-ciberterrorismo, Fecha de consulta: 31 de Julio de 2017.

- Carlini Agnese, ISIS: Una nueva amenaza en la era digital, Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 1 de Diciembre de 2017, p.5, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO1292015_ISIS_AmenazaEraDigital_AgneseCarlini.pdf, Fecha de consulta: 21 de Noviembre de 2017.
- Caro Bejarano J. María, Nuevo Concepto de Ciberdefensa de la OTAN, Ed. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 2011, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI092011ConceptoCiberdefensaOTAN.pdf,Fecha de consulta: 30 de Mayo de 2017.
- Chacón Vega Jehron, Seguridad informática: factor humano- principios, Revista digital En-Toas, disponible en línea: http://revistaentoas.com/seguridad-informatica-factor-humano-principios/, Fecha de consulta: 08 de Julio de 2017.
- Ciberdefensa-Ciberseguridad Riesgos y Amenazas, 2013, disponible en línea: http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf, Fecha de Consulta: 11 de Febrero de 2017.
- CNN, EE.UU. interceptó una amenaza terrorista de Al-qaeda para el 11-S, 9 de Septiembre de 2011, disponible en línea: https://cnnespanol.cnn.com/2011/09/09/ee-uu-confirma-una-amenaza-creible-de-atentado-para-el-11-s/, Fecha de consulta: 12 de Junio de 2017.
- Coleman G. Kevin, Private sector- Military Collaboration Vital to Confront Cyber Threats ,19 de Marzo de 2010, disponible en línea: http://www.defensetech.org/1010/04/19/private-sector-military-colaboration-vital-to-confront-cyber-threats/, Fecha de consulta: 09 de Mayo de 2017.
- Cruz Soto Luis Antonio, Hacia un concepto de globalización, Revista Contaduría y Administración, No. 195, Ed. Facultad de Contaduría y Administración, UNAM, México, Octubre diciembre 1999, p. 37, disponible en línea: http://www.ejournal.unam.mx/rca/195/RCA19504.pdf, Fecha de consulta: 21 de Noviembre de 2017.

- Cyber, Nacional Security Agency, 2016, disponible en línea: http://www.nsa.gov/what-we-do/cyber/, Fecha de consulta: 1 de Febrero de 2017.
- Directrices de la OCDE para la seguridad de sistemas y redes de información: Hacía una cultura de seguridad, disponible en línea: https://www.oecd.org/sti/ieconomy/34912912.pdf, Fecha de consulta: 18 de Abril de 2017.
- El Mundo, Rusia no sabe qué hacer con Edward Snowden, 11 de Febrero de 2017, disponibleenlínea:http://www.google.com.mx/amp/s/.amp.elmundo.es/.internacional/.2017/02/11/589f345ce2704e156a8b467c.html, Fecha de consulta: 26 de Noviembre de 2017.
- El país, Espías con vistas al Reichstag, 28 de Octubre de 2013, disponible en línea: http://internacional.elpais.com/internacional/2013/10/28/actualidad/1382993121_383527.html, Fecha de consulta: 20 de Junio de 2017.
- El país, Los peores ataques cibernéticos en Estados Unidos, 5 de junio 2015, disponible en línea:http://internacional.elpais.com/internacional/2015/06/05/actualidad/1433461961_205806.html, Fecha de consulta: 10 de Junio de 2017.
- El país, El soldado Manning, condenado a 35 años por las filtraciones a Wikileaks, 22 de Agosto de 2013, disponible en línea: https://elpais.com/internacional/2013/08/21/actualidad/1377090640_718161.html, Fecha de consulta: 28 de Agosto de 2017.
- El país, Obama conmuta la pena de la soldado Chelsea Manning, 18 de Enero de 2017, disponible en línea: https://elpais.com/internacional/2017/01/17/estados_unidos/1484689399_418245. html, Fecha de consulta: 17 de Noviembre de 2017.
- El país, Preguntas y respuestas sobre los papeles del Departamento de Estado, 28 de Noviembre de 2010, disponible en línea:

http://internacional.elpais.com/internacional/2010/11/28/actualidad/1290898811_850215.html, Fecha de consulta: 17 de Noviembre de 2017.

- Fayerwayer, Texto cifrado en el logo de USCYBERCOM, 2016, disponible en línea: https://www.fayerwayer.com/2010/07/codigo-cifrado-en-el-logo-del-uscybercom/, Fecha de consulta: 31 de Mayo de 2017.
- FORBES, Ninguna tecnológica se salva de la inteligencia de EU, 10 de Junio de 2013, disponible en línea: https://www.forbes.com.mx/pocas-opciones-para-que-firmas-desafien-a-inteligencia-de-eu/, Fecha de consulta: 20 de Junio de 2017.
- Forjón Chamorro Enrique, ¿Diplomacia para luchar contra el ciberespionaje?, Ed. Real Instituto el cano Royal Institute, 02 de Octubre de 2015, disponible en línea: http://www.blog.rielcano.org/diplomacia-para-luchar-contra-el ciberespionaje/, Fecha de consulta: 19 de Julio de 2017.
- Gómez Aguirre Gonzalo, WikiLeaks revela que EE usaba a sus embajadores para espiar en la ONU, 28 de noviembre de 2010, disponible en línea: http://www.elmundo.es/america/2010/11/28/estados_unidos/1290951375.html, Fecha de consulta: 17 de Noviembre de 2017.
- González Veiguela Lino, Los ciberataques (conocidos) más importantes, Ed. esglobal, 2 de Julio de 2013, disponible en línea: https://www.esglobal.org/la-lista-los-ciberataques-conocidos-mas-importantes/, Fecha de consulta: 11 de Junio de 2017.
- Granados Omar, CISPA, un nuevo intento por controlar internet, animal político, 10 de Abril de 2012, disponible en línea: http://www.animalpolitico.com/2012/04/cispa-un-nuevo-intento-de-controlar-internet/, Fecha de consulta: 03 de Julio de 2017.
- Gregory Anthony, El Estado de vigilancia bipartidista, 11 de Junio de 2008, disponible en línea: http://www.elindependent.org/articulos/article.asp?id=2263, Fecha de consulta: 11 de Junio de 2017.

- Hernández Lorente Adolfo, Vigilados por defecto, Ed. Ministerio de Defensa, 4 de Abril de 2014, p.5, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2014porDefecto_Hdez-Colom-Fojon.pdf, Fecha de consulta: 18 de Julio de 2017.
- Herrera Yopo Boris, La nueva estrategia de Seguridad Nacional de Estados Unidos: sus implicancias regionales, Academia Nacional de Estudios Políticos y Estratégicos, Boletín de investigación No.6, Diciembre de 2013, disponible en línea: https://anepe.cl/wp-content/uploads/boris_yopo_bolet%C3%ADnN%C2%BA-6.pdf, Fecha de consulta: 10 de Julio de 2017.
- Hoja de Datos: Plan Acción Nacional de Ciberseguridad, The White House, Office of the Press secretary, 09 de Febrero 2016, disponible en línea: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheetcybersecurity-national-action-plan, Fecha de consulta: 19 de Junio de 2017.
- Homland Security, Security National Network,United States, 16 de Marzo 2017, disponible en línea: https://www.dhs.gov/topic/cybersecurity, Fecha de consulta: 18 de Mayo de 2017.
- Iniciativa Nacional para la Educación de la Ciberseguridad, 20 de Enero 2016, disponible en línea: https: //www.nist.gov/itl/applied-cybersecurity/nice/about, Fecha de consulta: 02 de Mayo de 2017.
- J. Gebhardt J. Bruce, Ciberterrorismo: Nefasta evolución, 07 de Febrero de 2014, disponible en línea: https://es.scribd.com/document/205282600/ciberterrorismo-pdf, Fecha de consulta: 07 de Julio de 2017.
- Jarabo Valdivieso, El espionaje-pasado y presente, 2015, disponible en línea: https://apavaldeluz.files.wordpress.com/, Fecha de consulta: 06 de Agosto de 2017.
- La agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EEUU, Real Instituto Elcano, 11 de Noviembre de 2013, disponible en línea:

http://www.realinstitutoelcano.org/wps/wcm/connect/7366288041c9aefda642ae709b5c321/ARI41-2013, Fecha de consulta: 05 de Agosto de 2017.

- La Jornada, La NSA espiaba a la Secretaría de Seguridad Pública, 30 de Diciembre de 2013, disponible en línea: http://wikileaks.jornada.com.mx/notas/la-nsa-espiaba-a-la-secretaría-de-seguridad-publica, Fecha de consulta: 21 de Junio de2017.
- La nación, Un pen drive provoco el mayor ataque a computadoras militares de EE.UU, 25 de agosto de 2010, disponible en línea: http://www.lanacion.com.ar/1297971-un-pen-drive-provoco-el-mayor-ataque-a-computadoras-militares-de-eeuu, Fecha de consulta: 20 de Mayo de 2017.
- Loreto Vicente, ¿Movimientos sociales en la red? Los hacktivistas, Ed. El cotidiano, vol. 20, núm. 126, julio-agosto, México, 2004, p. 3, disponible en línea: http://www.redalyc.org/articulo.oa?idp=1&id=32512615&cid=5255, Fecha de consulta: 13 de Noviembre de 2017.
- Machín N. Gazapo M., La Ciberseguridad como factor crítico en la Seguridad de la Unión Europea, revista UNISCI Norteamericana, España, 2016, p.59, disponible en línea: http://revistas.ucm.es/index.php/RUNI/article/view/53786/49258, Fecha de consulta: 15 de noviembre de 2017.

- Márquez William, Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU., 2 de Julio de 2013, disponible en línea: http://www.bbc.com/mundo/noticias/2013/07/130702_eeuu_snowden_revelaciones_espionaje_wbm, Fecha de consulta: 07 de Agosto de 2017.
- Medero Sánchez Gema, El ciberespionaje, Derecom, No. 13, Marzo-Mayo 2013, Ed. Nueva Época, España, p. 117, disponible en línea: http://s3.amazonaws.com/academia.edu.documents/34001413/DialnetElCiberespionaje4330467.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1499300065&Signature=TGvZW1RKw%2BJUMQXbQyLKGYmOEWQ%3D&responsecontentdisposition=inline%3B%20filename%3DEl_ciberespionaje.pdf, Fecha de consulta: 05 de Julio de 2017.

- Mell Peter, Grance Tim, *Effectively and Securely Using the Cloud Computing Paradigm*, Octubre 2009, disponible en línea: http: //crsc.nist.gov/groups/SN/cloud-computing/cloud-computing-v25.ppt., Fecha de consulta: 08 de Mayo de 2017.
- Molina Javier, Polémica en México por el espionaje de Estados Unidos, El país, 04 de Septiembre de 2013, disponible en línea: http://internacional.elpais.com/internacional/2013/09/05/actualidad/1378341578_816433.html, Fecha de consulta: 21 de Junio de 2017.
- National intelligence strategy.White House, 2010, disponible en línea: http: //www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf., Fecha de consulta: 20 de Abril de 2017.
- National Security Agency, Mission and Strategy, Mayo 2016, disponible el línea: https://www.nsa.gov/,Fecha de consulta: 8 de Mayo de 2017.
- Nebreda Rodrigo Iván, El origen de Internet. El camino hacia las redes, Ed. DIATEL, 2013, disponible en línea: http://oa.upm.es/22577/1/PFC_IVAN_NEBREDA_RODRIGO.pdf, Fecha de consulta: 10 de Abril de 2017.
- Nuevo Proyecto de Ley sobre Ciberseguridad en Estados Unidos, 22 de Febrero de 2012, disponible en línea: http://www.telam.com.ar/notas/201202/13568-nuevo-proyecto-de-ley-sobre-ciberseguridad-en-estados-unidos.html, Fecha de consulta: 30 de Mayo de 2017.
- Organización de Estados Unidos Americanos (OEA), Seguridad cibernética, 2004, disponible en línea: https: //www.sites.oas.org/cyber/Es/Paginas/default.aspx, Fecha de consulta: 14 de Abril de 2017.
- Orta Martínez Raymond, Ciberterrorismo, conferencia dictada en la Facultad de Ciencias Jurídicas y Políticas de la Universidad de Carabobo, disponible en línea:

http://servicio.bc.uc.edu.ve/derecho/revista/relcrim21/art06.pdf, Fecha de consulta: 08 de Julio de 2017.

- Poitras Laura, Citizenfour, 10 de octubre de 2014, disponible en línea: https://www.youtube.com/watch?v=4EgTXEn15ls&t=328s, Fecha de consulta: 19 de noviembre de 2017.
- Ponce de León y Marcos Enrique Carlos, "Las redes sociales en el ciberespacio como herramienta de la política", seguridad y defensa del ciberespacio, Ed. Secretaría de Marina, Centro de Estudios Superiores Navales, México, 2015, p. 213.
- Proponen un sistema de vigilancia en Internet, Nuestra América, 23 de Diciembre de 2002, disponible en línea: http://nuestramerica.info/article/proponen-un-sistema-de-vigilancia-en-internet/, Fecha de consulta: 16 de Julio de 2017.
- Real Academia Española (RAE), Diccionario de la lengua Española, Disponible en línea: http://www.rae.es/, Fecha de consulta: 09 de Agosto de 2017.
- Rosas González María Cristina, La guerra de los Drones, Etcétera, 18 de Septiembre de 2013, disponible en línea: http://www.etcetera.com.mx/articulo.php?articulo=21586, Fecha de consulta: 09 de Mayo de 2017.
- Saiz Eva, La NSA usó aplicaciones como angry Birds o Google Maps para obtener datos, El país, 2014, disponible en línea: http://internacional.elpais.com/internacional/2014/01/27/actualidad/1390854460_566211.html,Fecha de consulta: 08 de junio de 2017.
- Salvador Carrasco de Luis, Internet, Filtraciones y Wikileaks, Diciembre 2010, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2010/DIEEEO25_2010Wikileaks.pdf,Fecha de consulta: 08 de Mayo de 2017.
- Sánchez Madero Gema, Los Estados y la Ciberguerra, Ed.Universidad complutense de Madrid, 2010, p. 69, disponible en línea: dialnet.unirioja.es, Fecha de consulta: 14 de Julio de 2017.

- Santiago de Freda Manuel, Wikileaks, periodismo y transparencia: los filtros de las filtraciones, DERECOM, 2010, disponible en línea: www.derecom.com/blog/item/download/83_01316c1003f735e67fd8b9-a202710328, Fecha de consulta: 14 de Mayo de 2017.
- Shane Scott, Lehren W. Andrew, Leaked Cables Offer Raw Look at U.S. Diplomacy, New York Times, 28 de Noviembre de 2010, disponible en línea: http://www.nytimes.com/2010/11/29/world/29cables.html?_r=1&hp,&pagewanted=1&,Fecha de consulta: 11 de Mayo de 2017.
- Stefano Pezzino, TOR (The Onion Router), Ed. Universidad Católica "Nuestra Señora de la Asunción", Facultad de Ciencias y Tecnología, Uruguay, 2014, p.3, Disponible en línea: http://www.uca.edu.py, Fecha de consulta: 09 de agosto de 2017.
- The Comprehensive National Cybersecurity Iniciative, White House, 2010, disponible en línea: http://www.whitehouse.gov/Issues/foreign-policy/cybersecurity/national-Iniciative, Fecha de consulta: 31 de Mayo de 2017.
- The Guardian, GCHQ utiliza cables de fibra óptica para obtener acceso secreto a las comunicaciones del mundo, 21 de Junio de 2013, disponible en línea: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, Fecha de consulta: 19 de Noviembre de 2017.
- The Guardian, Llamada de Ángela Merkel a Obama: ¿Estás molestando a mi teléfono móvil?, 24 de octubre de 2013, disponible en línea: https://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german, Fecha de consulta: 20 de Noviembre de 2017.
- The Guardian, Wikileaks lucha por seguir en la red tras la retirada de su dominio por parte de una compañía americana, 2010, disponible en línea: http://www.guardian.co.uk/media/blog/2010/dec/o3/ wikileaksknocked-off-net-dns-eveydns, Fecha de consulta: 14 de Mayo de 2017.
- The Washington post, Google, China *Cyberattack part of vast espionaje campaign experts say*, 14 de enero de 2010, disponible en línea:

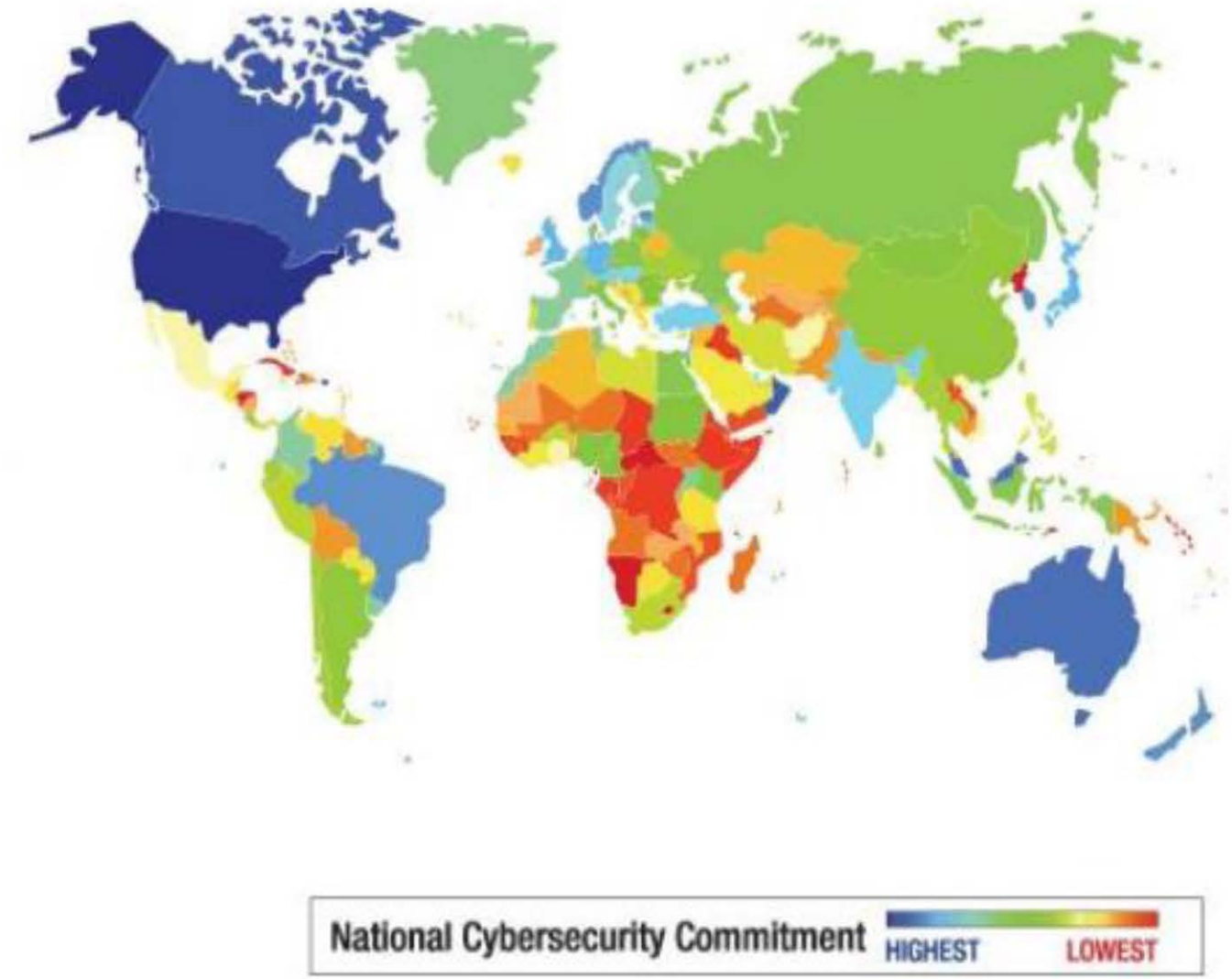
http://www.washingtonpost.com/wpdyn/content/article/2010/01/13/AR2010011300359.html, Fecha de consulta: 20 de Mayo de 2017.

- The White House, Remarcks by President Obama in a Press Conference at the G20, 06 de Septiembre de 2013, disponible en línea: https://obamawhitehouse.archives.gov/the-press-office/2013/09/06/remarks-president-obama-press-conference-g20, Fecha de consulta: 09 de Agosto de 2017.
- U.S. *Strategic Command, U.S. Cyber Command* (USCYBERCOM), 30 de Septiembre 2016, disponible en línea: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/, Fecha de consulta: 01 de Junio de 2017.
- Urueña Centeno J. Francisco, Ciberataques, la mayor amenaza actual, Ed. Instituto Español de Estudios Estratégicos, 2015, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09/2015_AmenazaCiberataques_Fco.Urueña.pdf, Fecha de consulta: 12 de Febrero de 2017.
- Varonas Nico, Top secret: La tecnología con la que espía la NSA, NEOTEO, 6 de Enero de 2014, disponible en línea: http://www.neoteo.com/top-secret-la-tecnologia-con-la-que-espia-la-nsa/, Fecha de consulta: 03 de Agosto de 2017.
- Villamizar Lamus Fernando, Drones: ¿Hacia una guerra sin regulación jurídica internacional, Revista de Relaciones exteriores, Estrategia y seguridad vol. 10, núm.2, Ed. Universidad Militar Nueva Granada, 2015, disponible en línea: http://www.redalyc.org, Fecha de consulta: 05 de Junio de 2017.
- Villanueva López D. Christan, La red Echelon, Ed.Política de defensa y Fuerzas armadas, Revista digital de armamento, 28 de Agosto de 2016, disponible en línea: http://www.ejercitos.org/2016/08/23/la-red-echelon/, Fecha de consulta: 29 de Julio de 2017.

- WikiLeaks, *Afghan War Diary*, 25 de julio de 2010, disponible en línea: https://wikileaks.org/afg/, Fecha de consulta: 17 de Noviembre de 2017.
- Wikileaks, ¿Qué es Wikileaks?, Noviembre 2015, disponible en línea: https://wikileaks.org/What-is-Wikileaks.html, Fecha de consulta: 08 de Mayo de 2017.
- Wood Teresa, Los 20 ciberataques perversos del siglo XXI, 13 de septiembre de 2015, Mit Technologies Review, disponible en línea: https://www.technologyreview.es/s/7413/los-20-ciberataques-mas-perversos-del-siglo-xxi, Fecha de consulta: 10 de Junio de 2017.
- Zazo Lara, ¿Toma medidas mañana Obama sobre ciberterrorismo?, Computer Hoy, 12 de Febrero de 2013, disponible en línea: http://computerhoy.com/noticias/software/tomara-medidas-manana-obama-ciberterrorismo-3078, Fecha de consulta: 12 de Septiembre de 2017.
- Zucher Anthony, Del imperio Romano a la NSA: la Historia del espionaje Internacional, BBC, 2013, disponible en línea: http: //www.bbc.com, Fecha de consulta: 19 de Abril de 2017.

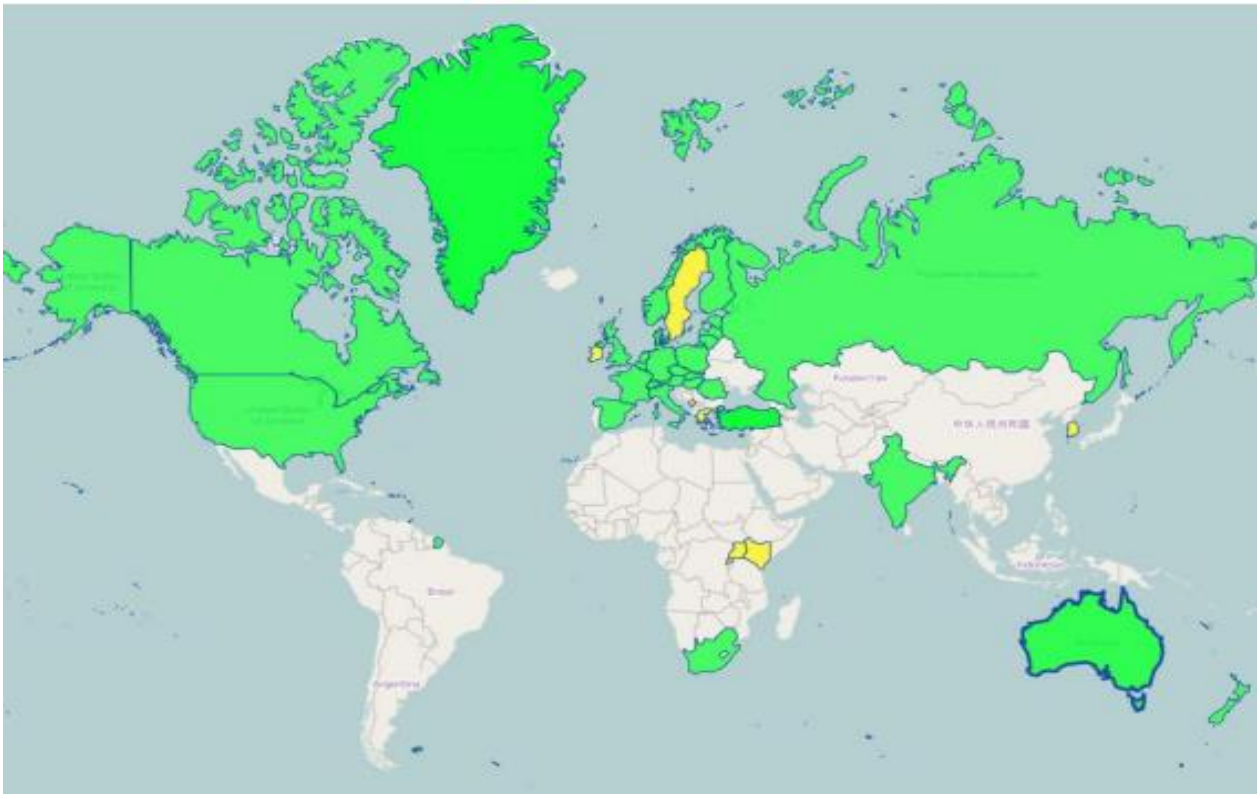
Anexos

Anexo 1 Compromiso de los Estados en tomar medidas de ciberseguridad.



Fuente: Ramírez Moran David, La visión internacional de la ciberseguridad, Instituto Español de Estudios Estratégicos, 2015,p.4, Disponible en línea: http://www.ieee.es/Galerias/fichero/docs_informativos/2015/DIEEEI02-2015_VisionInternacional_Ciberseguridad_DRM.pdf, fecha de consulta: 13 de Agosto de 2017.

Anexo 2 Países con estrategias sobre ciberseguridad.



Fuente: Ramírez Moran David, La visión internacional de la ciberseguridad, Instituto Español de Estudios Estratégicos, 2015,p.5, disponible en línea: http://www.ieee.es/Galerias/fichero/docs_informativos/2015/DIEEEI02-2015_VisionInternacional_ Ciberseguridad_DRM.pdf, Fecha de consulta: 13 de Agosto de 2017.

Anexo 3 National Cyber Alert Levels

National Cyber Risk Alert Levels			
Level	**Label**	**Description of Risk**	**Level of Response**
1	Severe	Highly disruptive levels of concequences are occurring or imminent.	Response functions are overwhelmed and top-level national executive authorities and engagements are essential.
2	Substantial	Observed or imminent degradation of critical functions with a moderate-to-significant level of consequences, posibly coupled with indicators of higher levels of concequences impending.	Surged posture becomes indefinitely necessary, rather than only temporarily. The Departament of Homeland Security secretary is engaged, and appropiate designation of authorities and activation of federal capabilities such as the Cyber UCG take place.
3	Elevated	Early indications of, or the potential for but no indicators of, moderate-to-severe levels of consequences.	Upward shift in precautionary measures occurs.Responding entities are capable of managing incidents/events whithin the parameters of normal, or slightly enhanced, operational posture.
4	Guarded	Baseline of risk acceptance.	Baseline operations, regular information sharing, exercise of processes and procedures, reporting, and mitigation strategy continue without undue disruption or resourse allocation.

Fuente: Chris Bronk, Cyber threat: the rise of information geopolitics in U.S. national security, Ed. Pranger, United States, 2016, p. 60.

Anexo 4 National Security Strategy 2010

Secure Cyberspace[223]

Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation. The very technologies that empower us to lead and create also empower those who would disrupt and destroy. They enable our military superiority, but our unclassified government networks are constantly probed by intruders. Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale. The Internet and e-commerce are keys to our economic competitiveness, but cyber criminals have cost companies and consumers hundreds of millions of dollars and valuable intellectual property.

The threats we face range from individual criminal hackers to organized criminal groups, from terrorist networks to advanced nation states. Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient. Our digital infrastructure, therefore, is a strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority. We will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by:

Investing in People and Technology: To advance that goal, we are working across the government and with the private sector to design more secure technology that gives us the ability to better protect and to improve the resilience of critical government and industry systems and networks. We will continue to invest in the cutting-edge research and development necessary for the innovation and discovery we need to meet these challenges. We have begun a comprehensive national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and to build a digital workforce for the 21st century.

Strengthening Partnerships: Neither government nor the private sector nor individual citizens can meet this challenge alone—we will expand the ways we work together. We will also strengthen our international partnerships on a range of issues, including the development of norms for acceptable conduct in cyberspace; laws concerning cybercrime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks. We will work with all the key players— including all levels of government and the private sector, nationally and internationally—to investigate cyber intrusion and to ensure an organized and unified response to future cyber incidents. Just as we do for natural disasters, we have to have plans and resources in place beforehand.

[223] National Security strategy 2010, disponible en línea: http://www.g8.army.mil/pdf/National_Security_Strategy_6Feb2015.pdf.

Anexo 5 Foreign Intelligence Surveillance Act of 1978 (FISA)

AUTHORIZATION FOR ELECTRONIC SURVEILLANCE FOR FOREIGN INTELLIGENCE PURPOSES

50 USC 1802.

SEC. 102. (a)(1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that—

(A) the electronic surveillance is solely directed at—

(i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 101(a) (1), (2), or (3); or

(ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 101(a) (1), (2), or (3);

(B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and

(C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 101(h); and

if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately.

Report to congressional committees.

(2) An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of section 108(a).

Report to congressional committees.

(3) The Attorney General shall immediately transmit under seal to the court established under section 103(a) a copy of his certification. Such certification shall be maintained under security measures established by the Chief Justice with the concurrence of the Attorney General, in consultation with the Director of Central Intelligence, and shall remain sealed unless—

(A) an application for a court order with respect to the surveillance is made under sections 101(h)(4) and 104; or

(B) the certification is necessary to determine the legality of the surveillance under section 106(f).

Fuente: Foreign Intelligence Surveillance Act of 1978 (FISA), disponible en línea: http://nsarchive2.gwu.edu//NSAEBB/NSAEBB436/docs/EBB-001.pdf