UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

La estrategia de ciberseguridad nacional de Estados Unidos para la protección de la Infraestructura Crítica: el caso del Sistema de Posicionamiento Global (GPS)".

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Licenciada en Relaciones Internacionales

P R E S E N T A:

Ana Karen Aguilar Zárate

DIRECTOR DE TESIS:

Dr. Jesús Gallegos Olvera

Investigación realizada gracias al Programa de Apoyo a Proyectos de Investigación e Innovación Tecnológica (PAPIIT) de la UNAM: IN308617 "Fundamentalismos y Orden Internacional".

Ciudad Universitaria, CDMX, Enero 2018.

Índice

Agradecimientos

A mis papás, Angelina y Vicente, este logro también es de ustedes. Ma, gracias por cuidarme, por los ánimos y regaños, por el amor incondicional, eres la mejor. Pa, gracias por cuidarme, por ser mi ejemplo a seguir, por confiar en mí y en mis logros, te admiro mucho. Gracias a los dos por ser mis pilares más importantes, por el tiempo invertido, por las oportunidades que me brindaron, por siempre apoyarme, sin ustedes esto no sería posible. Los amo.

A mi hermano, Huguín. Gracias por siempre estar al pendiente de mí, por esas partidas en el Wii para quitarme el estrés, por ser el mejor hermano que pude haber tenido y por soportar mi mal humor…a veces. Sabes cuánto te quiero.

A Axel, gracias por ser uno de mis pilares todo este tiempo. Gracias por apoyarme, por cuidarme, por tu infinita (infinita en verdad) paciencia, por tu ayuda incluso hasta con tareas durante la carrera *jajaja.* Por consentirme, por aguantar mi mal humor cuando estaba estresada, por hacer conmigo cada locura que se nos ocurría y por alentarme en aquellos momentos en los que ni yo misma creía en mí. Gracias por la confianza, por escuchar y por siempre recordarme de lo que era capaz. Sabes cuánto me inspiras. Gracias por estar. Gracias por tanto. ¡Te amo capitán!

A mis bebés, gracias por recorrer junto a mí este camino llamado universidad y ahora vida adulta *jajaja*. No podría escribir todos los momentos que vivimos juntas porque jamás acabaría, así que escribí uno con cada quien*,* gracias por todos y cada uno de ellos. No olvido que tuve que hacer una rifa para que ninguna se sintiera por el orden en que las voy a mencionar, están locas, y ¡las amoo!

Armin, bebé suave lomito, eres increíble, gracias por cuidarme cuando fue necesario y por esas fiestas inolvidables en las que siempre te voy a cuidar y a tener lista una bolsa (*you know what I mean*). Siempre voy a estar para ir por una cerveza y unos taquitos al pastor cuando lo necesites, para aconsejarte las mil horas y que termines haciendo exactamente lo contrario a lo que te dije *jajajaja.* Gracias por inventar los lunes de cochinadas y por las interminables partidas de *uno* en las que cuando ganabas, ya no era divertido.

Moni, gracias por ser siempre la persona más paciente del mundo y la más pacífica. Gracias por todas las aventuras juntas, por no morir conmigo en Cancún casi ahogadas en el mar mientras tratábamos de enseñar a Fernanda a nadar, por las risas, por los karaokes y por las mejores fiestas en tu casa *jajaja*. Gracias por ser la que nos calmaba cuando las demás peleábamos por culpa de nuestro lindo carácter. Estuvo padre ser *team* Estados Unidos por un tiempo.

Fer, mi chaira favorita, aunque ahora ya seas *team* capitalista, era divertido cuando hasta en las fiestas te ponías a defender la crisis sistémica *jajaja*. Gracias por ser siempre la más loca y por consiguiente, la que siempre decía que sí cuando se nos ocurría cualquier tontería. Gracias por cuidarme, por cantar conmigo las canciones de RBD en cada fiesta y por ser la culpable de nuestro primer viaje juntas, a Tequix, en donde terminamos hasta con serenata por parte de unos desconocidos *jajajaja.*

A la familia Mendoza Aguilar. Gracias porque cada uno de sus miembros aportó algo fundamental en mi vida, gracias por alentarme y por siempre confiar en mí. Tía Lupita, gracias por ofrecerme siempre el cariño de una segunda mamá cuando lo necesité. Vianey sabes cuánto te quiero, gracias por tu apoyo, cariño, por esas pláticas y por ofrecerme hospedaje siempre que me iba de fiesta *jajaja*. César, la *pinshesha* por fin se va a titular *jajaja* gracias por tanto bullying y por siempre sacarme una sonrisa. Eduardo, gracias por tanto, por ser un guía, un ejemplo a seguir y por siempre estar ahí para escuchar cuando me sentía perdida, te quiero mucho.

A Enrique, sabes que más que un primo eres un hermano, tú dices que menor pero todos sabemos que siempre has sido el mayor y mi guardaespaldas *jajaja.* Gracias por crecer conmigo y por todas esas anécdotas compartidas. Sigamos creando más…te quiero mucho.

A mi tío Yiyo. Gracias por ser como mi segundo papá, gracias por todas las enseñanzas, por ser parte fundamental en mi vida y por hacer de mi infancia la mejor. Gracias por esos partidos de béisbol de los Diablos Rojos, por ayudarme a hacer esas maquetas interminables en la primaria, por enseñarme a andar en bici, patines…todo lo que se me ocurría. Gracias por todo. Lo quiero mucho.

A mis abuelos, por ser parte de mi vida. A mi abuelita Lupita y a mi mamá Esperanza por hacer de mí una niña muy feliz. A mis dos ángeles en el cielo: Mi abuelito Rubén, ya no pudiste estar en mi graduación pero estoy segura que desde donde estás, lo viviste conmigo. A mi abuelito Jesús, te extraño como no te imaginas y hubiera dado lo que sea por tenerte conmigo más tiempo, tu *burruña* lo logró, gracias por siempre cuidarme, siempre te siento conmigo, estoy segura de que fuiste y eres el mejor abuelo del mundo.

A mi primo Gabriel, por enseñarme desde pequeña lo que era la UNAM y por sembrar esa semilla en mí de querer pertenecer a la mejor universidad del país. Orgullo azul y oro, siempre.

A mis amigos de la prepa. Jimeny, gracias por ser mi mejor amiga, por escuchar y por compartir muchos momentos conmigo. Sabes cuánto te *I love you jajaja* eres la persona más bulleable del mundo y te bulleo con amor, lo sabes. Kachito, gracias por ser mi mejor amigo, por estar y por compartir este amor por las Relaciones Internacionales. A Ily, mi stalker profesional, gracias por tu amistad, por esas risas y por esas repentinas comidas en tu facultad que me hacían extrañar un poquito menos la prepa. A Many, gracias por ser la abuela del grupo y por sacarme una sonrisa cada que nos vemos.

A mis amigos del cubículo, que se volvieron parte importante de mi vida estos últimos meses. Sharon, gracias por el apoyo y por los ánimos cada vez que lo necesitaba, por las pláticas y los momentos juntas, te has convertido en una gran amiga para mí y lo sabes. Pd. Estás bien loca. Sergio, Victoria, Tony, Melissa y Mich, gracias por la infinidad de risas y momentos que he compartido con ustedes, hicieron de todo esto más llevadero. Son unos amigos increíbles ¡los quiero!

A todas esas personitas que compartieron conmigo la carrera e hicieron que todo fuera más fácil…Celeste, gracias por los momentos juntas como aquella aventura en Cancún en la que nos reímos sin parar de las demás mientras estaban en el piso *jajajaja.* Mariel, gracias por estar, por cocinar en aquella cena y por hacer que el servicio social fuera mucho más divertido. Lety, Génesis, Lalo, gracias por todos esos momentos de los lunes, martes…el día que fuera…de cochinadas, en los que reíamos hasta que todo mundo en la cafetería se nos quedaba viendo con cara de asco *jajajaja.*

A mi asesor, el Dr. Jesús Gallegos, gracias por guiarme en todo este proceso y por el bullying incluido, sabe que tiene toda mi admiración y mi respeto. A la Dra. Kanety, por ser una de las mejores profesoras que tuve en la carrera y por tomarse el tiempo de leer mi tesis, la admiro. Al profesor Víctor Batta, gracias por su ayuda incondicional estos últimos meses y por su tiempo para leer este proyecto.

Al proyecto PAPIIT IN308617 “Fundamentalismos y Orden Internacional” y al Dr. José Luis Orozco quien lo dirige, gracias por darme la oportunidad de formar parte de su equipo y por la infinidad de cosas que se aprenden a su lado. A Dani, la coordinadora del proyecto, gracias por los consejos todo este tiempo y por la confianza, te admiro.

A Paul, mi perrito y mi fiel amigo, quien me acompañaba cada noche mientras intentaba terminar esta tesis.

Y por último pero no menos importante, a mi segunda casa, mi alma máter, la Universidad Nacional Autónoma de México, que desde el 2010 me abrió sus puertas y me permitió consolidar un sueño que tenía desde pequeña. Gracias por permitir que me formara en sus aulas. Es un orgullo pertenecer a esta gran universidad…

¡México, pumas, universidad!

Introducción

Hoy en día, gran parte de las naciones que conforman la sociedad internacional han integrado el uso de las Tecnologías de la Información y de la Comunicación en diversos aspectos. El ciberespacio y dentro de él, las redes (Internet por ejemplo), se han convertido en un elemento esencial del que dependen infraestructuras, transportes, el comercio, la economía, etc., de cada vez más países. Así, la red es una herramienta extraordinaria que ofrece una gama de nuevas oportunidades para las personas, las comunidades, las empresas y los gobiernos.

Sin embargo, el carácter crítico y la escasa regulación que hasta el momento caracterizan al ciberespacio, lo hace vulnerable a múltiples amenazas poniendo como temas prioritarios los aspectos ligados a la seguridad y a la defensa del mismo. La comprensión adecuada de las situaciones que surgen dentro del ciberespacio requiere un enfoque multidisciplinario, es decir, es necesario prestar atención a los aspectos políticos, económicos, técnicos, ideológicos, sociales y hasta militares que cada uno implica ya que el análisis desde un solo nivel no bastaría para su entendimiento.

La tecnología avanza a una velocidad imparable y la lucha por la superioridad tecnológica es una realidad, por lo que ésta, no se podrá alcanzar si no se cuenta con una infraestructura adecuada y una política nacional de defensa del ciberespacio que la acompañe. Aquellos países que no posean los elementos anteriores con un grado razonable de madurez, están abocados a depender de un tercero y por lo tanto, al consiguiente menoscabo de su soberanía nacional.

Sólo el desarrollo de una sociedad digital capaz de proteger los intereses de la nación en un mundo cada vez más dependiente de la tecnología, garantizará tanto su prosperidad como su seguridad; esto requiere de una visión estratégica y de la implementación de medidas urgentes capaces de resolver las necesidades actuales.

A medida que crece el número de usuarios del ciberespacio su complejidad también va en aumento. Las revelaciones de Edward Snowden afectaron significativamente la coyuntura de las relaciones internacionales teniendo como resultado que personas, empresas, organizaciones y Estados se preguntaran ¿qué tan seguro es el ciberespacio? Así, surge la ciberseguridad como un mecanismo de protección para toda la información que se almacena o transporta a través del ciberespacio.

La seguridad cibernética o ciberseguridad ya es un tema de gran relevancia en la agenda de política global. En los últimos años, países líderes en cuestiones cibernéticas han mantenido considerables debates y cambios en el nivel legislativo directamente relacionados con el ciberespacio. Estos procesos son un fenómeno complejo y nada convencional para la política tradicional y la geopolítica clásica debido a la rapidez con la que la tecnología avanza.

El ciberespacio es particularmente difícil de asegurar debido a una serie de factores: la capacidad de los actores maliciosos para operar desde cualquier parte del mundo, los vínculos entre el ciberespacio y los sistemas físicos, y la dificultad de reducir las vulnerabilidades y las consecuencias en las redes complejas. A la luz de los riesgos y posibles consecuencias de los eventos cibernéticos, el fortalecimiento de la seguridad y resistencia del ciberespacio se ha convertido en una importante misión de seguridad nacional[1].

En la actualidad los ataques cibernéticos se han vuelto algo común y continúan floreciendo debido a diversos motivos que van desde errores de software, configuraciones incorrectas de los sistemas operativos y aplicaciones y/o errores del usuario que hacen que los sistemas cibernéticos sean susceptibles de ataques o explotación. El uso potencial del ciberespacio para llevar a cabo ataques por parte de Estados, organizaciones, grupos y/o individuos presenta un nuevo dilema y un cambio de juego dentro de las relaciones internacionales.

La transformación de las sociedades en sociedades de información, gracias a la integración de nuevas tecnologías en todas sus actividades e infraestructuras, aumenta la dependencia de los individuos, de las organizaciones, de las empresas y de los Estados, de los sistemas de información y de las redes. Esto constituye un riesgo de primer orden que debe contemplarse como un peligro para la seguridad, y el entender las capacidades de ciberseguridad de cada uno de los actores (desde Estados hasta empresas, organismos e individuos) y las tendencias de los ataques cibernéticos es el primer paso hacia el fortalecimiento de la capacidad de respuesta.

A pesar de los grandes avances tecnológicos logrados en las áreas de *hardware* y *software* de los sistemas informáticos, los ciberataques perpetrados los últimos años

[1] Gobierno de Estados Unidos. Homeland Security. *Cybersecurity Overview,* Homeland Security. Dirección URL: https://www.dhs.gov/cybersecurity-overview. [Fecha de consulta: 14 de agosto de 2016.]

han resultado en enormes fugas de datos que a su vez se han traducido en escándalos políticos por espionaje, y en grandes pérdidas económicas. Entre los ataques cibernéticos más importantes se encuentran los dirigidos contra la Casa Blanca de Estados Unidos, contra *Sony Pictures Entertainment, eBay*, una fábrica alemana de acero y contra una planta nuclear de Irán, en donde se rompe la barrera de lo virtual y lo físico afectando también el *hardware*.

Estos ataques y muchos otros más, demuestran la vulnerabilidad de las infraestructuras cibernéticas y la necesidad crítica de una fuerte protección de las mismas. Las infraestructuras críticas, se han protegido durante años contra sabotajes y los ataques físicos. Sin embargo, a medida que fue pasando el tiempo, se dio un crecimiento exponencial del número de infraestructuras críticas que operan sobre las redes del ciberespacio. Esto también ha traído consigo un aumento del número de ataques cibernéticos a las mismas, comprometiendo así la capacidad de un país de proveer servicios imprescindibles para sus ciudadanos.

La infraestructura crítica de Estados Unidos está compuesta por instituciones privadas y públicas en diferentes sectores como el agua, la energía eléctrica, el sector energético, el sistema bancario, las telecomunicaciones, el sector salud, el gobierno, transportes, servicios postales, materiales químicos y peligrosos, alimentos y servicios de emergencia. El ciberespacio, es el entorno de control de todos esos servicios, por lo tanto, el óptimo funcionamiento del mismo es esencial para la economía y la seguridad nacional del país.

Es por todo lo anterior, que el objetivo de esta investigación es analizar la estrategia de ciberseguridad de Estados Unidos para la protección de la infraestructura crítica en el caso específico del Sistema de Posicionamiento Global así como evaluar las consecuencias que podría tener un ataque cibernético en el mismo, partiendo de que la protección de la infraestructura crítica es considerada para la política de seguridad nacional de Estados Unidos como uno de los pilares fundamentales. En consecuencia, un ataque al GPS, desde el interior o el exterior, establece una prioridad para Estados Unidos porque se pone en juego la estabilidad y seguridad de la nación.

En la primera mitad del Capítulo I *De la seguridad tradicional a la ciberseguridad* se hace un breve recuento de la evolución del concepto de seguridad en las relaciones internacionales hasta el surgimiento de la ciberseguridad. Asimismo, se explican los

conceptos que han surgido a partir del nuevo espacio creado por la red, el ciberespacio, considerado como el cuarto dominio, y las implicaciones que éste representa en el siglo XXI.

En la segunda mitad del primer capítulo se desarrolla el concepto de infraestructura crítica y el rol que ha desempeñado la ciberseguridad para su protección. Además, se exhibe el panorama existente en los países de América Latina con respecto a la relación ciberseguridad-infraestructura crítica haciendo un balance de los logros y los retos por enfrentar en la región en cuanto a cuestiones cibernéticas.

En el Capítulo II *La ciberseguridad como estrategia de seguridad nacional en Estados Unidos* se realiza un recuento de las estrategias de seguridad nacional de Estados Unidos a través del tiempo, haciendo énfasis en sus coincidencias y diferencias así como los cambios que presentan después de acontecimientos parteaguas como el ataque del once de septiembre de 2001 a las Torres Gemelas en Nueva York.

Una vez que se hace esta revisión en la que a la par se establece el momento en el que la ciberseguridad se vuelve una prioridad para la seguridad nacional de Estados Unidos, se exponen los actores no estatales que juegan un rol relevante en ella. En la última parte de este segundo capítulo, se analizan las acciones tomadas por el gobierno estadounidense hasta la administración más reciente, la de Donald Trump, para la protección de su infraestructura crítica en el marco de la seguridad cibernética.

Por último en el Capítulo III *La ciberseguridad en el Sistema de Posicionamiento Global (GPS)* se exponen todas las características técnicas del GPS y su desarrollo tecnológico a lo largo del tiempo. También se explica su funcionamiento, todos los aspectos fundamentales que lo componen como la parte legislativa y su financiamiento, sus múltiples usos en las diferentes esferas civil, militar y científica, y la cooperación internacional que ha llevado a cabo Estados Unidos con otros países que cuentan con Sistemas de Navegación por Satélite.

En la segunda parte de este último capítulo se muestra la importancia que tiene el Sistema de Posicionamiento Global como infraestructura crítica para la seguridad nacional de Estados Unidos. Se exhiben sus vulnerabilidades y se plantean diferentes vías por las que puede sufrir un ataque cibernético así como las posibles consecuencias del mismo. Para cerrar el capítulo se habla de la prospectiva del GPS, es decir, la

adquisición por parte del gobierno estadounidense de satélites mejorados y más resilientes a ciberataques con el fin de proteger toda la infraestructura nacional que depende del sistema y, por consiguiente, para la conservación de su seguridad nacional.

La investigación concluye con un balance de lo que se ha hecho en cuestiones de ciberseguridad, los objetivos alcanzados y los retos y obstáculos por superar y lograr no sólo de Estados Unidos sino a nivel global.

I. De la seguridad tradicional a la ciberseguridad.

1.1. Aspectos conceptuales y aproximaciones históricas-disciplinarias.

De acuerdo con la Real Academia de la Lengua Española, la seguridad es definida como la cualidad de seguro[2], siendo éste a su vez el que está libre y exento de riesgo[3]. Como el mismo diccionario lo indica, existen diversos tipos de seguridad: social, pública, jurídica, etc., lo que denota los diferentes usos de este concepto y lo extenso de su contenido.

En cada una de sus acepciones el concepto de seguridad abarca diferentes objetivos, por lo que en esta investigación será abordado desde las Ciencias Sociales y en particular desde las Relaciones Internacionales a través de una breve cronología que describe la evolución que éste ha tenido y el impacto que ha generado su utilización por los diversos actores en la sociedad internacional.

1.1.1. El concepto de seguridad y su evolución en las relaciones internacionales.

Como concepto social, la seguridad ha sido un eje de debate en las Ciencias Sociales y entre ellas, en las Relaciones Internacionales, debido a sus extensas acepciones utilizadas por las diferentes escuelas teóricas de la disciplina. Este debate no sólo se ha dado en dicha disciplina, sino también en la historia de las relaciones internacionales; es así como se puede hablar de algunas de las principales posturas que comenzaron a deliberar en torno al concepto de seguridad y todo lo que este implicaba.

> Hugo Grocio desde un punto de vista jurídico, afirmaba que los Estados son los principales actores de la política internacional y que sólo el abordaje racional de la realidad internacional permitiría dirimir las disputas que aquejaban a las diversas naciones de la convulsionada Europa del siglo XVII. Los Estados son entidades que luchan por preservar su existencia e intereses y en un entorno donde no existe autoridad común se debe encontrar algún orden jurídico que, estando por encima de los Estados, sirviese como norma reguladora de sus políticas externas[4].

[2] Real Academia Española, *Diccionario: seguridad,* [en línea]. Dirección URL: http://dle.rae.es/?id=XTrIaQd. [Fecha de consulta: 28 de marzo de 2017].

[3] Real Academia Española, *Diccionario: seguro,* [en línea]. Dirección URL: http://dle.rae.es/?id=XTrgHXd. [Fecha de consulta: 28 de marzo de 2017].

[4] Jonathan, Arriola; Javier, Bonilla Saus; Campo Macarena del, *Hugo Grocio: en los orígenes del pensamiento internacional moderno,* [en línea], Universidad ORT Uruguay, 2010. Dirección URL: https://dspace.ort.edu.uy/bitstream/handle/20.500.11968/2779/documentodeinvestigacion59.pdf. [Fecha de consulta:

Su obra *Del derecho de la guerra y la paz (De iure belli ac pacis)*, es considerada como el primer tratado, completo y sistemático, de derecho internacional[5]. Grocio adjudicaba a las naciones la responsabilidad moral de recurrir a la guerra sólo cuando el Derecho lo permitiera y pretendía que mediante la imposición universal de una serie de principios reguladores se estableciera un orden y cierta estabilidad entre los Estados, logrando de esta manera la paz internacional.

Por su parte, Thomas Hobbes en su obra *Leviatán* afirma que el fin del Estado es, particularmente, la seguridad. "[…] La causa final, fin o designio de los hombres (que naturalmente aman la libertad y el dominio sobre los demás) al introducir esta restricción sobre sí mismos (en la que los vemos vivir formando Estados) es el cuidado de su propia conservación y, por añadidura, el logro de una vida más armónica"[6]. Hobbes describe una sociedad internacional anárquica en la que designa al Estado como el responsable de la seguridad tanto al interior como al exterior.

Asimismo, define al Estado como "una persona de cuyos actos se constituye en autora una gran multitud mediante pactos recíprocos de sus miembros con el fin de que esa persona pueda emplear la fuerza y todos los medios como lo juzgue conveniente para asegurar la paz y defensa común. El titular de esta persona se denomina SOBERANO, y se dice que tiene poder soberano; cada uno de los que le rodean es SÚBDITO suyo"[7]. Esta tradición hobbesiana daría paso a los principios que más tarde, caracterizarían al realismo.

Emmanuel Kant con una visión más filosófica, también confiere al Estado la responsabilidad de proteger a sus ciudadanos sin embargo, asegura que dentro del sistema internacional los Estados se comportan de acuerdo con normas morales. Es por esto que confía en la labor de las instituciones internacionales para mantener la paz y la seguridad, sancionando a aquellas naciones que no cumplan con dichos objetivos.

En 1787, Alexander Hamilton en *El Federalista* también trató el tema de la seguridad refiriéndose al caso específico de lo que después sería conocido como

---

5 de julio de 2017].

[5] Instituto de Investigaciones Jurídicas UNAM, "Hugo Grocio, vida y obra", *Fundadores del Derecho Internacional,* [en línea]. Dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/1/383/7.pdf. [Fecha de consulta: 5 de julio de 2017].

[6] Thomas, Hobbes, *Leviatán. O la materia, forma y poder de una República, Eclesiástica y Civil,* Fondo de Cultura Económica, Buenos Aires, Argentina, 1992, p.137.

[7] *Ibídem,* p. 141.

Estados Unidos. Hamilton afirmaba en uno de sus ensayos que las circunstancias que ponen en peligro la seguridad de las naciones eran infinitas, y que por esta razón no era prudente imponer trabas constitucionales al poder a quien está confiada. Este poder según él, debería ser tan amplio como todas las combinaciones posibles de esas circunstancias; y ejercerse bajo la dirección de los mismos consejos nombrados para presidir la defensa común[8].

Hamilton consideraba que las facultades para organizar ejércitos, construir y equipar flotas, dictar las reglas que gobernarían a ambos y dirigir sus operaciones, debían existir sin limitación alguna porque resultaba imposible prever o definir la extensión y variedad de las exigencias nacionales o de los medios necesarios para la defensa común. De esta manera, también confirió al Estado la responsabilidad de proveer seguridad a sus ciudadanos poniéndole a su alcance todas las herramientas posibles para lograrlo.

Todas las visiones mencionadas abarcan diferentes aristas del concepto de seguridad: jurídica, teológica, política, moral, militar y filosófica; y de alguna manera, ejercieron cierta influencia en los posteriores debates dentro de la Teoría de Relaciones Internacionales sobre lo que implica el concepto de seguridad en el sistema internacional. A continuación, se muestra una tabla que resume las principales teorías y sus postulados acerca de la seguridad.

[8] Alexander, Hamilton; James, Madison; John, Jay, *El Federalista,* [en línea], p. 25. Dirección URL: https://d3n8a8pro7vhmx.cloudfront.net/danielcassidyforld24/pages/1/attachments/original/1418716919/El-Federalista.pdf?1418716919. [Fecha de consulta: 5 de julio de 2017].

Tabla 1.1. Principales teorías de las Relaciones Internacionales y su concepción de la seguridad.

Teoría	Realismo	Neorrealismo	Liberalismo	Neoliberalismo	Constructivismo
Actor principal	Estado	Estados Organizaciones internacionales	Individuo Estado	Estado Individuo Nuevos actores: Organizaciones Internacionales	Estado Nuevos actores
Premisas	Anarquía en el sistema internacional Tendencia permanente del conflicto Balance de poder Lucha por el poder Juego suma cero Dilema de seguridad Garantizar la supervivencia del Estado Interés nacional Fuerza militar	Anarquía en el sistema internacional Lucha por el poder Cooperación con limitaciones Conducta de los Estados producto de la competencia entre ellos Balance de poder Ganancias relativas	Valores (Democracia) Cooperación Paz Integración Interdependencia	Cooperación: intereses comunes Choque de valores=conflicto Ganancias relativas Fuerza militar y económica Interdependencia económica	Seguridad: construcción social en un contexto específico. Identidad: central para la construcción de la seguridad. Normas que surgen de la interacción social. Actores compiten para definir la identidad y los valores de un grupo en particular.
Representantes	Tucídides Hobbes Hans Morgenthau	Kenneth Buzan Waltz Glaser	Immanuel Kant Woodrow Wilson	Robert Keohane Robert Axelrod Joseph Nye Michael Doyle	Raymond Duvall Michael Barnett Alexander Wendt

Elaboración propia con información de Williams, Paul D. (ed.), *Security studies: an introduction,* Routledge, USA, 2008, 551 pp.

Sin duda alguna la visión realista de la seguridad ha ejercido una gran influencia, como se pudo ver durante el periodo de la segunda postguerra. El enfrentamiento bipolar Estados Unidos versus URSS definiría la seguridad internacional y sus amenazas en términos militares mediante alianzas bajo la premisa de defensa colectiva, interviniendo en diferentes países o estableciendo bases militares en los mismos,[9] y/o contando con un gran ejército armado.

[9] La Organización del Tratado del Atlántico Norte (EE.UU.) y la Organización del Tratado de Varsovia (URSS) serían las principales alianzas militares que establecidas por los hegemones. En un segundo plano pero no menos importante, se encontrarían otros pactos militares en zonas geopolíticamente importantes para Estados Unidos: el Tratado Interamericano de Asistencia Recíproca (TIAR) o Tratado de Río en 1947; en el Pacífico del Sur, el Tratado de Seguridad entre Australia, Nueva Zelandia y Estados Unidos (ANZEU) o Tratado de Seguridad del Pacífico, en 1951; en Asia Suroriental, la Organización del Tratado del Sudeste de Asia (OTSEA) en 1954; y en 1959 la Organización del Tratado de Asia Central (OTAC).

Las amenazas en este periodo venían del exterior, por lo que era fundamental preservar la integridad del Estado. El llamado *hardpower* donde la capacidad militar que poseían para atacar al enemigo era fundamental, así como el *softpower*[10] en el que cada potencia promovía los beneficios de su ideología y cultura, fueron piezas clave para salvaguardar el interés nacional. La carrera armamentista llevaría a cada una de las potencias a destinar gran parte de su capacidad económica a la investigación militar, dándole una concepción tradicional a la seguridad.

En este periodo mejor conocido como Guerra Fría, se haría evidente otra segmentación mundial a partir de 1960 derivada del proceso de descolonización gracias a la "Declaración sobre la Concesión de la Independencia a los Países y Pueblos Coloniales"[11], misma que modificaría la estructura del mapa internacional al aumentar en una década, de 51 a 130 el número de Estados integrantes de la sociedad mundial. Esta "nueva" división económica-moral estaría constituida por dos conjuntos o bloques de países diferenciados por su grado de desarrollo económico: los "desarrollados" en el Norte y los "subdesarrollados" en el Sur; en su mayoría antiguas metrópolis y colonias, respectivamente[12].

Mientras los países del Norte trataban de difundir e imponer una visión militar de la seguridad internacional, los países del Sur tratarían, por primera vez en conjunto, de definir su seguridad ya no sólo a partir de amenazas relacionadas directamente con el ámbito militar sino a partir también de amenazas derivadas del propio subdesarrollo -pobreza, analfabetismo, hambre, intervenciones militares, conflictos internos, luchas civiles, disputas territoriales, enfrentamientos tribales, desigualdad entre otros-. A pesar

[10] La implementación de definiciones, doctrinas, discursos y estrategias de seguridad y desarrollo a lo largo de este período, fungirían como instrumentos de dominación, de control, de disuasión y de contención. Cada uno de los discursos difundidos por ambos hegemones, irían acompañados de los valores inherentes al enfrentamiento bipolar. La libertad del individuo entendida como la independencia para poseer propiedad privada, la religión y la democracia sería un paradigma utilizado por el capitalismo. La lucha antiimperialista y la promesa del bienestar común serían utilizados por el socialismo.
Además, uno de los elementos más importantes de *softpower* serían las diversas doctrinas que constituirían el andamiaje ideológico. Dentro del bloque occidental, la Doctrina Truman en 1947 (por la que EE.UU. proporcionó ayuda militar a fuerzas anticomunistas), la Doctrina Johnson en 1965 (que justificó la intervención militar territorial en República Dominicana) y la doctrina Nixon en 1969, serían los mecanismos de disuasión y contención del socialismo. Mientras que en el bloque oriental y como respuesta especialmente a la doctrina Johnson, el Secretario General del Partido Comunista de la Unión Soviética Leonid Bresniev anunciaría en 1968 una doctrina que llevaría su nombre y que buscaría contener al capitalismo.
[11] También conocida como Resolución 1514 de la Organización de las Naciones Unidas.
[12] Sandra Kanety, Zavaleta Hernández, *Más allá de la visión tradicional de la seguridad y del desarrollo. Hacia la consecución de la seguridad humana y el desarrollo humano en las relaciones internacionales contemporáneas,* Tesis doctoral, FCPyS-UNAM, México, 2012, p. 79.

de esto, sería la concepción hegemónica realista/militar de la seguridad y el enfoque modernista/económico del desarrollo las que prevalecerían[13].

La Segunda Guerra Mundial había dejado debilitados a los imperios coloniales europeos obligándolos a centrar su atención y recursos al interior de sus fronteras y dando pie a una oleada de movimientos de liberación. De esta manera la herencia colonial aunada a las promesas de seguridad y de desarrollo, facilitarían que Estados Unidos y la Unión Soviética fueran *adueñándose* de los nuevos Estados frágiles y vulnerables atrayéndolos, cuando no forzándolos, hacia una de las dos esferas de influencia[14].

Una vez que llegó el fin del enfrentamiento de las dos superpotencias con la implosión de la Unión Soviética y el declive del socialismo, así como el ascenso de Estados Unidos como única hegemonía y la persistencia de organizaciones como la OTAN, instituciones como el Banco Mundial, el Fondo Monetario Internacional y la ONU, se suscitarían numerosos cambios[15] que dieron paso a un nuevo orden internacional, y dentro de éste, un replanteamiento de la creciente participación de nuevos actores y/o sujetos en la dinámica global.

Asimismo, el término de la Guerra Fría también evidenciaría numerosos conflictos de índole religioso, étnico, fronterizo, entre otros,[16] que habían permanecido de cierta manera *invisibles* en el escenario mundial, la mayoría de ellos producto de la injerencia de las potencias, ampliando así la percepción de posibles amenazas a la seguridad mundial y como consecuencia de ello, una significativa mutación del arquetipo tradicional y dominante de seguridad insertando una plétora de temáticas variadas en los asuntos internacionales.

---

[13] *Ídem.*
[14] *Ídem.*
[15] Acontecimientos significativos como la unificación de Alemania en octubre de 1990, el golpe de Estado contra Gorbachov durante agosto de 1991, la independencia de los países bálticos (Estonia, Letonia y Lituania), la creación de la Comunidad de Estados Independientes (CEI), el reconocimiento internacional de Eslovenia y Croacia como Estados, la división de Checoeslovaquia en República Checa y República Eslovaca, la progresiva inserción de los "países del Este" a la economía de mercado, entre otros, terminarían así con la arquitectura mundial que definiría las relaciones internacionales durante el periodo de posguerra. El fin del viejo orden significaría la instauración del "Nuevo Orden Mundial".
[16] Algunos ejemplos claros son las guerras civiles en República del Congo o en Sudán, los conflictos religiosos en Uganda y en Nigeria, los enfrentamientos étnicos en Ruanda, Burundi o Bosnia, los problemas fronterizos en varios países de América Latina como Perú-Ecuador, el de Venezuela-Guyana, Venezuela-Colombia, Nicaragua-Honduras y Argentina-Chile, sólo por citar algunos.

En efecto, el predominio de enfrentamientos de carácter interestatal caracterizados por motivaciones religiosas, políticas, sociales, económicas y culturales, la inexistencia ya de una amenaza comunista y la participación de diversos actores en la sociedad internacional, conllevarían a numerosas controversias y críticas a las premisas realistas, reduccionistas, unidimensionales y unidireccionales del concepto de seguridad y contribuirían en consecuencia, a la construcción de una noción amplia, multidimensional y multidireccional del mismo[17].

Con un nuevo y reconfigurado orden mundial, la concepción tradicional de seguridad en términos militares, de lucha por el poder y la protección del territorio contra agresiones externas, se fue modificando poco a poco. La seguridad entonces comienza a verse más allá de lo usual, tomando en cuenta sus múltiples aristas que van desde la seguridad humana, hasta la medioambiental, política, cultural, económica, entre otras.

Es así como en un mundo pos Guerra Fría, surge la Escuela de Copenhague, en la que varios autores desarrollaron una serie de observaciones acerca de los estudios de seguridad llevados a cabo hasta ese momento. En particular, destacó el trabajo de Barry Buzan, con su libro *People, States and Fear,* publicado en 1983 y en el que argumentó que la seguridad no se refería sólo a los Estados, sino también a las colectividades humanas; asimismo, tampoco podía limitarse a un enfoque de la fuerza militar.[18] Es por esto, que la seguridad en este sentido es afectada por diferentes factores clasificados en cinco grandes sectores[19]:

- Militar: refiriéndose a la capacidad defensiva y ofensiva armada con la que cada Estado cuenta.
- Político: centrado en la estabilidad organizacional de los Estados, es decir, el sistema de gobierno y las ideologías que le brindan legitimidad.
- Económico: enfocado en los recursos, las finanzas y los mercados necesarios para mantener niveles aceptables de bienestar y el poder del Estado.
- Social: incluye el lenguaje, la identidad nacional, la cultura, la religión y las tradiciones y costumbres.
- Ambiental: concerniente al mantenimiento de la biósfera local y del planeta como

[17] Sandra Kanety, Zavaleta Hernández, *Más allá de la visión tradicional de la seguridad y del desarrollo. Hacia la consecución de la seguridad humana y el desarrollo humano en las relaciones internacionales contemporáneas,* Tesis doctoral, FCPyS-UNAM, México, 2012, p. 82.
[18] Paul D., Wiliams (ed.), *Security studies: an introduction,* Routledge, USA, 2008, p. 3.
[19] *Ibídem*, p. 4.

un soporte esencial del que dependen todos los seres humanos.

De esta manera, las agendas nacionales e internacionales de seguridad y defensa de los países presentaron diversos cambios, mismos que se verían claramente reflejados en el creciente interés en temáticas diversas como el respeto a los derechos humanos y de las libertades fundamentales, el medio ambiente, la salud pública, educación, participación ciudadana, cuestiones de género, ayuda humanitaria, los procesos de democratización, entre muchos otros más, mismos que serían considerados de ahora en adelante los pilares de una novedosa noción de seguridad en la que el Estado ya no figuraba como el actor único y/o principal.

Así, el crimen organizado, la delincuencia organizada transnacional, la pobreza, la violación a los derechos humanos, el hambre, las epidemias, pandemias, los regímenes autoritarios o no democráticos, la proliferación de armas, las migraciones, los refugiados y desplazados, la sobre explotación de los recursos y como consecuencia el deterioro ambiental, las guerras civiles, los conflictos étnicos o religiosos, el desempleo, la falta de educación y más recientemente, los ataques cibernéticos, serían considerados como las nuevas amenazas a la seguridad internacional.

1.1.2. El ciberespacio: el nuevo espacio creado por la red.

El surgimiento de un nuevo orden tanto nacional como internacional de comunicación que va adquiriendo forma y dirección social principalmente a través de la *World Wide Web* (WWW), es uno de los resultados más impactantes de la revolución telemática. Con ello, se ha creado un espacio libre, público y distinto a todos los ya conocidos: el ciberespacio.

Las definiciones del concepto *ciberespacio* han sido diversas. El término fue utilizado por primera vez en el año de 1981 en un cuento de William Ford Gibson llamado "*Burning Chrome*"; no obstante, es hasta 1984 en su obra de ciencia ficción titulada "*Neuromancer*" (Neuromante), en la que realmente lo define como:

> [...] Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos... Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz clasificadas en el no-espacio de la mente, conglomerados y constelaciones de información [...][20].

[20] William, Gibson, *Neuromante,* Minotauro, España, 1984, p. 35.

Por supuesto cuando lo escribió, Gibson no se imaginaba lo que este concepto significaría en un futuro y él aceptó que no era un experto informático por lo que en su obra sólo se dedicó a describir una distopía en la que la tecnología superaba a la humanidad. Por su parte, la Real Academia Española lo define de una manera simple como aquel ámbito artificial creado por medios informáticos[21].

El ciberespacio es según el Departamento de Defensa de Estados Unidos, "un dominio global dentro del entorno de información que consiste en las redes interdependientes de infraestructuras de tecnología de la información y datos residentes, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados"[22]. Es decir, es mucho más que Internet, más que los mismos sistemas y equipos, el *hardware* y el *software* e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el ser humano para su servicio[23].

El ciberespacio es un ámbito que no puede ser controlado exclusivamente por alguna persona o Estado, es decir, se ha convertido en lo que se conoce como un *global common,* como lo son el espacio marítimo, el aéreo y el exterior, siendo a su vez diferente a éstos debido a su naturaleza artificial. Para comprender de mejor manera el ciberespacio, el autor estadounidense Martin Libicki[24], le ha dado una estructura conformada por tres capas: la física, la sintáctica y la semántica.

Se puede decir que la capa física es la más inmediata, pues es la base de todos los sistemas de información, esto es, desde un ordenador y todo lo que éste implica, hasta cables, satélites, cables submarinos y servidores. Por su naturaleza, son susceptibles a cualquier tipo de ataque físico que si bien no implica mucha elaboración, esto no quiere decir que los daños sean de menor gravedad, pues basta con saber que si se elimina esta capa simplemente desaparecen los sistemas de información.

---

[21] Real Academia Española, *Ciberespacio,* [en línea]. Dirección URL: http://dle.rae.es/?id=98Wdd57. [Fecha de consulta: 28 de noviembre de 2016].

[22] DoD, *Dictionary of Military and Associated Terms: cyberspace,* [en línea]. Dirección URL: http://www.dtic.mil/doctrine/dod_dictionary/?zoom_query=cyberspace&zoom_sort=0&zoom_per_page=10&zoom_and=1. [Fecha de consulta: 25 de noviembre de 2016].

[23] Escuela Superior de Ingenieros de Telecomunicaciones, *Seguridad nacional y ciberdefensa. Aproximación conceptual: ciberseguridad y ciberdefensa,* [en línea], Madrid, Enero de 2013, pág.4. Dirección URL: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf. [Fecha de consulta: 25 de noviembre de 2016].

[24] Martin C., Libicki, *Cyberdeterrence and Cyberwar,* RAND, USA, 2009, p. 210.

Por encima de la capa física, se encuentra la capa sintáctica, que contiene todas aquellas instrucciones que los diseñadores y los usuarios dan a un ordenador, así como los elementos necesarios para que estos últimos se comuniquen entre sí. Además, aquí se encuentran los sistemas operativos y los lenguajes utilizados para el funcionamiento de los programas y hacer legibles los datos. Es por esto, que es la capa más susceptible al hacking, es decir, la actividad que hace referencia a la manipulación de la tecnología para lograr que ésta haga algo para lo cual no fue diseñada[25].

La capa superior es la semántica, en la que se encuentra toda la información que contiene la computadora, es decir, la razón por la que los ordenadores existen[26]. Los datos, los programas que introducimos para gestionarlos y todo el conocimiento acumulado en los servidores forman parte de este nivel. La distinción entre información e instrucciones en estos niveles tiende a ser imprecisa, sin embargo, se puede hacer al analizar la primera como semántica en forma pero sintáctica en propósito.

Con lo anterior, se da a notar que el ciberespacio es un medio virtual, un espacio sin fronteras geográficas, característica que ha provocado que los riesgos y amenazas que surgen dentro de él puedan expandirse y ubicarse en cualquier parte del mundo, dificultando a su vez localizar a quien o quienes las producen. Es de esta manera, en la que surgen paralelamente los conceptos de ciberseguridad y ciberdefensa.

1.1.3. La ciberseguridad: tema prioritario en la agenda de seguridad global.

Hoy en día, el uso de la violencia en los conflictos no sólo está presente de manera física, sino en acciones que van desde el ámbito político, económico, psicológico y hasta el cibernético. Si no se tiene un control adecuado del ciberespacio, una nación puede ver amenazada su seguridad y libertad de acción. La ciberseguridad resulta así, un componente o aspecto muy importante de la seguridad nacional. Mediante la Resolución 181, la Unión Internacional de Telecomunicaciones[27] aprobó una definición de ciberseguridad tal como se expresa en la Recomendación UIT–T X.1205:

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas,

[25] Sevilla, Rodríguez José Luis, "Hablando correctamente de seguridad de la información*, Ambientes óptimos. De la incertidumbre a la acción segura,* Revista Seguridad. Cultura de prevención para TI, No. 20, abril-mayo 2014, México, UNAM, p. 14.
[26] Martin C., Libicki, *Op. cit.*, p. 12.
[27] La Unión Internacional de Comunicaciones (UIT o ITU por sus siglas en inglés) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación.

seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. 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. Las propiedades de seguridad incluyen una o más de las siguientes:

- disponibilidad;
- integridad, que puede incluir la autenticidad y el no repudio;
- confidencialidad[28].

Es importante destacar que los conceptos de ciberseguridad y seguridad informática suelen usarse como sinónimos, siendo la última definida como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema[29].

Es así, que ambos conceptos se refieren a todos aquellos medios utilizados para la protección de diversos elementos como son los sistemas informáticos y los usuarios con el fin de conservar su integridad y confidencialidad ante cualquier daño que pudiera destruirlo o interrumpir su correcto funcionamiento, todo esto, dentro de un mismo entorno, el ciberespacio.

Además, es necesario mencionar, que existe una confusión del concepto de ciberseguridad con el de seguridad de la información, siendo que en realidad, la primera está inmersa dentro de la segunda. La seguridad de la información, según la norma internacional ISO27001, se refiere a "la confidencialidad, la integridad y la disponibilidad de la información y los datos, independientemente del formato que tengan pues estos pueden ser electrónicos, en papel, audio, vídeo, etc."[30], y he aquí donde se distingue de la ciberseguridad pues su ámbito de protección es sólo el ciberespacio.

---

[28] UIT, Rec. UIT-T X.1205. Sector de Normalización de las Telecomunicaciones de la UIT (04/2008). Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad*. Seguridad en el ciberespacio – Ciberseguridad. Aspectos generales de la ciberseguridad.* (04/2008) *[en línea]*. Dirección URL: http://www.itu.int/es/Pages/default.aspx. [Fecha de consulta: 14 de agosto de 2016].

[29] Álvaro, Gómez Vieites, *Enciclopedia de la seguridad informática.* Alfaomega, México, 2007, p.11.

[30] Sistemas de Gestión de Seguridad de la Información, *¿Qué significa la Seguridad de la Información?,* [en línea]. Dirección URL: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/. [Fecha de consulta: 17 de mayo de 2017].

Una vez teniendo claro lo anterior, ¿cuándo fue que se comenzó a hablar de ciberseguridad? El dos de noviembre del año 1988, un estudiante graduado de la Universidad de Cornell llamado Robert Tappan Morris creó el malware que causó el mayor daño visto hasta el momento: el Gusano Morris o el Gran Gusano. Este virus lo puso en marcha a través de la red ARPANET[31], afectando hasta el 10%[32] (aproximadamente seis mil) de los ordenadores pertenecientes a instituciones gubernamentales y a universidades de Estados Unidos.

Aunque el Gusano Morris tenía diversas fallas, su éxito se debió a lo vulnerable que era la programación de los sistemas y las conexiones, y si bien, estas fallas eran conocidas por sus creadores, no se hizo nada para solucionarlas. Debido a sus graves consecuencias, Morris fue juzgado y declarado culpable de violar una ley hecha sólo dos años antes, la Ley de Fraude y Abuso Informáticos, por lo que fue condenado a tres años de libertad condicional, 400 horas de servicio comunitario y una multa de 10,000 dólares[33].

Sin embargo, no todas las consecuencias que provocó el Gusano Morris fueron negativas, pues hizo que el gobierno estadounidense creara el Equipo de Respuesta ante Emergencias Informáticas (CERT) para atender futuros ataques informáticos[34]. Es a partir de este momento que comienza el desarrollo de la seguridad informática, obligando a los proveedores de *software* a tener más cuidado con los errores en sus productos.

Acontecimientos como la creación de la *World Wide Web* (WWW) en 1991, el surgimiento un año después de la organización *Internet Society* (ISOC), la conexión a las redes de la Casa Blanca a través de su página *whitehouse.gov* en 1993*,* dos años después el lanzamiento de *Internet Explorer* por parte de Microsoft, la fundación de la Corporación de Internet para la Asignación de Nombres y Números (ICANN por sus siglas en inglés), la creación de *Google* en 1998; y el problema del año 2000 o también

[31] Considerada como el precursor de Internet.
[32] Fredy A., Escárcega García, *La estrategia de ciberseguridad de Barack Obama: El ataque (ciberguerra) al Programa Nuclear Iraní en 2010*, FCPyS, UNAM, 2017, p. 71.
[33] History, *Lanzamiento del primer gusano informático,* [en línea]. Dirección URL: https://uy.tuhistory.com/hoy-en-la-historia/lanzamiento-del-primer-gusano-informatico. [Fecha de consulta: 17 de mayo de 2017].
[34] El Equipo de Respuesta ante Emergencias Informáticas estadounidense fue el primero en su tipo y su creación hizo posible la fundación de estos equipos en diversas partes del mundo. Como se verá más adelante en esta investigación, países de Europa y América Latina han ido avanzando en la fundación de los mismos.

conocido como el Y2K[35], entre algunos otros, marcarían de manera definitiva las Tecnologías de la Información y la Comunicación del siglo venidero, el siglo XXI.

Es entonces, cuando la Organización de Naciones Unidas también comienza a plantear algunas resoluciones en esta área[36]:

- Resoluciones de la Asamblea General 55/63 (2000) y 56/121 (2001). Se invita a los Estados Miembros a que tomen en cuenta medidas como la elaboración de leyes y políticas nacionales, para combatir la utilización de la tecnología de la información con fines delictivos.
- Resoluciones de la Asamblea General 57/239 (2002) para la creación de una cultura global de ciberseguridad. A través de esta resolución se exhorta a crear la citada cultura teniendo en cuenta los principios de: conciencia, responsabilidad, respuesta ética, democracia, evaluación de riesgos, diseño y puesta en práctica de la seguridad, gestión de la seguridad y reevaluación.
- Resolución de la Asamblea General 58/199 (2004) para la protección de las infraestructuras de información. Se persigue estimular el desarrollo de normas de conducta en el ciberespacio que sirvan para la promoción del desarrollo socioeconómico y el suministro de bienes y servicios esenciales, la gestión de sus asuntos y el intercambio de información.

En los años siguientes, se generó un amplio debate internacional sobre la importancia de la ciberseguridad, reflejando el interés de los Estados por responder a los desafíos actuales dentro del ciberespacio, considerando también las amenazas emergentes y futuras, y así poder proponer estrategias globales para enfrentarlas. Es de esta forma, que surge la Agenda sobre Ciberseguridad Global de la Unión Internacional de Telecomunicaciones.

La Agenda sobre Ciberseguridad Global fue creada en el año 2007 por el Dr. Hamadoun I. Touré, Secretario General de la UIT en ese momento, y es un marco de cooperación internacional destinado a mejorar la seguridad y la confianza en la sociedad

[35] El Y2K fue un error de software que prometía un caos generalizado en ordenadores e infraestructuras críticas de todo el mundo en cuanto entrara el nuevo milenio. Muchos sistemas habían sido programados de tal forma que su reloj interno sólo podía alcanzar las 23:59 horas del día 31 de diciembre de 1999, por lo que al llegar al año 2000, los equipos lo marcarían como año 00, sin tener en cuenta el cambio de siglo. Esto significa que el mundo informático viviría en 1900.

[36] Universidad de Granada, *Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario,* Grupo de Estudios en Seguridad Internacional, Marzo 2015, [en línea]. Dirección URL: http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario. [Fecha de consulta: 17 de mayo de 2017].

de la información[37]. Asimismo, trabaja en cinco pilares fundamentales en un marco de cooperación internacional: medidas legales, medidas técnicas y de procedimiento, estructuras institucionales, la creación de capacidades y la cooperación internacional.

Cada uno de los rubros anteriores se encuentra brevemente explicado en la siguiente imagen.

Imagen 1.1. Aspectos que abarca la Agenda sobre Ciberseguridad Global.

Tomada de UIT, *Agenda sobre Ciberseguridad Global.* Dirección URL: http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html.

Meses después de que la Agenda fuera lanzada, se creó el Grupo de Expertos de Alto Nivel sobre Ciberseguridad (GEANC) con el fin de elaborar recomendaciones y crear estrategias que en conjunto, ayudaran a combatir las amenazas a las redes en

[37] UIT, *La Agenda sobre Ciberseguridad Global,* [en línea]. Dirección URL: http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html. [Fecha de consulta: 17 de mayo de 2017].

todo el mundo. En materia legal este grupo pretende establecer una legislación modelo sobre ciberdelincuencia, que sea globalmente aplicable y se adapte a las legislaciones nacionales y regionales existentes[38].

El GEANC recomendó también que la UIT se convirtiera en el "centro de excelencia" mundial para la compilación y distribución de información sobre ciberseguridad[39]. Además, reconoció que los principios contenidos en el Convenio sobre la Ciberdelincuencia[40] adoptada por el Consejo de Europa en Budapest en el año 2001, pueden servir como directrices en esta materia.

Por último, se debe destacar que independientemente de que cada país o región esté creando constantemente estrategias e iniciativas en cuestiones de ciberseguridad, en las que incluso, la Unión Internacional de Telecomunicaciones ofrece su apoyo y cooperación, esta última continúa promoviendo por su parte la organización de conferencias y foros regionales y mundiales[41] para enfrentar los retos y las amenazas que trajo consigo la creación del ciberespacio pues se estima que el cibercrimen le cuesta al mundo hasta US $575,000 millones al año, lo que representa 0,5% del PIB global[42].

1.1.4. La ciberdefensa y los ciberataques: sus implicaciones en el siglo XXI.

Hoy en día, el ciberespacio es un punto estratégico a considerar al establecer las estrategias de Seguridad Nacional de los países ya que las acciones tomadas para protegerse con anticipación a un ataque son de vital importancia para salvaguardar sus intereses como nación. La capacidad organizada para proteger, mitigar y recuperarse

[38] UIT, *Ciberseguridad-Grupo de Expertos,* [en línea]. Dirección URL: http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=06&ipage=05&ext=html. [Fecha de consulta: 21 de mayo de 2017].

[39] *Ídem.*

[40] También es conocido como Convenio de Budapest. Es el único acuerdo internacional que tiene como objetivo armonizar las legislaciones de los Estados miembros y que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional). Trata con carácter prioritario una política penal contra la ciberdelincuencia y está abierto a aquellos Estados que deseen adherirse.
Fue adoptado por el Comité de Ministros del Consejo de Europa en su sesión N. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

[41] International Intergovernmental High Level Panel: Protecting Critical Infraestructure from cyber attacks: a Global Challenge llevado a cabo en febrero de 2017 en Austria, el Regional Cybersecurity Forum en Bulgaria, el Regional Cybersecurity Summit and FIRST Arabic and African Regional Symposium en Egipto y el Central European Cybersecurity Public-Private Dialogue Platform a finales del año 2016 son sólo algunos de los foros y conferencias que la UIT ha organizado en temas de ciberseguridad en los últimos meses.

[42] OEA&BID, *Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016,* [en línea]. Dirección URL: http://www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420.html. [Fecha de consulta: 5 de abril de 2017].

rápidamente de los efectos de un ataque cibernético, es lo que comúnmente se conoce como ciberdefensa[43].

La capacidad de dominar la generación, manejo, uso y manipulación de la información se ha convertido en un recurso de poder altamente deseado en las relaciones internacionales, y como consecuencia de esto, la capacidad de defenderse de las ciberamenazas en el quinto dominio, como también es considerado el ciberespacio[44], se ha vuelto indispensable desde el comienzo del siglo XXI.

El ciberespacio es un dominio en el que las limitaciones clásicas de la distancia, el espacio, el tiempo y la inversión se reducen[45], por lo que se considera que la ofensa tiene un grado mayor de facilidad que la defensa, ya que esta última debe tener éxito siempre, lo que es casi imposible, mientras que con una sola vez que el atacante tenga éxito es suficiente. La confianza de la sociedad moderna en las redes informáticas, ha hecho que cualquier atacante tenga un sin fin de objetivos, lo que da lugar a una gran presión en el defensor para proteger con éxito sus sistemas.

Las amenazas, peligros y riesgos en el ciberespacio, tienen tres características generales[46]:

[43] EastWest Institute, *Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity,* [en línea], 2014, p. 47. Dirección URL: https://www.eastwest.ngo/idea/critical-terminology-foundations-2. [Fecha de consulta: 24 de noviembre de 2016].
[44] Considerando la tierra, el agua, el mar y el espacio como los otros cuatro dominios.
[45] Fred, Schreier, *On Cyberwarfare,* [en línea], DCAF Horizon, 2015, p. 31. Dirección URL: http://www.dcaf.ch/Publications/On-Cyberwarfare. [Fecha de consulta: 23 de mayo de 2017].
[46] *Ibídem*, p. 32.

Esquema 1.1. Características generales de las amenazas, los peligros y riesgos en el ciberespacio.

Elaboración propia con datos de Fred, Schreier, *On Cyberwarfare,* [en línea], DCAF Horizon, 2015, p. 32. Dirección URL: http://www.dcaf.ch/Publications/On-Cyberwarfare.

1. Son amplios como el ciberespacio mismo. Cualquier aspecto que dependa del dominio cibernético está potencialmente en riesgo: la integridad y la seguridad de las infraestructuras nacionales críticas, el sistema financiero, información clasificada de seguridad nacional, secretos comerciales explotables, etc.
2. La incrustación. Es decir, están arraigados porque la amenaza es una característica intrínseca del ciberespacio, que puede no ser totalmente erradicada.
3. Son diversos. Las amenazas, riesgos y peligros en el ciberespacio son tan diversos como la plétora de actores que explotan estas vulnerabilidades, las acciones que toman y los objetivos que atacan. Hay más actores además del Estado-nación: extremistas ideológicos y políticos, organizaciones terroristas, bandas criminales bien organizadas, hackers patrocinados por el Estado, mercenarios o individuales. Cada uno representa una amenaza distinta, que requiere una respuesta diferenciada.

Como la mayoría de los conceptos presentados en este capítulo, el de *ciberataque o ataque cibernético* presenta variaciones según quien lo defina. El autor

Martin Libicki, lo explica como “la interrupción deliberada o la corrupción por un Estado de un sistema de interés para otro Estado, siendo el primero el atacante y el último el objetivo”[47]. Mientras que un manual bilateral Estados Unidos-Rusia de terminología en ciberseguridad, define al ciberataque como “un uso ofensivo de un arma cibernética que pretende dañar un objetivo designado”[48].

Para fines de este trabajo, se combinarán las dos definiciones anteriores, siendo así el ciberataque, un uso ofensivo de un arma cibernética para dañar un objetivo de interés por parte del atacante. Nótese, que no se asegura que este último ni la parte atacada sean un Estado, puesto que, como se verá a lo largo de la investigación, los ciberataques pueden ser dirigidos por y/o hacia otros actores que no necesariamente son estatales.

De acuerdo con el Reporte de Riesgos Globales 2017 del Foro Económico Mundial, los ciberataques se encuentran dentro del top 10 de los riesgos con mayor probabilidad de que ocurran. Ocupan el sexto lugar después de riegos como los eventos climáticos extremos, la migración, los desastres naturales, los ataques terroristas y el fraude de datos. Aquí la tabla que lo muestra:

[47] Martin C., Libicki, *Op. Cit.,* p. 23.
[48] EastWest Institute, *Op. Cit.,* p. 44.

Tabla 1.3. Los 10 principales riesgos en términos de probabilidad.

Tomada de World Economic Forum, *The Global Risks Report 2017,* 12th Edition, [en línea]. Dirección URL: https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/The%20Global%20Risks%20Report%202017-01-2017.pdf.

En un mundo interconectado y donde la dependencia de las redes va en aumento, este dato es alarmante pues cualquier falla o intrusión en un sistema informático puede causar daños irreparables. Los ciberataques pueden clasificarse de manera muy general como la siguiente tabla lo indica.

Tabla 1.4. Clases de ciberataques.

Clase de ataque	Descripción
Pasivo	Incluyen analizar el tráfico, supervisar las comunicaciones no protegidas, descifrar el tráfico débilmente cifrado y capturar información de autenticación (por ejemplo, contraseñas). La interceptación pasiva de operaciones de red puede dar a los adversarios indicaciones y advertencias de acciones inminentes. Los ataques pasivos pueden resultar en la divulgación de información o archivos de datos a un atacante sin el consentimiento o conocimiento del usuario. Otros ejemplos pueden ser la divulgación de información personal como números de tarjetas de crédito y archivos médicos.
Activo	Incluyen intentos de evitar o romper las funciones de protección, introducir códigos maliciosos o robar o modificar información. Estos ataques pueden ir en contra de un backbone, explotar información en tránsito, penetrar electrónicamente en un enclave o atacar a un usuario remoto autorizado durante un intento de conexión a un enclave. Los ataques activos pueden resultar en la divulgación o difusión de archivos de datos, denegación de servicio o modificación de datos.
Cercano	Consiste en que un individuo normal alcance una proximidad física cercana a redes, sistemas o instalaciones con el propósito de modificar, recopilar o denegar el acceso a la información.
Interno	Pueden ser maliciosos o no maliciosos. Los maliciosos escuchan, roban o dañan información. Utilizan la información de manera fraudulenta, o no permiten el acceso a otros usuarios autorizados. Los ataques no maliciosos típicamente resultan de descuido, falta de conocimiento o elusión intencional de la seguridad.
Distribución	Se centran en la modificación maliciosa de hardware o software en la fábrica o durante la distribución. Estos ataques pueden introducir código malicioso, como una puerta trasera, en un producto para obtener acceso no autorizado a información o una función del sistema en una fecha posterior.

Tomada de Fred, Schreier, *On Cyberwarfare,* [en línea], DCAF Horizon, 2015, pp. 55-56. Traducción propia. Dirección URL: http://www.dcaf.ch/Publications/On-Cyberwarfare.

Otra categorización más específica de los ciberataques es la siguiente:

Tabla 1.5. Categorización de los ciberataques.

Categoría	Subcategoría	Ejemplos
Integridad Los ciberataques pueden usar técnicas de hacking para modificar, destruir o hacer otras acciones que comprometan la integridad de los datos.	Propaganda/desinformación	Modificación o manipulación de datos o introducción de datos contradictorios para influir en resultados políticos o de negocios o desestabilizar un régimen extranjero.
	Intimidación	Ataques a sitios web para ejercer coerción sobre sus propietarios (públicos o privados) para remover o modificar contenido o perseguir otros fines.
	Destrucción	Destrucción permanente de datos para afectar competidores o atacar gobiernos extranjeros. Puede ocurrir por ejemplo, dentro de un conflicto a gran escala.
Disponibilidad Ataques de negación de servicio ejecutados por botnets, por ejemplo, pueden ser usados para prevenir que usuarios accedan a datos que de otra manera no estarían disponibles.	Información Externa	Accesos denegados, etc. Ataques contra servicios del gobierno o privados disponibles para el público, por ejemplo, medios de comunicación, sitios de información gubernamentales, etc.
	Información Interna	Ataques a intranets gubernamentales o privadas, por ejemplo, redes de servicios de emergencia, sitios de banca electrónica, email corporativo, sistemas de control y comando, etc.
Confidencialidad Los ciberataques pueden apuntar a varios tipos de información confidencial, a menudo para propósitos criminales.	Espionaje	Firmas buscando información sobres sus competidores; Estados envueltos en actividades espías (en contra de gobiernos extranjeros e individuos).
	Robo de datos personales	Suplantación de identidad (o similares) dirigidos a usuarios débiles que engañados revelan datos personales, como números de cuentas bancarias; virus que almacenan y suben datos desde una computadora de un usuario.
	Robo de identidad	Troyanos, y demás, usados para robar la información de identidad y usarla para cometer crímenes.
	Extracción de datos	Técnicas de código abierto empleadas para descubrir, por ejemplo, información personal de los datos a disposición del público.
	Fraude	Con frecuencia enviado vía email mediante spam, el fraude incluye el popular nigeriano “419” o técnicas avanzadas de fraude, así como intentos de convencer al destinatario para comprar bienes o servicios fraudulentos.

Tomada de Fredy A., Escárcega García, *La estrategia de ciberseguridad de Barack Obama: El ataque (ciberguerra) al Programa Nuclear Iraní en 2010,* FCPyS, UNAM, 2017, pp. 55-56.

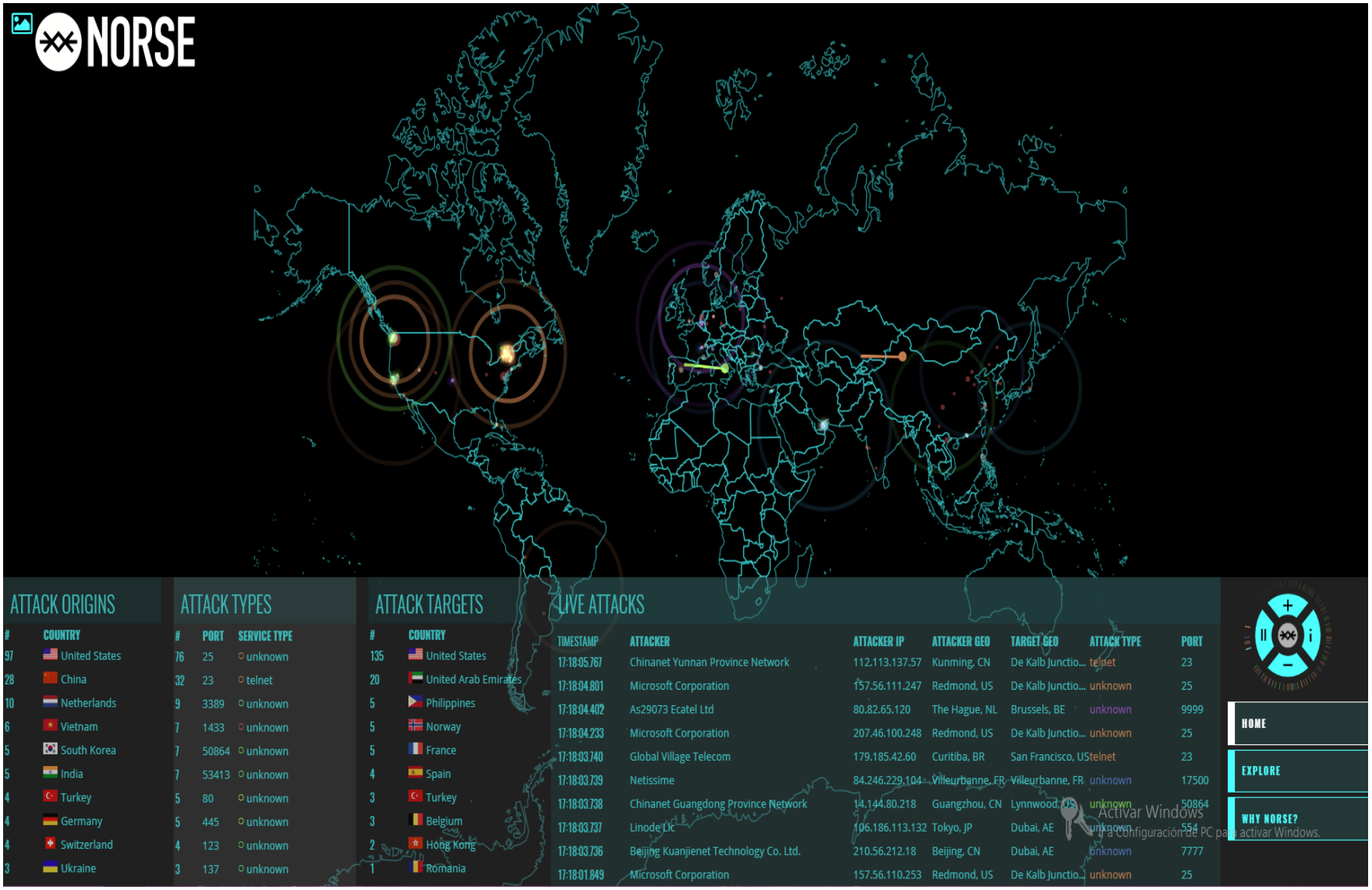
La corporación estadounidense *Norse*, se dedica a entregar informes de inteligencia de ataques cibernéticos en vivo, lo que ayuda a sus clientes a bloquear dichos ataques, descubrir brechas ocultas y contar con un seguimiento de las amenazas emergentes en todo el mundo[50]. En su página de internet, cuentan con un mapa en el que se muestran los ciberataques llevados a cabo en ese momento, así como su clasificación y dos listas que muestran de dónde proviene el ataque y su objetivo.

Como se puede observar en el mapa proporcionado por dicha empresa, el lugar donde se muestra más actividad es en Estados Unidos siendo el país desde donde se origina la mayor cantidad de ciberataques pero también el país que más los recibe. Seguido de China en cuanto a los países de origen sin embargo, este no se encuentra en la lista de los primeros 10 países objetivos de ciberataques pues el segundo más atacado son los Emiratos Árabes.

La lista debajo del mapa también nos muestra que los principales objetivos de ciberataques son compañías informáticas y que los países europeos y asiáticos se encuentran entre los primeros diez que atacan y son atacados. Siendo diferente la situación para los países de América Latina y África donde es rara la vez que se muestra cierta actividad cibernética de este tipo.

[50] Norse, *Who we are,* [en línea]. Dirección URL: http://www.norse-corp.com/about-us/who-we-are/. [Fecha de consulta: 22 de mayo de 2017].

Mapa 1.1. Ciberataques en el mundo.



Tomada de Norse, *Norse Attack Map,* [en línea]. Dirección URL:

http://map.norsecorp.com/#/.

Entre los ataques cibernéticos ocurridos en el siglo XXI de mayor relevancia por sus consecuencias, se encuentran los siguientes:

Tabla 1.6. Ciberataques más importantes del Siglo XXI.

Fecha	Atacante	Atacado	Descripción del Ataque
2000	Onel de Guzmán (Hombre filipino)	Nivel internacional Estados Unidos, Gran Bretaña, Alemania y España entre los más afectados	Virus *I Love You*. Afectó a sistemas informáticos de empresas, bancos, bolsas, periódicos, oficinas gubernamentales, etc. Generó una pérdida total de más de 5,500 millones de dólares.[51]
2002 (2000-2002)	Israel	Palestina	Adolescentes israelíes crearon un sitio web para atascar los sitios web de Hezbollah y Hamas en Líbano y de la Autoridad Nacional Palestina. Este aparentemente ataque menor provocó una guerra cibernética que rápidamente se convirtió en un incidente internacional. En enero de 2001, el conflicto había afectado a más de 160 sitios israelíes y 35 palestinos[52].
2003	China	Taiwán	Ciberataque de denegación de servicio (DDoS) a infraestructuras como hospitales y la bolsa.
2007	Rusia	Estonia	La reubicación del monumento conmemorativo del sacrificio de las fuerzas armadas soviéticas en la liberación de Estonia del yugo nazi durante la Segunda Guerra Mundial, desde Tallin a un cementerio militar fuera de la ciudad, provocó protestas de la minoría rusa seguidas de ataques DDoS que paralizaron los sitios web del gobierno de Estonia, la industria bancaria y los medios de comunicación.
2007	China	Europa	El Servicio de Seguridad Británico, la Oficina del Primer Ministro francés y la Oficina de la Canciller alemana Angela Merkel acusaron a China de las intromisiones en sus redes gubernamentales.
2007	Israel	Siria	La "operación Huerto" fue un ataque aéreo israelí a un reactor nuclear en construcción en territorio sirio fabricado por técnicos norcoreanos para procesar plutonio. El ataque cibernético alcanzó el objetivo militar de hacer indefensas las fuerzas defensivas, sin una destrucción generalizada de la propiedad o la pérdida de vidas de cualquier lado.
2008	Rusia	Georgia	Es el primer ejemplo de ataques cibernéticos que coincidió directamente con una invasión terrestre, marítima y aérea por parte de un Estado contra otro. Rusia invadió Georgia en respuesta al ataque de Georgia contra los separatistas en Osetia del Sur. El ciberataque fue dirigido contra sitios web del gobierno georgiano, las instituciones financieras y educativas, las asociaciones empresariales, sitios web de los medios de comunicación y otros sitios estratégicos, entre ellos las embajadas de Estados Unidos y Gran Bretaña.

[51] Fredy A., Escárcega García, *Op. Cit.,* p. 74.
[52] Fred, Schreier, *Op. Cit.,* p. 108.

Fecha	Atacante	Atacado	Descripción del Ataque
2009	China	Estados Unidos	"Operación Aurora". 34 empresas entre ellas *Google* y *Yahoo* sufrieron robo de información a través de un *malware*. El servidor de donde salió el troyano y a donde se comunicaba el *software* malicioso se localizó en China.
2010	Se acusa a Israel y a Estados Unidos pero esto no ha sido comprobado	Irán	*Stuxnet*. El gusano tomó el control de 1000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse. Fue la primera vez que un ataque cibernético logró dañar la infraestructura del mundo real.
2014	Corea del Norte (sin comprobar)	Sony	Los atacantes habían pedido a *Sony* cancelar el estreno y distribución de *The Interview*, una película de Seth Rogen donde los personajes infiltran a Corea del Norte para matar a su dictador. *Sony* a pesar de las amenazas realizó el estreno y como consecuencia los delincuentes tuvieron acceso a más 100 *terabytes* de datos. Robaron información confidencial del estudio, lo que incluyó datos personales de los empleados, salarios, contenido de correos electrónicos, copias de películas terminadas y más.
2016	Rusia	Partido Demócrata de Estados Unidos	Se cree que *crackers* patrocinados por el gobierno ruso entraron al sistema del Partido Demócrata en plenas elecciones presidenciales. Tuvieron acceso al correo electrónico de John Podesta, jefe de la campaña de Hillary Clinton. Los documentos robados fueron liberados al público y afectaron la campaña presidencial de Clinton.
2017	Sin conocimiento	Disney y Netflix	Dos grupos distintos robaron dos de los próximos estrenos de las compañías: *Pirates Of The Caribbean: Salazar's Revenge* y la quinta temporada de *Orange Is the New Black*. Para recuperarlos, los delincuentes les han pedido exorbitantes sumas de dinero, ninguna de las empresas ha cedido.
2017	Grupo de hackers "Shadow Brokers"	Agencia de Seguridad Nacional (NSA) de Estados Unidos	Filtración de documentos y robo de datos de las herramientas de *hackeo* utilizadas por la Agencia.
2017	Sin conocimiento	Nivel internacional Más de 100 países afectados	Virus *WannaCry*. Este virus tipo *ransomware*, es una vulnerabilidad descubierta por la NSA y luego liberada por los piratas informáticos en Internet. Atacó sistemas informáticos, a una velocidad increíble, de más de 100 países incluyendo hospitales, bancos y compañías de telecomunicaciones. El virus encripta los documentos de los ordenadores y a cambio pide un pago a un número de cuenta en *bitcoins*. Un experto británico ha detenido su esparcimiento temporalmente.

Elaboración propia con datos tomados de diversas fuentes.

Como se pudo observar en la tabla, los ciberataques han ido incrementando con el paso del tiempo no sólo en número sino en su capacidad de provocar grandes daños tanto a empresas como a numerosos países, es por esto, que la preocupación por contar con una capacidad de ciberdefensa eficaz se ha vuelto primordial.

1.2. La infraestructura crítica: desarrollo y situación actual.

1.2.1. El debate alrededor del concepto de infraestructura crítica.

Toda nación, cuenta con infraestructuras que proporcionan servicios que hacen que la vida diaria de sus ciudadanos pueda llevarse a cabo sin complicaciones. Dentro de estas infraestructuras, hay algunas que tienen mayor importancia dado que proveen servicios básicos e indispensables, éstas han sido denominadas como *infraestructuras críticas.*

Sin embargo, existe una gran controversia y debate alrededor del concepto de *infraestructura crítica* puesto que no hay un consenso sobre lo que este implica, dando lugar a que cada Estado decida qué servicios considerar dentro de dicha categoría. Por ejemplo, la Unión Europea decidió crear el llamado "Plan Europeo para la Protección de Infraestructuras Críticas" (PEPIC) en el año 2007, y aunque dicho plan sirve como guía para los Estados miembros, éstos a su vez, también cuentan con sus propias medidas de protección.

El PEPIC, define como infraestructura crítica aquellas instalaciones, equipos físicos y de tecnología de la información, redes, servicios y activos cuya interrupción o destrucción pueden tener grandes repercusiones en la salud, la seguridad o el bienestar económico de los ciudadanos o en el funcionamiento de los gobiernos de los Estados miembros[53]. Este plan, se centra en tres aspectos principales[54]:

1. Los aspectos estratégicos y la elaboración de medidas aplicables horizontalmente a todas las actividades en materia de protección de infraestructuras críticas (PIC);
2. La protección de las Infraestructuras Críticas de la Unión Europea (ICE) reduciendo su vulnerabilidad;
3. El tercero, se inscribe en un marco nacional y está destinado a ayudar a los Estados miembros a proteger sus Infraestructuras Críticas Nacionales (ICN).

El Plan Europeo para la Protección de Infraestructuras Críticas pretende facilitar la cooperación entre los Estados miembros, permitiendo el intercambio de información sobre amenazas y vulnerabilidades, así como estrategias que garanticen una adecuada protección de sus infraestructuras críticas. La profunda interdependencia que existe entre los Estados hoy en día, ha hecho que se creen planes como el europeo debido a

[53] EUR-Lex, *Programa Europeo para la Protección de Infraestructuras Críticas,* [en línea]. Dirección URL: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l33260. [Fecha de consulta: 30 de mayo de 2017].
[54] *Ídem.*

que si se llegara a presentar la vulneración de alguna infraestructura crítica nacional, los efectos pueden llegar a ser devastadores.

Como se mencionó anteriormente, la elaboración de planes regionales para la protección de infraestructuras críticas, no descarta que cada nación establezca el propio y el claro ejemplo de este caso lo es España. En el año 2011, el gobierno español lanzó la Ley 8/2011 en la que se establecen medidas para la protección de las infraestructuras críticas, definiendo éstas como "las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales"[55].

Se puede observar que en la descripción anterior se utiliza el término *infraestructuras estratégicas*, que son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales[56] según la misma ley. Es decir, el gobierno de España considera como infraestructuras críticas aquellas instalaciones y servicios relacionados con los siguientes sectores estratégicos:

- Industria nuclear y química
- Transportes
- Energía
- Tecnologías de la Información y las Comunicaciones
- Salud
- Telecomunicaciones
- Sistema financiero y tributario
- Alimentación
- Agua
- Espacio
- Administración del Estado

Es importante destacar una vez más, que el concepto de *infraestructura crítica* puede abarcar diferentes sectores para las diversas personas y/o para cada uno de los Estados, de ahí que surja el debate sobre lo que es o no es considerado dentro de dicho

[55] Gobierno de España, *Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas,* [en línea], Ministerio de la Presidencia y para las Administraciones Territoriales. Dirección URL: http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630. [Fecha de consulta: 30 de mayo de 2017].
[56] *Ídem.*

rubro. Por ejemplo, para Estados Unidos las infraestructuras críticas abarcan 16 sectores[57], mientras que como se vio, España las engloba en tan sólo 11 áreas.

Una mención especial también se merece el hecho de que en algunos países, las infraestructuras críticas son operadas por el sector privado como en España, Chile o Estados Unidos por mencionar algunos, no obstante, esto no implica que el gobierno no se encargue de su defensa por lo que la cooperación Estado-entidades privadas es fundamental para poder crear estrategias que las protejan y reduzcan su nivel de vulnerabilidad.

Entonces, para fines de esta investigación y de una manera general, las infraestructuras críticas son aquellas instalaciones físicas o virtuales vitales que al sufrir un ataque que las inhabilite o destruya por completo, generan un debilitamiento en la seguridad, en la economía nacional y en la capacidad del Estado para proveer de servicios esenciales a sus ciudadanos.

1.2.2. El rol de la ciberseguridad en la protección de la infraestructura crítica.

El ciberespacio se distingue de los demás dominios: tierra, mar, aire y espacio, por ser creado por y para el hombre, además de ser intangible. No obstante, eso no quiere decir que se mantenga alejado o separado de ellos, pues hoy en día muchas de las infraestructuras que se encuentran en estos dominios físicos, están conectadas de alguna forma con las redes del ciberespacio.

Con el rápido avance de la tecnología, las infraestructuras críticas se han ido modernizando y conectando a las redes del ciberespacio, existiendo la posibilidad de automatizar procesos y tener un enorme potencial para crear mejoras y así aumentar el crecimiento económico de una empresa o una nación. Sin embargo, así como esta conexión ha generado numerosos beneficios también ha creado diversos riesgos, por años los Estados han protegido sus infraestructuras críticas contra ataques físicos y sabotajes, pero hoy en día el plano de la seguridad física no es el único y muchos menos suficiente, sino que además, se tiene que contemplar el de la ciberseguridad.

La Protección de la Infraestructura de Información Crítica (CIIP), es una derivación del concepto más ampliamente conocido de Protección de la Infraestructura Crítica (CIP), o la protección de las infraestructuras de energía, telecomunicaciones,

[57] Las infraestructuras críticas de Estados Unidos se ahondarán en el segundo capítulo de esta investigación.

suministro de agua, transporte, finanzas, salud y otras que permiten que funcione una nación[58]. Los ataques a la infraestructura crítica se han convertido en una gran preocupación para los gobiernos y proveedores privados de todo el mundo debido a la importancia que representan.

Hasta hace relativamente poco tiempo, se creía que un *malware* no tenía la capacidad de destruir equipos físicos y que sólo podía dañar bases de datos, respaldos de información, imágenes, etc., sin embargo, ese paradigma ha sido destruido: ya es posible dañar *hardware*. El primer ataque de este tipo ocurrió en 2010 a unas instalaciones iraníes con el virus *Stuxnet*, causando daños a las mismas y marcando así el inicio de los ciberataques que borran la frontera entre la seguridad física y digital.

En gran medida, las principales fallas de seguridad se deben a que los sistemas operativos (SO) y de control utilizados en el tipo de plataformas de las infraestructuras son obsoletos. Uno de los más utilizados es el Sistema de Control de Supervisión y Adquisición de Datos (SCADA, por sus siglas en inglés), este es una aplicación *software* de control de producción que se comunica con los dispositivos de campo y controla el proceso de forma automática desde la pantalla del ordenador.

Asimismo, SCADA proporciona información del proceso a diversos usuarios: operadores, supervisores de control de calidad, supervisión, mantenimiento, etc., y está presente en sistemas que controlan las defensas contra inundaciones, las represas, las instalaciones de generación de electricidad, los oleoductos, los controles de plantas químicas y muchos otros componentes de la infraestructura crítica.

Antes, eran controles manuales o eran controlados por *hardware* y *software* especiales y que sólo algunos expertos en el tema entendían. Hoy eso ha cambiado. En la actualidad, la utilización creciente de equipos, sistemas operativos y plataformas de red similares a los usados en internet, ha ampliado la cantidad de actores con conocimiento de su funcionamiento así como las amenazas a las que están expuestos, mismas que pueden generar un gran impacto no sólo afectando a las empresas que las utilizan sino que también pueden causar daños a un país entero.

Pocos años después de *Stuxnet* surgieron otros *malwares* como *Flame* o *Duqu* que funcionaban de manera muy similar al primero. A finales del año 2015, un código

[58] OEA, *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas,* 2015, p. 13.

malicioso bautizado como *Black Energy* fue capaz de infectar los sistemas de control industrial SCADA de compañías eléctricas ucranianas, dejando sin electricidad por varias horas miles de hogares. Después de esto, es innegable que los ataques cibernéticos en los sistemas de control industrial son ya una realidad.

Instalaciones de generación de energía, plantas de agua, gas, sistemas de control de tránsito, fábricas, entre muchos otros más, se han convertido en objetivos de los atacantes. Ya sean ataques cometidos por criminales cibernéticos que buscan tener ganancias económicas, ventajas competitivas en el mercado o como actos políticos que buscan debilitar la seguridad de los gobiernos y las compañías, se hace imprescindible crear un plan con medidas eficaces de prevención y protección contra las amenazas emergentes hacia tales infraestructuras.

La globalización de las economías representa una amenaza de escala internacional. Esto destaca la necesidad de actuar en cuestiones de ciberseguridad en cuatro niveles distintos: internacional, nacional, sector privado e individual, siendo los tres primeros los primordiales en la protección de las infraestructuras críticas. Para que la colaboración entre el gobierno y el sector privado sea provechosa, la confianza entre ellos es esencial y debe abordar cuestiones tales como qué información compartir, cómo se compartirá, y qué uso se le dará.

La colaboración entre los participantes del gobierno y del sector privado también es fundamental en las fases de respuesta y recuperación de un incidente, ya que es aquí, cuando se habla del concepto de ciber-resiliencia. Para entender este último, es necesario primero definir lo que se entiende por resiliencia: “una cualidad intrínseca, una característica propia de una organización que le permite enfrentarse de forma exitosa a los cambios y a los eventos tanto internos como externos”[59].

Partiendo de la definición de resiliencia, se puede explicar la ciber-resiliencia como la capacidad que posee una organización, empresa y/o Estado para enfrentar de manera eficaz cualquier amenaza procedente del ciberespacio que pueda afectar su infraestructura de tecnologías de la información y comunicación. La ciber-resiliencia es

[59] Luis de Salvador, Carrasco, *Ciber-resiliencia,* [en línea], Instituto Español de Estudios Estratégicos, Abril, 2015, p. 3. Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf. [Fecha de consulta: 3 de julio de 2017].

un enfoque inteligente de la seguridad y se trata de la administración de riesgos, no de su eliminación, ya que esta es imposible.

Dada la interdependencia entre los distintos elementos que forman las organizaciones: personal, entorno social, suministros, infraestructura TIC, procesos, etc., no se puede trazar una línea divisoria clara entre la resiliencia y la ciber-resiliencia de sus sistemas. Una y otra están íntimamente relacionadas, es más, son un mismo concepto. No se puede crear una infraestructura tecnológica ciber-resiliente si la organización en sí no es resiliente[60].

Los delincuentes cibernéticos cuentan con métodos cada vez más sofisticados por lo que encontrarán grietas incluso en los sistemas de seguridad más avanzados, la mejor defensa es anticiparse a las fallas, identificarlas tan pronto como ocurren y arreglarlas rápidamente. Para lo cual el desarrollo de las capacidades de identificación, detección, prevención, contención, recuperación, cooperación y mejora continua, frente a las distintas ciberamenazas es lo esencial.

Una organización, empresa o Estado ciber-resiliente será aquel en el que su infraestructura que depende de las tecnologías de información y comunicación (TIC), bajo cualquier circunstancia que intente dañarla o lo logre, continúe operativa con un grado de eficacia que tal vez no alcance el 100% del rendimiento deseable, pero que sí permita mantener la vida de la misma. El conjunto de las capacidades antes mencionadas y su operación en el momento adecuado permitirá a una organización, empresa o gobierno alcanzar un grado competente de ciber-resiliencia.

Los gobiernos de cada país también necesitan hablar entre sí sobre estos asuntos, tanto bilateralmente como multilateralmente para compartir experiencias y soluciones. Un foro global de este tipo son las Conferencias Meridian, las cuales se realizan en diferentes países y regiones cada año, y tienen por objetivo el intercambio de ideas y el inicio de acciones para la cooperación entre cuerpos gubernamentales sobre temas relacionados con la Protección de las Infraestructuras Críticas de la Información globalmente[61].

[60] *Ídem*.

[61] Meridian 2016, *El Proceso Meridian,* [en línea]. Dirección URL: https://www.meridian2016.mx/spanish/Paginas/inicio.aspx. [Fecha de consulta 2 de julio de 2017].

Las Conferencias Meridian buscan crear una comunidad de decisores políticos gubernamentales con experiencia en CIIP mediante la promoción de la colaboración continua. Todos los países están invitados a participar. En el año 2016 esta conferencia se llevó a cabo en la ciudad de México con la participación de más de 130 delegados de 36 países y Organizaciones Internacionales.

El resultado más importante de la Conferencia Meridian en México, fue la redacción de la "Guía de Buenas Prácticas de CIIP", la cual contiene diversas estrategias y consejos generales que son de ayuda para las naciones en cuestiones de protección y ciber-resiliencia de sus Infraestructuras Críticas de Información. En el año 2017, Meridian se llevó a cabo en Noruega a finales del mes de octubre.

Algunas otras muestras de la preocupación por proteger las infraestructuras críticas son las iniciativas de la Fundación Nacional para la Ciencia (National Science Foundation, en inglés) de los Estados Unidos, que entregó un donativo a la Universidad Cristiana de Texas para ayudarla a crear medidas efectivas que protejan los dispositivos médicos de ciberataques. Por otra parte, la Agencia Europea de Seguridad de la Información y las Redes (ENISA, por la sigla de European Union Agency for Network and Information Security en inglés) también ha enfocado su atención a la CIIP[62].

Como se pudo observar a lo largo de este apartado, las industrias que utilizan los sistemas de control como SCADA se encargan de brindar servicios esenciales para la población, se trata de sistemas que manejan información sensible y de ahí la criticidad de los riesgos y el gran impacto si alguno de ellos llegara a fallar o fuera vulnerado. Si bien se han realizado algunos cambios en muchas industrias buscando mejorar la ciberseguridad, aún falta mucho trabajo por realizar en los diferentes sectores.

Según el informe *La seguridad como rehén. Tendencias 2017* realizado por la compañía de seguridad informática *ESET*, para 2017 la tendencia probable era que los ataques a infraestructuras críticas se incrementarían si no se continuaba avanzando de forma rápida en su adecuada protección[63]. También se pronosticó el aumento de ataques a la misma infraestructura de internet interrumpiendo el acceso a datos y

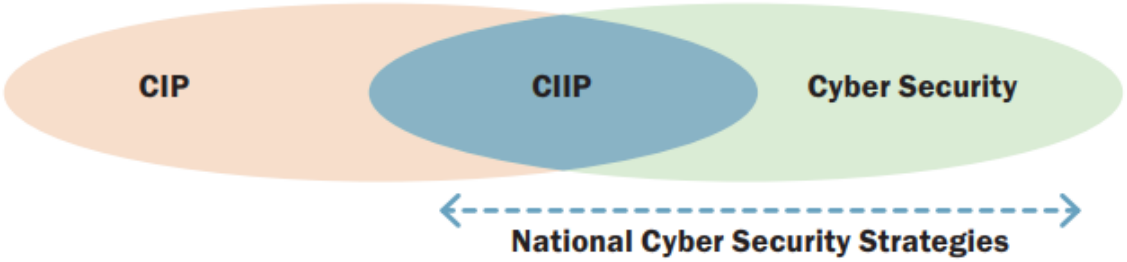
[62] ESET, *Tendencias 2016: (In) Security Everywhere,* [en línea], p. 56.Dirección URL: https://www.welivesecurity.com/la-es/2016/01/20/tendencias-2016-seguridad-parte-de-nuestras-vidas/. [Fecha de consulta: 30 de junio de 2017].

[63] ESET, *La seguridad como rehén. Tendencias 2017,* [en línea]. Dirección URL: http://www.eset-la.com/centro-prensa/articulo/2016/eset-informe-tendencias-2017-la-seguridad-como-rehen/4429. [Fecha de consulta: 1 de julio de 2017].

servicios, mismos que podrían ser vitales para el buen funcionamiento de una o más infraestructuras críticas.

A medida que la sociedad internacional se vuelve cada vez más interconectada e interdependiente superando todo tipo de fronteras, los riesgos y amenazas creados por el ciberespacio también aumentan, superando el límite de dicho dominio y siendo capaz de dañar hardware. Los Estados ahora también necesitan luchar con las implicaciones de un ataque a su infraestructura crítica que, de ocurrir, es indispensable que tengan preparada una respuesta defensiva y/u ofensiva apropiada para el mismo.

Esquema 1.2. Relación entre CIP, CIIP y Ciberseguridad



Tomado de GFCE, *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection,* [en línea], p. 8. Dirección URL: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.

1.2.3. América Latina y la ciberseguridad: protección de la infraestructura crítica.

La seguridad cibernética para la protección de las infraestructuras críticas se ha vuelto de vital importancia a la hora de crear estrategias de seguridad nacional, no siendo la excepción los países de América Latina. En respuesta al aumento de ciberataques y ciberamenazas a las infraestructuras críticas, la Organización de los Estados Americanos (OEA) desarrolló un programa regional de seguridad cibernética.

El Programa de Seguridad Cibernética de la OEA se centra en siete puntos: la participación de la sociedad civil y el sector privado; el concientizar a las personas sobre este tema; el desarrollo de estrategias nacionales; el brindar capacitación técnica y el establecimiento de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRTs, por sus siglas en inglés) nacionales; la realización de ejercicios de gestión de

crisis; misiones de asistencia técnica que generalmente culminan en recomendaciones; y en compartir información y experiencias entre los países miembros.

En el *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas* del año 2015 hecho también por la OEA, donde fueron encuestados 575 participantes, 26 de ellos funcionarios de Estados miembros y el resto organizaciones privadas que controlan infraestructuras críticas de América, se obtuvo que el 76%[64] de los mismos consideró que los incidentes cibernéticos contra dichas infraestructuras se han vuelto más sofisticados, lo que indica la necesidad de generar mejores estrategias de protección y tener una mayor eficacia en la respuesta a los mismos.

Por otro lado, el mismo reporte indica que la mayoría de los países del continente, han sufrido ataques dirigidos a sus infraestructuras críticas, seguir el mapa que lo muestra:

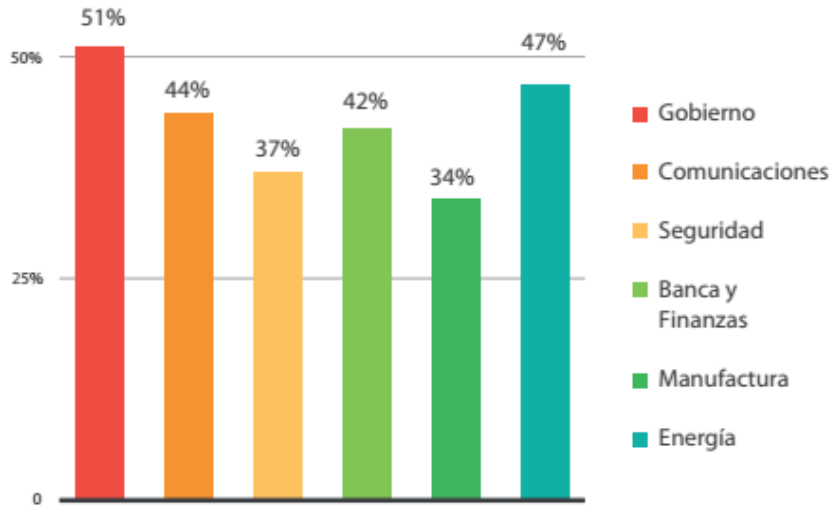
Mapa 1.2. Países que han experimentado ciberataques en diferentes sectores de infraestructuras críticas.

Tomado de OEA, Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, 2015, p. 26.

[64] OEA, *Op. Cit.*, p. 24.

Asimismo, el reporte indicó que los sectores más atacados son el gubernamental con un 51%, seguido por el de energía con el 47% y el de comunicaciones con el 44% como se puede observar en la siguiente gráfica.

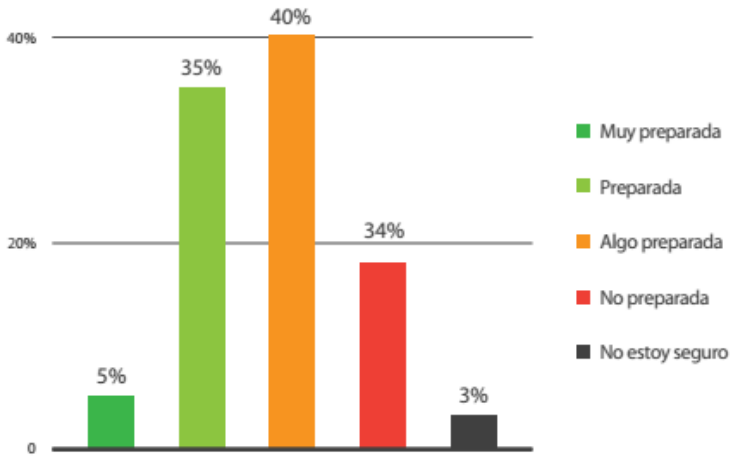
Gráfica 1.1. Infraestructuras críticas que sufren mayor cantidad de ciberataques.



Tomada de OEA, Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, 2015, p. 25.

También, se les preguntó a los participantes qué tan preparados se sentían en caso de que ocurriera un incidente cibernético, a lo cual sólo un 40% respondió que “algo preparado” y un 35% que “preparado”. Sin embargo, un 34% respondió que no se sentía preparado, lo que deja a la vista la falta de estrategias de protección o la falta de madurez de las mismas.

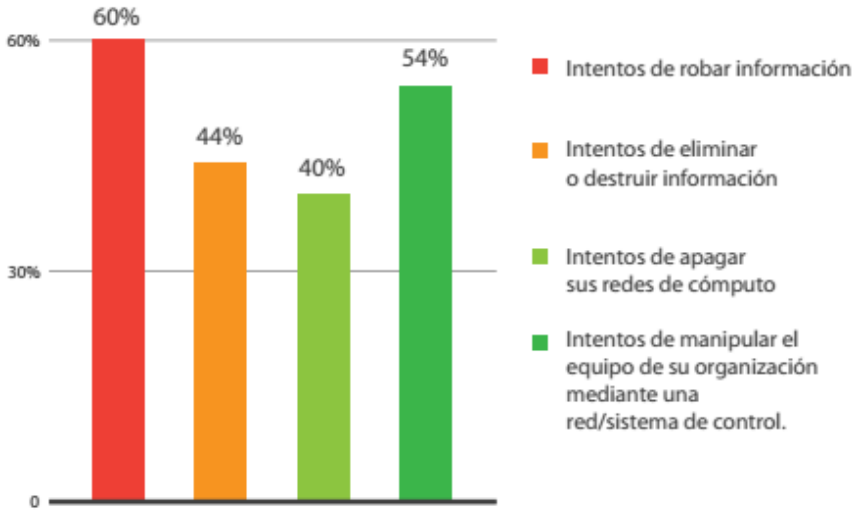
Gráfica 1.2. ¿Qué tan preparados se sienten en caso de un ciberataque?



Tomada de OEA, Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, 2015, p. 25.

Como se sabe, los que llevan a cabo los ataques cibernéticos lo hacen con diversos fines. Los siguientes fueron los más comunes según los encuestados en el reporte:

Gráfica 1.3. ¿Qué fines han tenido los ataques cibernéticos sufridos?

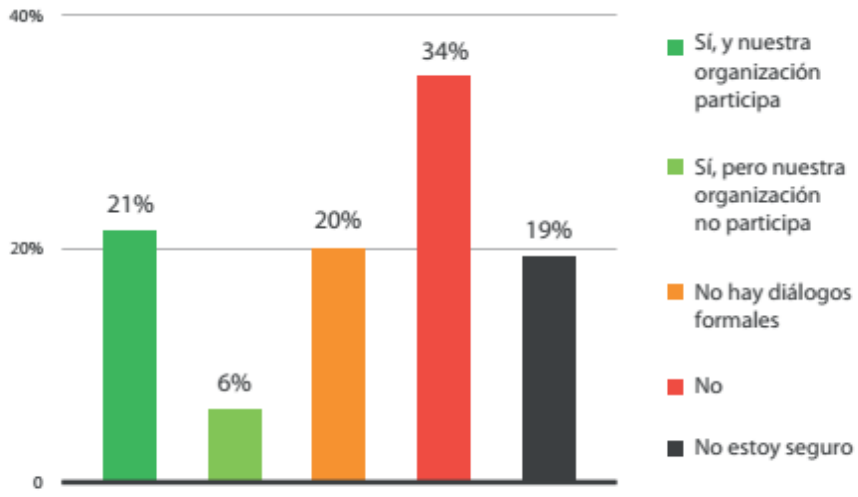


Tomada de OEA, Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, 2015, p. 50.

En diversos apartados de esta investigación, se ha mencionado que la cooperación Estado-Empresas privadas es esencial para la protección de

infraestructuras críticas debido a que la mayoría de estas son controladas por organizaciones no estatales. Es por esto, que en el reporte se preguntó si existe algún tipo de diálogo con el gobierno de cada país con respecto al tema, a lo que desafortunadamente, un 34% contestó que no, seguido de un 21% que afirmó que existen discusiones sobre ello pero que su empresa no colabora en ellas.

Gráfica 1.4. ¿Existe algún tipo de diálogo de su organización con el gobierno acerca de los incidentes cibernéticos que sufren las infraestructuras críticas?



Tomada de OEA, Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, 2015, p. 53.

Los datos anteriores son alarmantes, y no hacen más que reflejar lo mucho que falta por avanzar en la región en cuestiones de ciberseguridad. No obstante, hay que recordar que esta encuesta fue realizada a principios del año 2015, y para el año siguiente, ya 17 países de América Latina contaban con un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés o también conocidos como CERT), encargados de actuar de acuerdo con los procedimientos y políticas predefinidos para responder rápida y eficazmente a los incidentes de seguridad y para reducir el riesgo de ataques cibernéticos[65].

[65] OEA; BID, *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?,* Informe Ciberseguridad 2016, p. 13.

Mapa 1.3. Equipos de Respuesta ante Incidentes de Seguridad Informática en América Latina.

Tomado de OEA; BID, *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?*, Informe Ciberseguridad 2016, p. 13.

La mayoría de estos equipos de respuesta aún se encuentran en etapas iniciales. Según el reporte elaborado en 2016 por la OEA y el BID titulado *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* cuatro de cada cinco países de dicha región no tienen estrategias de ciberseguridad o planes de protección de infraestructura crítica y dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética[66].

[66] OEA; BID, *Op. Cit.,* p. IX.

Es por lo anterior que los países miembros de la Organización de Estados Americanos han desarrollado a lo largo de los años diversos instrumentos y estrategias en materia de seguridad cibernética, entre ellas se encuentra la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética, creada en el año 2004 con el fin de luchar contra las amenazas cibernéticas en el hemisferio y proporcionar un marco inicial para cultivar y guiar tal enfoque.

Los esfuerzos por desarrollar marcos legales integrales para combatir los delitos cibernéticos no han sido menores, y aunque sólo dos de los 32 Estados miembros de la OEA, la República Dominicana y Panamá (hasta finales del año 2016)[67], se han adherido al Convenio de Budapest sobre el Delito Cibernético, la mayoría de ellos han aumentado sus esfuerzos para la aplicación de leyes a nivel nacional que castiguen dichos delitos.

Los compromisos en América Latina en cuestiones de ciberseguridad han ido en aumento y se han reafirmado y fortalecido con los años a partir de la adopción de numerosas declaraciones oficiales, a través de la OEA, en promoción de la seguridad cibernética, la lucha contra la delincuencia informática y la protección de infraestructuras de información crítica. La creación de los ya mencionados Equipos de Respuesta ante Incidentes de Seguridad Informática ha sido uno de los mayores logros en conjunto.

Es así, como el panorama en América Latina se vuelve cada vez más alentador en cuestiones de seguridad cibernética y de ciber-resiliencia, pues éstas ocupan un lugar destacado en las agendas de seguridad nacional y en los programas sociales. Si bien ningún país está protegido por completo cibernéticamente, muchos comienzan a tomar medidas significativas para evaluar sus desafíos específicos sobre todo en términos económicos y de infraestructura, para lograr sus objetivos. Aunque sigue habiendo brechas entre ellos, como lo demuestran diversos estudios realizados por la OEA, como el de *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?* en el que se muestran las capacidades y los esfuerzos de seguridad cibernética de cada país, la región entera está avanzando y madurando en su compromiso con la creación de una sociedad conectada, ciber-resiliente y por consiguiente, más segura.

[67] A pesar de las numerosas invitaciones que le ha hecho la Unión Europea a los países de América Latina para unirse al Convenio de Budapest, las respuestas no han sido las más satisfactorias, pues muchos de ellos se han quedado a la mitad del proceso de adhesión debido a las numerosas modificaciones y a la creación de instituciones necesarias que ello implica, entre ellos, México es el claro ejemplo.

II. La ciberseguridad como estrategia de seguridad nacional en Estados Unidos.

> No nos disculparemos por nuestra forma de vida, ni dudaremos en su defensa. Y para aquellos que buscan avanzar en sus objetivos induciendo el terror y matando inocentes, les decimos ahora que nuestro espíritu es más fuerte y no se puede romper: no pueden superarnos**, y los derrotaremos**.
>
> -Presidente Barack Obama, Discurso inaugural, 20 de enero de 2009.

2.1. Aspectos fundamentales del origen y evolución de la estrategia de seguridad nacional de Estados Unidos.

La necesidad de articular un sistema de seguridad nacional de Estados Unidos surgiría después de la Segunda Guerra Mundial. En el año 1947 el presidente Harry Truman promulgó el Acta de Seguridad Nacional mediante la cual se dio una importante reorganización de la política exterior y los establecimientos militares del gobierno de los Estados Unidos que en términos generales, continúa vigente hoy en día. La ley creó el Consejo de Seguridad Nacional (NSC por sus siglas en inglés), el Departamento de Defensa (fusionando el Departamento de Guerra y el Departamento de la Marina) y la Agencia Central de Inteligencia (CIA, también por sus siglas en inglés).

El Consejo de Seguridad Nacional incluía al Presidente, el Vicepresidente, el Secretario de Estado, el Secretario de Defensa y a otros miembros como el Director de la CIA, quienes en conjunto debatían con respecto a la integración de las políticas nacionales, extranjeras y militares relacionadas con la seguridad nacional. Es relevante destacar que esta Ley no define el concepto de lo que implica la *seguridad nacional*, sino sólo que la finalidad del Consejo es resguardarla. Asimismo, se estableció que un pequeño grupo parte del NSC coordinaría los asuntos de política exterior de otros organismos para el Presidente. A partir de 1953, el Asistente del Presidente para Asuntos de Seguridad Nacional dirigió este personal[69].

[69] Department of State, *National Security Act of 1947,* [en línea], Office of the Historian. Dirección URL: https://history.state.gov/milestones/1945-1952/national-security-act. [Fecha de consulta: 11 de julio de 2017].

Por otra parte, la CIA surgió de la Oficina de Servicios Estratégicos de la Segunda Guerra Mundial y pequeñas organizaciones de inteligencia de posguerra. Mientras que el Departamento de Defensa quedó bajo el mandato del Secretario de Defensa, quien también dirigió el recién creado Departamento de la Fuerza Aérea, sin embargo, cada una de las tres ramas mantuvo sus propias secretarías de servicio. En 1949 el Acta sufrió una enmienda para dar al Secretario de Defensa más poder sobre los servicios individuales y sus secretarios.

Cada presidente ha concedido al Consejo de Seguridad Nacional diferentes grados de importancia y ha dado al personal del mismo, niveles variables de autonomía e influencia sobre otros organismos tales como los Departamentos de Estado y Defensa. El presidente Dwight Eisenhower (1953-1961) por ejemplo, continuó con el proceso de institucionalización y lo utilizó como vehículo central para la formulación y promulgación de políticas.

En la etapa en que Eisenhower deja la presidencia para ser asumida por John F. Kennedy (1961-1963) y, posteriormente, por Lyndon B. Johnson (1963-1969), el sistema del NSC había empezado a ser objeto de críticas, al ser excesivamente burocratizado. Ambos prefirieron los esquemas informales y el control personal con su círculo interno diluyendo la institucionalidad del Consejo.

Bajo el presidente Richard M. Nixon se reconstruye el sistema formal del Consejo de Seguridad Nacional bajo el mandato de Henry Kissinger, poniéndolo en el centro de la elaboración de la política exterior. Nixon y Kissinger tenían como objetivo asegurar el control presidencial y la conducción de la política exterior por lo que establecieron la autoridad en la toma de decisiones en la Casa Blanca[70], lo que ocasionó que las reuniones del Consejo sólo sirvieran para confirmar las decisiones ya acordadas por ambos con anticipación.

Gerald Ford (1974-1977) en su periodo presidencial decide dejar a Kissinger como Asistente para Asuntos de Seguridad Nacional pero a su vez, lo nombra Secretario de Estado, decisión que generó fuertes críticas por la excesiva concentración de poder en manos de un solo individuo, situación que quiso cambiar al nombrar a Brent

[70] Emersson, Forigua Rojas, *El Consejo de Seguridad Nacional de Estados Unidos: evolución, organización y lecciones,* [en línea], Papel Político, vol. 17, núm. 1, enero-junio, 2012, p. 250. Dirección URL: http://www.redalyc.org/articulo.oa?id=77724876009. [Fecha de consulta: 11 de julio de 2017].

Scowcroft como asistente. Cuando Jimmy Carter llega a la presidencia (1977-1981), empezó por evitar la concentración del poder de la política exterior en las manos de un solo individuo, preservando el rol de la Casa Blanca en la coordinación de la burocracia de la política exterior.

Asimismo, Carter procedió a reelaborar la estructura del NSC, dividiéndolo en dos comités. Por un lado, un Comité de Revisión de Política responsable de los proyectos de largo plazo y que estaba dirigido por un gabinete conformado por los miembros de los departamentos involucrados en el tema; y por otro, un Comité Especial de Coordinación responsable de los proyectos de corto plazo incluyendo operaciones de inteligencia encubierta y la gestión de crisis, dirigido por el Asistente para Asuntos de Seguridad Nacional[71].

Carter deja un sistema con debilidades, pero en funcionamiento, que será tomado por el nuevo presidente de Estados Unidos, Ronald Reagan (1981-1989), quien opta por utilizar como principal herramienta de su gestión al gabinete, apoyándose principalmente en los secretarios de los departamentos. Por lo tanto, se establecieron altos grupos interdepartamentales en defensa, exteriores e inteligencia y una serie de grupos interdepartamentales al nivel de asistentes de secretario y presididos por los principales responsables de cada agencia[72].

Posteriormente, se estableció el Grupo de Planeamiento para la Seguridad Nacional con el propósito de fortalecer la planeación y la coordinación de políticas, estando conformado por los miembros constitutivos del NSC según el Acta de 1947 y reuniéndose periódicamente con el presidente Reagan[73]. La incapacidad para construir un esquema organizacional que direccionara el sistema y garantizara su funcionamiento de acuerdo con los objetivos de la administración fue el problema principal de la administración Reagan.

Antes de que Reagan dejara la presidencia, se creó la Ley Goldwater-Nichols, también conocida como Acta de Reorganización del Departamento de Defensa de 1986[74], misma que obligó al Presidente a presentar una Estrategia de Seguridad

[71] *Ibídem,* p. 252.
[72] *Ibídem,* p. 253.
[73] *Ibídem,* p. 254.
[74] Esta Ley además como su nombre lo dice, reorganizó el Departamento de Defensa. La autoridad operacional de las diversas instituciones militares dejó de estar en manos de los Jefes de Estado Mayor institucionales (Ejército, Armada,

Nacional anual al Congreso. El objetivo era contar con "un documento de planificación político-estratégico en el que se encontraran de manera explícita los intereses globales, metas y objetivos vitales para la seguridad nacional estadounidense"[75].

No obstante, desde la presidencia de Harry S. Truman ya se delineaban las estrategias de seguridad nacional a seguir para la contención del socialismo. El documento NSC-68 titulado *Objetivos y Programas para la Seguridad Nacional de los Estados Unidos* fue un informe secreto elaborado por el personal de Planificación de Políticas del Departamento de Estado de Estados Unidos el 7 de abril de 1950. El memorándum de 58 páginas figura entre los documentos más influyentes que hizo el gobierno estadounidense durante la Guerra Fría y no fue desclasificado hasta 1975[76].

Entre las posibles líneas de acción del documento NSC-68 se encontraban el retorno al aislacionismo, la guerra, el continuar con esfuerzos diplomáticos para negociar con los soviéticos o "la rápida construcción de la fuerza política, económica y militar del mundo libre"[77]. Se concluyó que la única manera de disuadir a la Unión Soviética era la acumulación masiva de armas tanto convencionales como nucleares, recomendación que se siguió y aunque el NSC-68 no hizo ninguna mención específica con respecto al aumento de los gastos de defensa, la administración de Truman casi triplicó el gasto en defensa como porcentaje del PIB entre 1950 y 1953 (del 5% al 14.2%)[78].

Cuando la Guerra Fría estaba por llegar a su fin George H. Bush (1989-1993) obtiene la presidencia y busca un sistema centralizado conformado por tres componentes. En la parte superior, estaba el Comité de Directores (Principals Committee) presidido por el NSC, los secretarios de Estado y Defensa, el director de la CIA, el jefe del Estado Mayor y el fiscal general o el secretario del Tesoro cuando eran

---

Fuerza Área) y se centralizó en el Jefe de Estado Mayor de las Fuerzas Armadas. Este último, también fue designado como el principal asesor militar del presidente de Estados Unidos, del Secretario de Defensa y del Consejo de Seguridad Nacional.
Además, el Acta creó la posición de Subjefe de Estado Mayor y definió la línea de mando del presidente en su calidad de Comandante en Jefe con los diversos Comandantes de Comandos Operativos, pasando por la autoridad administrativa del Secretario de Defensa.

[75] Griffiths, Spielman John, *Teoría de la Seguridad y Defensa en el continente Americano. Análisis de los casos de EE.UU. de América, Perú y Chile,* [en línea], RiL Editores, Chile, 2011, p. 277. Dirección URL: https://books.google.com.mx/books?id=LnAMhN7NXcIC&pg=PA277&lpg=PA277&dq=Acta+Goldwater-Nichols&source=bl&ots=yqBh5insQy&sig=jgIdaMDEjK8MejXSEQAonulizQ4&hl=es419&sa=X&ved=0ahUKEwjympzXpoTVAhWE7SYKHbsCDBwQ6AEIZjAJ#v=onepage&q=Acta%20Goldwater-Nichols&f=false. [Fecha de consulta: 11 de julio de 2017].

[76] Department of State, *NSC-68, 1950,* [en línea], Office of the Historian. Dirección URL: https://history.state.gov/milestones/1945-1952/NSC68. [Fecha de consulta: 11 de julio de 2017].

[77] *Ídem.*

[78] *Ídem.*

requeridos. Este Comité se encargaba de revisar, coordinar y monitorear el desarrollo e implementación de la política de seguridad nacional.

Luego se encontraba el Comité de Suplentes (Deputies Committee), precedido por el suplente del Asistente para Asuntos de Seguridad Nacional y conformado por personal del nivel de subsecretarios. Este Comité era el responsable de preparar las cuestiones de política, papeles, documentos y recomendaciones para el Comité de Directores. El último componente eran los Comités de Coordinación de Políticas (Policy Coordinating Committees), conformados por ocho comités regionales y funcionales, siendo estos los responsables del desarrollo inicial de las opciones de política y de la vigilancia en su implementación.

En noviembre de 1992 William Jefferson Clinton, mejor conocido como Bill Clinton, ganó las elecciones a George H. Bush y asumió la presidencia de Estados Unidos en enero del siguiente año. Su discurso inaugural reflejaba los numerosos cambios por los que la sociedad internacional estaba pasando.

> [...] Cuando nuestros fundadores declararon la indepen-dencia de América ante el mundo y nuestros propósitos ante el Todopoderoso, sabían que América, para poder durar, iba a tener que cambiar. No se trata de un cam-bio por el cambio, sino de un cambio para preservarlos ideales de América: la vida, la libertad, la búsqueda de la felicidad. Aunque marchemos al compás que nos marca el tiempo en que vivimos, nuestra misión es eterna.
>
> [...] Hoy, una generación que ha crecido a la sombra de la Guerra Fría asume nuevas responsabilidades en un mundo calentado por el sol de la libertad, pero amenazado aún por antiguos odios y nuevas plagas.
>
> [...] Nuestra democracia debe ser no sólo la envidia del mundo, sino el motor de nuestra renovación. No hay nada malo en América que no pueda curarse a través de lo que en América va bien.
>
> Y así, en el día de hoy, con este juramento, una época de deriva, un callejón sin salida termina, y una nueva época de la renovación americana comienza.
>
> [...] Para renovar América debemos responder a los desafíos que tenemos planteados tanto en el exterior como en el interior. Ya no existe división entre lo que es exterior y lo que es interior, la economía es mundial, el medioambiente es mundial, la crisis del sida es mundial, la carrera de armamentos es mundial, y nos afec-ta a todos.
>
> Hoy, cuando un viejo orden desaparece, el mundo nuevo que surge es más libre, pero menos estable. El desmoronamiento del comunismo ha dado nueva vida a antiguas animosidades y nuevos peligros. Sin lugar a dudas, América debe seguir liderando el mundo que tanto hizo por construir.

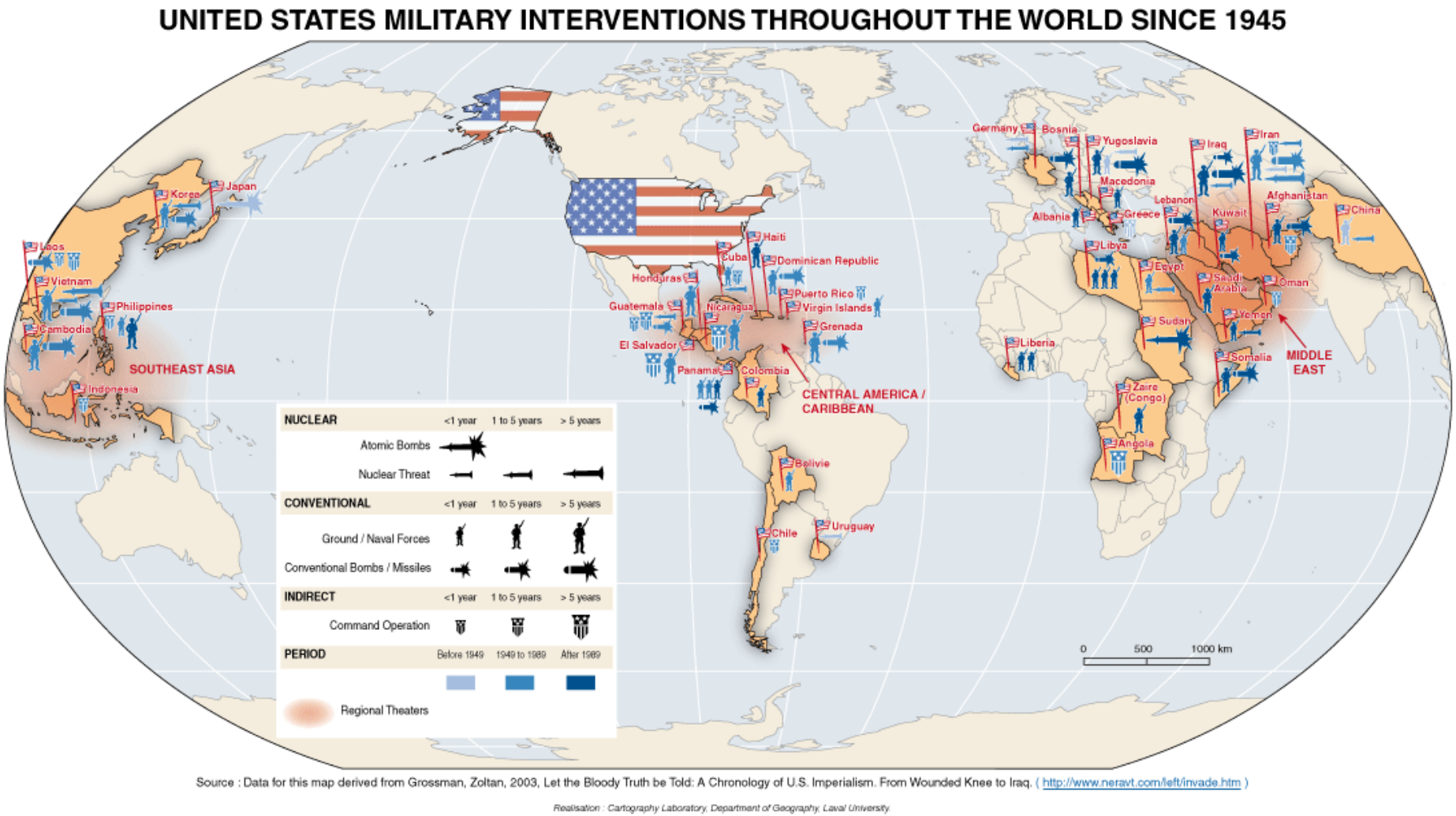
> [...] Cuando nuestros intereses vitales sean puestos en peligro o se desafíe la voluntad y la conciencia de la comunidad internacional, actuaremos mediante la fuerza de la diplomacia siempre que sea posible y con la fuer-za cuando sea necesario. Los valientes norteamericanos que hoy sirven a nuestra nación en el golfo Pérsico, en Somalia y en cualquier otro lugar en que se hallen, dan testimonio de nuestra determinación.
>
> Pero nuestra mayor fuerza es el poder de nuestras ideas, que aún son nuevas en muchas tierras. En todo el mundo vemos cómo las abrazan y nos llena de regocijo. Nuestras esperanzas, nuestros corazones, nues-tras manos están con aquellos que en cada continente fortalecen la democracia y la libertad. Su causa es la causa de América [...][79].

Clinton entró en la Casa Blanca con tropas estadounidenses desplegadas por todo el mundo: en enero de ese año Bush había ordenado la entrada de soldados estadounidenses en Somalia; la Marina y la Guardia Costera habían comenzado una cuarentena de Haití; y la Fuerza Aérea estadounidense recientemente había bombardeado estaciones de radar iraquíes[80]. Además de estas operaciones militares, Clinton enfrentó una serie de desafíos urgentes de política exterior: la crisis constitucional rusa, la guerra de Bosnia, Corea del Norte estaba desarrollando armas nucleares y el proceso de paz en Medio Oriente se encontraba en un punto muerto.

[79] Discursos para la historia, *El discurso inaugural de Bill Clinton,* [en línea]. Dirección URL: https://discursosparalahistoria.wordpress.com/2010/03/26/el-discurso-inaugural-de-bill-clinton/. [Fecha de consulta: 12 de julio de 2017].

[80] Véase mapa 2.1.

Mapa 2.1. Intervenciones militares de Estados Unidos alrededor del mundo desde 1945 hasta 2003.



Source : Data for this map derived from Grossman, Zoltan, 2003, Let the Bloody Truth be Told: A Chronology of U.S. Imperialism. From Wounded Knee to Iraq. (http://www.neravt.com/left/invade.htm)

Realisation : Cartography Laboratory, Department of Geography, Laval University

Obtenido de Global Research, *World Conquest: The United States' Global Military Crusade (1945-),* [en línea]. Dirección URL: http://www.globalresearch.ca/the-united-states-global-military-crusade-1945/4610.

De esta manera, con el fin de la Guerra Fría y la desaparición de la amenaza comunista, Clinton pretendía iniciar una nueva etapa en la que Estados Unidos dejaba en claro su pretensión de liderar el mundo y de difundir sus valores como los ideales a seguir. Esto iría acompañado de siete estrategias de seguridad nacional, la primera de ellas en 1994 llamada *Estrategia de Seguridad Nacional de Compromiso y Ampliación* (National Security Strategy of Engagement and Enlargement). Después, en febrero de 1995 y 1996 saldrían dos documentos más con el mismo nombre.

Es importante destacar que estas estrategias no dan un concepto definido de manera explícita de lo que es la seguridad nacional, no obstante, al referirse a ella, Clinton engloba a los estadounidenses, a la forma de vida de los mismos (el conocido *American way of life*) y al territorio. Las tres primeras estrategias de seguridad nacional eran en esencia lo mismo, sólo se cambiaron o agregaron algunos temas. Éstas destacaron los conflictos étnicos, la proliferación de armas de destrucción masiva, el terrorismo, el tráfico de drogas y la degradación ambiental a gran escala exacerbada por el rápido crecimiento de la población, como las principales amenazas a la seguridad.

Además, se agregó el término de *Estados bribón* (Rogue States, en inglés) para describir aquellas naciones no democráticas que ponían en peligro la estabilidad política en muchas regiones del mundo. Los objetivos centrales de estas estrategias se resumían en tres puntos[81]:

1. Sostener nuestra seguridad con fuerzas militares que estén listas para la lucha y con una representación efectiva en el extranjero.
2. Fortalecer la revitalización económica de los Estados Unidos.
3. Promover la democracia en el extranjero.

Entre otros temas también se encontraban el Tratado de Libre Comercio de América del Norte, la cooperación económica con Asia Pacífico, la Ronda de Uruguay del Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT, por sus siglas en inglés), la expansión del libre comercio, la promoción de la democracia, seguridad energética y las acciones a seguir en regiones como Europa, África, Medio Oriente y Asia. En la Estrategia de Seguridad Nacional de Compromiso y Ampliación de febrero de

[81] National Security Strategy Archive, *A National Security Strategy of Engagement and Enlargement,* [en línea], 1994. Dirección URL: http://nssarchive.us/national-security-strategy-01994/. [Fecha de consulta: 12 de julio de 2017].

1996, se incluyó un apartado sobre la preparación de las instituciones económicas internacionales para el siglo XXI[82].

Las siguientes tres estrategias de la administración de Bill Clinton llevaron por nombre *Estrategia de Seguridad Nacional para un Nuevo Siglo* (National Security Strategy for a New Century) publicadas en los años 1997, 1998 y 2000. Estas estrategias comenzaron a hablar ya de la globalización, definiéndola como el proceso que acelera la integración económica, tecnológica, cultural y política, hecho que significó que Estados Unidos se vería afectado por eventos más allá de sus fronteras.

Las primeras dos estrategias (1997 y 1998) clasificaron las amenazas a los intereses de Estados Unidos en las siguientes categorías[83]:

- Amenazas regionales o centradas en el Estado: Incluye Estados que tienen las capacidades y el deseo para amenazar intereses vitales, ya sea mediante la coerción o la agresión transfronteriza. En muchos casos, estos Estados se están esforzando por obtener armas nucleares, biológicas o químicas.
- Amenazas transnacionales: Terrorismo internacional, delincuencia, tráfico de drogas, tráfico ilícito de armas, migraciones incontroladas de refugiados y el daño ambiental.
- Difusión de tecnologías peligrosas: armas de destrucción masiva.
- Servicios de Inteligencia extranjeros: La rápida adopción de nuevas tecnologías y métodos innovadores por parte de algunos servicios de inteligencia extranjeros

[82] Por iniciativa del Presidente Clinton en la Cumbre Económica de Nápoles en 1994, el G-7 emprendió una intensa revisión de las instituciones financieras y económicas internacionales para considerar cómo prepararlas para el siglo XXI. En la cumbre del año siguiente en Halifax, Canadá, el G-7 propuso una serie de reformas e iniciativas importantes. Estos incluyen medidas para mejorar la capacidad para prevenir y mitigar las crisis financieras internacionales; la creación de un sistema de alerta temprana y prevención más eficaz, con énfasis en una mejor divulgación de los datos financieros y económicos; el establecimiento de un nuevo Mecanismo de Financiamiento de Emergencia para proporcionar los medios para una respuesta internacional rápida a las crisis con implicaciones sistémicas; e instituir una revisión de los procedimientos que podrían facilitar la resolución ordenada de las crisis de deuda internacional en un entorno financiero caracterizado por una mayor diversidad de acreedores e instrumentos financieros.
En este contexto, no hay que olvidar que a finales del año 1994 e inicios de 1995 México además de pasar por una crisis política debido al asesinato del principal candidato presidencial, Luis Donaldo Colosio, del levantamiento del EZLN y del sufriría una crisis económica. El llamado "efecto tequila" o "error de diciembre" provocó un ambiente de desconfianza e incertidumbre afectado a otros países de la región como Argentina. Para poder recuperarse de esta crisis, Estados Unidos y el FMI tuvieron que intervenir para Al llamado "Efecto tequila" se le consideró como la primer crisis de las economías globalizadas pues sus repercusiones impactaron a varios países latinoamericanos.

[83] National Security Strategy Archive, *A National Security Strategy for a New Century,* [en línea], 1998. Dirección URL: http://nssarchive.us/NSSR/1998.pdf. [Fecha de consulta: 13 de julio de 2017].

para obtener información secreta. Se incluyen los intentos de penetrar sistemas informáticos y redes para acceder a información sensible.

- Estados fallidos: Estados que no tienen un gobierno estable y no pueden proporcionar servicios básicos y oportunidades para sus poblaciones generando conflictos internos, crisis humanitarias o inestabilidad regional.

Es destacable que en la Estrategia de Seguridad Nacional para un Nuevo Siglo de 1998, por primera vez se incluyó la protección a las infraestructuras críticas, tema que se ahondará en el punto 2.3 de este capítulo. Asimismo, ya se habla de la posibilidad de un ciberataque aunque no es definido con ese término.

Por otra parte, la Estrategia de Seguridad Nacional para un Nuevo Siglo del año 2000, destaca la preparación de Estados Unidos para el nuevo siglo, sin embargo, las amenazas a su seguridad nacional no cambian con respecto a las estrategias anteriores. Sucede lo mismo con los objetivos que aunque en esencia son lo mismo, se agrega la promoción de los derechos humanos universales:

- Mejorar la seguridad de los Estados Unidos.
- Fortalecer la prosperidad económica de Estados Unidos.
- Promover la democracia y los derechos humanos en el extranjero.

Asimismo, en dicha estrategia y en la *Estrategia de Seguridad Nacional para una Era Global* del año 2001 (A National Security Strategy for a Global Age) se establecen tres categorías para diferenciar los intereses nacionales de Estados Unidos[84]:

- Intereses vitales: Son aquellos de una importancia amplia y primordial para la supervivencia, la seguridad y la vitalidad de la nación. Es decir, la seguridad física del territorio y la de los aliados, la seguridad de los ciudadanos, el bienestar económico de la sociedad y la protección de las infraestructuras críticas de un ataque paralizante.
- Intereses nacionales importantes: Estos intereses no afectan la supervivencia de la nación pero afectan el bienestar nacional y el carácter del mundo. Incluyen las regiones en las que se tiene un interés económico considerable o compromisos con los aliados, la protección del medio ambiente y la gestión de crisis con un potencial para generar flujos de refugiados sustanciales y desestabilizadores.

[84] *Ibídem,* 2000.

- Intereses humanitarios y de otro tipo: La respuesta a los desastres naturales o provocados por el hombre, promover los derechos humanos y tratar de poner fin a las graves violaciones de esos derechos, apoyar la democratización, la adhesión al estado de Derecho, el control civil de los militares y promover el desarrollo sostenible.

El futuro de la seguridad nacional de Estados Unidos daría un giro tras el ataque terrorista a las Torres Gemelas en Nueva York el once de septiembre de 2001, también conocido como el 11-S. Por primera vez el propio territorio estadounidense había sido el objetivo de estos ataques, apareciendo como consecuencia una sensación de inseguridad desconocida hasta la fecha. Días después del atentado el entonces presidente George W. Bush, dio un discurso en el que dejaba clara la posición y el papel que tomaría Estados Unidos desde ese momento:

> […] Los estadounidenses se están preguntando: ¿por qué nos odian? Ellos odian lo que ven aquí en esta Cámara: un gobierno democráticamente elegido. Sus líderes son nombrados por ellos mismos. Ellos nos odian por nuestras libertades: nuestra libertad de religión, nuestra libertad de expresión, nuestra libertad de votar y congregarnos y de estar en desacuerdo entre nosotros.
>
> […] Pedimos a todas las naciones que se unan a nosotros. Pediremos y necesitaremos la ayuda de fuerzas de policía, servicios de inteligencia y sistemas bancarios de todo el mundo. […] Quizás la carta de la OTAN refleja mejor la actitud del mundo: un ataque contra uno es un ataque contra todos. El mundo civilizado se está alineando junto a Estados Unidos. Ellos comprenden que si este terror queda sin castigo, sus propias ciudades, sus propios ciudadanos podrían ser los próximos.
>
> […] Se nos ha hecho gran daño. Hemos sufrido una gran pérdida. Y en nuestro dolor y en nuestra ira, hemos encontrado nuestra misión y nuestro momento. La libertad y el temor están en guerra. El avance de la libertad humana, el gran logro de nuestro tiempo y la gran esperanza de cada era, depende ahora de nosotros[85].

En este y todos los discursos que dio después del 11 de septiembre, se mostraba un mundo dividido entre el bien y el mal. Se hablaba de una sola moralidad que debía regir para todos. George W. Bush creó un posicionamiento del discurso sobre la seguridad internacional y el terrorismo, el uso político de conceptos teológicos y las

[85] Filosofía, *Jorge Bush: Discurso en el Capitolio*, [en línea]. Dirección URL: http://www.filosofia.org/his/20010921.htm. [Fecha de consulta: 2 de diciembre de 2016].

referencias constantes a una clase de moral que sirvió de base para la definición y posicionamiento de un nuevo enemigo, la división del mundo entre los amantes de la libertad y los tiranos.

Bush que al iniciar su gobierno había sido fuertemente criticado por no contar con una agenda que le diera rumbo al país, inició una guerra contra el terrorismo que incluía bases y lineamientos para la política interior y la exterior. Esto no sólo le sirvió para legitimarse, sino que además, se vio un claro fortalecimiento de la solidaridad, unión y nacionalismo de la población estadounidense.

Fue así como el mandatario lanzó la Estrategia de Seguridad Nacional de Estados Unidos del año 2002, sin ningún otro nombre, como lo había hecho su antecesor. Los objetivos de la misma serían[86]:

- Defender la dignidad humana.
- Fortalecer las alianzas para derrotar al terrorismo global y trabajar para prevenir los ataques contra EE.UU. y sus aliados.
- Trabajar con otros para desactivar los conflictos regionales.
- Evitar las amenazas de enemigos hacia Estados Unidos y sus amigos/aliados con armas de destrucción masiva.
- Comenzar una nueva era de crecimiento económico mundial mediante mercados libres.
- Ampliar el círculo del desarrollo abriendo sociedades y construyendo la infraestructura de la democracia.
- Desarrollar agendas de acción cooperativa con otros centros principales de poder global.
- Transformar las instituciones de seguridad nacional de Estados Unidos para hacer frente a los desafíos y oportunidades del siglo XXI.

También, esta administración propuso la mayor reorganización gubernamental desde que el presidente Truman creó el Consejo de Seguridad Nacional y el Departamento de Defensa. La creación del Departamento de Seguridad Nacional (Department of Homeland Security) y la Ley Patriótica (USA Patriot Act)[87] fueron algunas

[86] National Security Strategy Archive, *The National Security Strategy of the United States,* [en línea], 2002. Dirección URL: http://nssarchive.us/national-security-strategy-2002/. [Fecha de consulta: 15 de julio de 2017].

[87] La Ley Patriótica fue promulgada el 26 de octubre de 2001. Esta legislación fue duramente criticada por organizaciones defensoras de las libertades civiles no sólo por permitir el espionaje telefónico masivo sin autorización judicial, sino también porque legalizó la tortura y suspendió el habeas corpus (equivalente al amparo en México) en

de las respuestas más importantes a los ataques del 11 de septiembre de 2001, cada uno de ellos con la finalidad de fortalecer la seguridad del país.

En el año 2002 quedó establecido el Departamento de Seguridad Nacional, que combinó 22 diferentes departamentos y agencias federales en una agencia unificada e integrada. Este departamento tendría una estructura organizativa clara y eficiente con cuatro divisiones:

1. Seguridad Fronteriza y de Transporte.
2. Preparación y Respuesta ante Emergencias.
3. Contramedidas químicas, biológicas, radiológicas y nucleares.
4. Análisis de la Información y Protección de la Infraestructura.

El Departamento de Seguridad Nacional se creó con la finalidad de garantizar una *patria* segura y resiliente contra el terrorismo y otros peligros. En la actualidad y de una forma más específica, tiene como misión prevenir el terrorismo y mejorar la seguridad; asegurar y administrar las fronteras; aplicar y administrar las leyes de inmigración; proteger el ciberespacio; y asegurar la resiliencia a los desastres[88].

En febrero de 2003 se lanzó la Estrategia Nacional para Combatir el Terrorismo y un año después por recomendación de la Comisión Nacional de Ataques Terroristas a los Estados Unidos[89], se dio una gran reforma a la Comunidad de Inteligencia[90]. Se creó el puesto de Director de Inteligencia Nacional, un nuevo Centro Nacional de Contraterrorismo (National Counterterrorism Center) y un Centro Nacional de Contraproliferación (National Counterproliferation Center) para gestionar y coordinar la planificación y actividades en esas áreas críticas.

Hoy en día, el Centro Nacional de Contraterrorismo produce análisis, mantiene la base de datos autorizada de terroristas conocidos y sospechosos, comparte información

---

investigaciones sobre terrorismo. Cuando el Presidente Bush firmó la Ley Patriótica tenía algunas estipulaciones permanentes y provisionales. Las estipulaciones provisionales expirarían después de cierto tiempo a menos que fueran renovadas por el Congreso. En el año 2005 ante la lluvia de críticas y la enorme presión popular que generó la revelación de Snowden dos años atrás, el entonces presidente Barack Obama aceptó modificar algunos puntos de dicha Ley y negoció con la oposición republicana la creación de la Ley de Libertades.

[88] Department of Homeland Security, *About DHS,* [en línea]. Dirección URL: https://www.dhs.gov/about-dhs. [Fecha de consulta: 15 de julio de 2017].

[89] También conocida como la Comisión 9-11, fue una comisión independiente, bipartidista creada por la legislación del Congreso y la firma del Presidente George W. Bush a finales de 2002. Tuvo como misión preparar un reporte completo de las circunstancias que rodearon los ataques terroristas del 11 de septiembre de 2001. Una vez que la Comisión hizo público su informe final en julio de 2004, fue cerrada el 21 de agosto del mismo año.

[90] Estos cambios están sustentados en la Reforma de Inteligencia y la Ley de Prevención del Terrorismo de 2004 (Intelligence Reform and Terrorism Prevention Act (IRTPA)).

y lleva a cabo una planificación operativa estratégica. Mientras que el Centro Nacional de Contraproliferación previene la proliferación de armas de destrucción masiva, sus sistemas de entrega, tecnologías y conocimientos especializados relacionados. Todos estos logros se mencionaron en la Estrategia de Seguridad Nacional del año 2006.

Cuatro años después, en 2010, se publicó la siguiente Estrategia de Seguridad Nacional en la que se incluyó por primera vez el tema de ciberseguridad. Desde que Barack Obama llegó a la presidencia de Estados Unidos se le conoció como el "ícono 2.0" por haber obtenido resultados bastante favorables a partir del uso de nuevos medios como las redes sociales durante su campaña hacia la presidencia. Obama utilizó la llamada política 2.0, misma que está definida como "la aplicación de valores profundamente democráticos a la relación entre los políticos y los ciudadanos aprovechando las capacidades que la red pone en nuestras manos"[91].

Mientras otros candidatos construían sus *websites* y posteaban vídeos en *Youtube*, el equipo demócrata creó un programa definido que pretendía acercarse a sus electores, involucrándolos no sólo con la información que ellos querían escuchar, sino con actividades mucho más comprometidas como la aportación de fondos para el financiamiento de la campaña. Se estima que a través de las redes sociales Obama recaudó 3.1 millones de dólares[92].

La población a través de las redes sociales expuso sus preferencias, creencias, situación laboral, entre otros datos, mismos que fueron utilizados con maestría y sirvieron para ejercer un control ideológico y político sobre los electores influenciando directamente en su decisión a la hora de votar. Obama reconocería que así como los grandes avances tecnológicos le habían permitido llegar a la presidencia, también podría significar la aparición de una enorme cantidad de riesgos no sólo para los ciudadanos sino para la nación, de ahí su decisión de incluir de manera oficial el tema de ciberseguridad en la Estrategia de Seguridad Nacional del año 2010.

Empero, si bien se puede decir que durante la administración de Obama fue la primera vez que apareció de manera formal el tema de ciberseguridad en una estrategia de seguridad nacional, hay que recordar que nunca se puso a un lado por el gobierno

[91] Lucas, Lanza; Natalia, Fidel, *Política 2.0 y la comunicación en tiempos modernos*, [en línea], Centro de Estudios en Diseño y Comunicación, 2011, p. 59. Dirección URL: http://www.scielo.org.ar/pdf/ccedce/n35/n35a06.pdf. [Fecha de consulta: 4 de julio de 2017].
[92] *Ídem.*

estadounidense pues desde la aparición del Gusano Morris ya se habían tomado medidas como la creación del Equipo de Respuesta ante Emergencias Informáticas para atender futuros ataques informáticos.

De hecho, a principios del año 2000, las redes del Gobierno Federal comenzaron a experimentar un alarmante número de infracciones cibernéticas. En respuesta, el Congreso creó el Centro Federal de Respuesta a Incidentes Informáticos (FedCIRC, en inglés) y con la creación del Departamento de Seguridad Nacional en 2002, el Congreso transfirió estas responsabilidades al mismo[93].

En 2003, FedCIRC pasó a llamarse *US-CERT* (Equipo de Respuesta ante Emergencias Informáticas de Estados Unidos), y su misión se amplió para incluir la protección de límites para el dominio ejecutivo civil federal y el liderazgo en seguridad cibernética[94]. Hoy en día el US-CERT trabaja en conjunto con el gobierno federal, empresas privadas y Organizaciones Internacionales para responder a incidentes importantes, analizar amenazas e intercambiar información de seguridad cibernética.

En todo el mundo, Estados Unidos ha estado en la vanguardia del desarrollo de la política y estrategia de seguridad cibernética. También en el año 2003, el gobierno estadounidense publicó la primera *Estrategia Nacional para Asegurar el Ciberespacio* como un complemento a la *Estrategia Nacional para la Protección Física de Infraestructuras Críticas y Activos Clave*[95] y con el fin de proporcionar dirección a los departamentos del gobierno federal y agencias que tienen roles en seguridad del ciberespacio.

Esta estrategia identifica pasos que gobiernos estatales y locales, empresas privadas, organizaciones y los ciudadanos estadounidenses pueden tomar para mejorar la ciberseguridad a un nivel nacional. Los objetivos de esta *Estrategia Nacional para Asegurar el Ciberespacio* son[96]:

- Prevenir los ataques cibernéticos contra Infraestructuras críticas;
- Reducir la vulnerabilidad nacional a ataques; y

[93] US-CERT, *About Us,* [en línea]. Dirección URL:https://www.us-cert.gov/about-us. [Fecha de consulta: 16 de julio de 2017].
[94] *Ídem.*
[95] Se hablará de esta estrategia más a fondo en el punto 2.3 de este capítulo.
[96] US-CERT, *The National Strategy to Secure Cyberspace,* [en línea], 2003. Dirección URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. [Fecha de consulta: 17 de julio de 2017].

- Minimizar los daños y el tiempo de recuperación de ataques cibernéticos que sí ocurren.

Además, articula cinco prioridades nacionales que incluyen[97]:

I. Un Sistema Nacional de Respuesta de Seguridad en el Ciberespacio;

II. Un Programa Nacional de Seguridad para la Reducción de la Vulnerabilidad y las Amenazas en el Ciberespacio;

III. Un Programa Nacional de Sensibilidad y Capacitación en Seguridad del Ciberespacio;

IV. Asegurar el ciberespacio de los gobiernos; y

V. La protección de la Seguridad Nacional y la Cooperación Internacional para la Seguridad en el Ciberespacio.

La primera prioridad se centra en mejorar la respuesta del gobierno estadounidense a incidentes cibernéticos y reducir el daño potencial de tales eventos. La segunda, tercera y cuarta prioridades tienen como objetivo reducir las amenazas y las vulnerabilidades a los ataques cibernéticos. La quinta prioridad es prevenir los ciberataques que puedan afectar los activos de seguridad nacional y mejorar la gestión internacional y la respuesta a esos ataques.

Por otra parte, en el año 2006 el Departamento de Defensa publicó la *Estrategia Militar Nacional para las Operaciones del Ciberespacio* (National Military Strategy for Cyberspace Operations (NMS-CO)) que tenía como fin asegurar la superioridad militar de los EE.UU. en el ciberespacio. El NMS-CO establece "un marco estratégico militar que orienta y enfoca la acción del Departamento de Defensa en las áreas de operaciones militares, de inteligencia y de negocios en/y a través del ciberespacio"[98].

Como se puede observar, si bien la *Estrategia de Seguridad Nacional de 2010* fue la primera estrategia de seguridad nacional de Estados Unidos dedicada a prestar atención sustancial a las amenazas cibernéticas, el tema nunca fue relegado. También, el tema de ciberseguridad en esta estrategia representó un cambio en la caracterización de las amenazas cibernéticas por parte del gobierno federal con énfasis en el terrorismo pero además con una preocupación económica en el ámbito cibernético.

[97] *Ídem.*

[98] NSA Archive, *National Military Strategy for Cyberspace Operations*, [en línea], 2006. Dirección URL: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf. [Fecha de consulta: 16 de julio de 2017].

La Revisión Cuadrienal de la Seguridad Nacional de 2010[99] identificó el "Salvaguardar y asegurar el ciberespacio" como una de las cinco misiones prioritarias para la seguridad nacional de Estados Unidos. Las otras misiones consistían en la prevención del terrorismo y aumento de la seguridad, el asegurar y gestionar las fronteras, la aplicación y administración de las leyes de inmigración y el garantizar la resiliencia a los desastres. Además se mostraron las que se consideraban como las principales amenazas:

Tabla 2.1. Amenazas, Peligros y Retos y Tendencias Globales a Largo Plazo.

Amenazas y peligros	Desafíos globales y tendencias
➔ Armas de destrucción masiva de alta consecuencia ➔ Al-Qaeda y el extremismo violento global ➔ Ciberataques, invasiones, interrupciones y explotaciones de alta consecuencia y/o gran escala ➔ Pandemias, accidentes graves y peligros naturales ➔ Tráfico ilícito y delincuencia transnacional ➔ Terrorismo de menor escala	➔ Inestabilidad económica y financiera ➔ Dependencia de los combustibles fósiles y las amenazas del cambio climático global ➔ Naciones que no quieren respetar las normas internacionales ➔ Tecnología sofisticada y ampliamente disponible ➔ Otros conductores de movimientos ilícitos, peligrosos o incontrolados de personas y bienes

Tabla obtenida de Department of Homeland Security, *Quadrennial Homeland Security Review,* [en línea], 2010. Dirección URL: https://www.dhs.gov/sites/default/files/publications/2010-qhsr-executive-summary.pdf. Traducción propia.

Dentro de la misión de salvaguardar y asegurar el ciberespacio se encontraban los siguientes objetivos[100]:

- ❑ Comprender y priorizar las amenazas cibernéticas: Identificar y evaluar las amenazas más peligrosas para las redes federales civiles y del sector privado y la nación.
- ❑ Gestionar los riesgos para el ciberespacio: Proteger y hacer sistemas de información resistentes, redes y datos personales y sensibles.

[99] La Revisión Cuadrienal de la Seguridad de la Patria (Quadrennial Homeland Security Review) es un documento de la estrategia principal del Departamento de Seguridad Nacional, que se actualiza cada cuatro años. El informe ofrece recomendaciones sobre la estrategia a largo plazo y las prioridades para la seguridad nacional. Cada ciclo de QHSR implica un extenso proceso de revisión de tres años de duración antes de que el informe finalice y se presente al Congreso. El Departamento de Seguridad Nacional se esfuerza por hacer que el QHSR sea lo más completo e inclusivo posible trabajando con una amplia gama de partes interesadas dentro y fuera del gobierno, que comparten la responsabilidad de salvaguardar la nación. El QHSR de 2018 será presentado al Congreso en diciembre de 2017.

[100] Department of Homeland Security, *Quadrennial Homeland Security Review,* [en línea], 2010. Dirección URL: https://www.dhs.gov/publication/2010-quadrennial-homeland-security-review-qhsr#. [Fecha de consulta: 17 de julio de 2017].

- ❑ Prevenir el delito cibernético y otros usos maliciosos del ciberespacio: Interrumpir las organizaciones criminales y otros actores maliciosos involucrados en delitos cibernéticos de alta o gran escala.
- ❑ Desarrollar una sólida capacidad de respuesta de incidentes cibernéticos entre los sectores público y privado: Gestionar los incidentes cibernéticos de la identificación a la resolución de manera rápida y replicable con una acción rápida y apropiada.

En el mismo año se creó el Cibercomando de Estados Unidos (United States Cyber Command (USCYBERCOM)) bajo el mando del Comando Estratégico. Este Cibercomando planea, coordina, integra, sincroniza y realiza actividades para dirigir las operaciones y la defensa de determinadas redes de información del Departamento de Defensa; prepara y dirige operaciones ciberespaciales militares de espectro completo para permitir acciones en todos los dominios y así garantizar la libertad de acción de los EE.UU. y sus aliados en el ciberespacio[101].

El USCYBERCOM tiene tres áreas de enfoque principales: Defender el Departamento de Defensa al interior, proporcionar apoyo a los comandantes combatientes para la ejecución de sus misiones en todo el mundo, y fortalecer la capacidad de la nación para resistir y responder a los ataques cibernéticos. El Comando unifica la dirección de las operaciones del ciberespacio, fortalece las capacidades del ciberespacio del DoD, e integra y refuerza la experiencia cibernética del DoD. También trabaja estrechamente con socios interinstitucionales e internacionales en la ejecución de estas misiones críticas.

Entre sus elementos de servicio están el Comando Cibernético del Ejército (ARCYBER), el Comando Cibernético de la Flota (FLTCYBER), el Comando Cibernético de la Fuerza Aérea (AFCYBER) y el Comando Cibernético de las Fuerzas Marítimas (MARFORCYBER). El Comando Cibernético de la Guardia Costera (CGCYBER), aunque subordinado al Departamento de Seguridad Nacional, tiene una relación de apoyo directo con el USCYBERCOM[102].

Para el año 2011, el presidente Barack Obama lanzó la *Estrategia Internacional para el Ciberespacio: Prosperidad, Seguridad y Apertura en un Mundo en Red* (International

[101] U.S. Strategic Command, *U.S. Cyber Command (USCYBERCOM),* [en línea]. Dirección URL: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/. [Fecha de consulta: 17 de julio de 2017].
[102] *Ídem.*

Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World), que es considerada como una hoja de ruta que permite a los departamentos y agencias del gobierno de los Estados Unidos definir y coordinar mejor su papel en la política internacional del ciberespacio.

En ella, se reconoce que el rápido crecimiento de las redes trajo consigo nuevos desafíos para la seguridad nacional y económica y la de la sociedad internacional. Estos desafíos se presentan en una variedad de formas: los desastres naturales, los accidentes o el sabotaje pueden interrumpir los cables, los servidores y las redes inalámbricas en tierra de los EE.UU.; los desafíos técnicos también pueden causar daños, ya que el método de bloqueo de un sitio web puede convertirse en una interrupción de red internacional mucho mayor[103].

Los riesgos tanto a nivel de la seguridad personal de los ciudadanos hasta la seguridad económica de la nación como el robo de la propiedad intelectual por ejemplo, van en aumento. El anonimato y los bajos costos de entrada al ciberespacio son circunstancias que permiten que éste sea un refugio seguro para los delincuentes, las amenazas de la seguridad cibernética pueden incluso poner en peligro la paz y la seguridad internacionales de manera más amplia, a medida que las formas tradicionales de conflicto se extienden al ciberespacio.

En esta *Estrategia Internacional para el Ciberespacio: Prosperidad, Seguridad y Apertura en un Mundo en Red*, se reconoce abiertamente que Estados Unidos promoverá, junto con otras naciones, un comportamiento responsable y se opondrá a quienes busquen interrumpir redes y sistemas, y va a disuadir y a frenar a actores maliciosos reservándose el derecho a defender los bienes nacionales vitales cuando sea necesario y apropiado[104].

El gobierno de Estados Unidos también en dicha estrategia propone tres enfoques que considera como los centrales en sus esfuerzos internacionales por mantener un ciberespacio seguro: la diplomacia, la defensa y el desarrollo.

---

[103] White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World,* [en línea], 2011, p. 4. Dirección URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. [Fecha de consulta: 18 de julio de 2017].

[104] *Ibídem,* p. 12.

Esquema 2.1. Áreas prioritarias para mantener un ciberespacio seguro.

Elaboración propia con información de White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World,* [en línea], 2011, p. 11. Dirección URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

En la diplomacia Estados Unidos pretende un fortalecimiento de las alianzas tanto con otros Estados, como con Organizaciones Internacionales y el sector privado para generar un consenso de las estrategias a seguir para lograr un ciberespacio abierto, interoperable, seguro y confiable. En cuanto a la defensa, el gobierno declara el uso de todos los medios necesarios, diplomáticos, informativos, militares y económicos, según sea apropiado y consistente con el derecho internacional aplicable para defender a la nación, a sus aliados, socios e intereses.

Y en el desarrollo hace referencia a que Estados Unidos "facilitará la creación de capacidad cibernética en el extranjero, de manera bilateral y por conducto de organizaciones multilaterales, para que cada país cuente con los medios para proteger su infraestructura digital, fortalecer las redes mundiales y establecer asociaciones más estrechas en el consenso para una cooperación abierta, interoperable, segura y fiable de las redes"[105].

Asimismo, se establecen algunas prioridades en diferentes áreas, mismas que se encuentran detalladas a continuación:

[105] *Ibídem,* p. 14.

Tabla 2.2. Objetivos de Estados Unidos en su Estrategia Internacional para el Ciberespacio.

Objetivos de Estados Unidos	
Economía: Promoción de estándares internacionales y mercados innovadores y abiertos.	Sostener un entorno de libre comercio que fomente la innovación tecnológica en redes accesibles y globalmente vinculadas. Proteger la propiedad intelectual, incluidos los secretos comerciales, contra el robo. Asegurar la primacía de normas técnicas interoperables y seguras, determinadas por expertos técnicos.
Protegiendo nuestras redes: Mejorando la seguridad, la confiabilidad y la resistencia.	Promover la cooperación ciberespacial, en particular sobre las normas de comportamiento de los Estados y la seguridad cibernética, en forma bilateral y en una serie de organizaciones multilaterales y asociaciones multinacionales. Reducir las intrusiones y las interrupciones de las redes de Estados Unidos. Garantizar una sólida capacidad de gestión de incidentes, resiliencia y recuperación para la infraestructura de información. Mejorar la seguridad de la cadena de suministro de alta tecnología, en consulta con la industria.
Aplicación de la ley: extender la colaboración y el estado de derecho.	Participar plenamente en el desarrollo de la política internacional de cibercrimen. Armonizar las leyes de cibercrimen internacionalmente mediante la ampliación de la adhesión al Convenio de Budapest. Enfocar las leyes de cibercrimen en la lucha contra las actividades ilegales, no restringiendo el acceso a internet. Negar a los terroristas ya otros delincuentes la capacidad de explotar Internet para la planificación operativa, el financiamiento o los ataques.
Militares: preparándose para desafíos de seguridad del siglo XXI.	Reconocer y adaptarse a la creciente necesidad de redes confiables y seguras de los militares. Construir y mejorar las alianzas militares existentes para enfrentar las amenazas potenciales en el ciberespacio. Ampliar la cooperación ciberespacial con aliados y socios para aumentar la seguridad colectiva.
Gobernanza de Internet: Promoviendo Estructuras Efectivas e Inclusivas.	Priorizar la apertura y la innovación en internet. Preservar la seguridad y la estabilidad de la red global, incluido el sistema de nombres de dominio (DNS). Promover y mejorar los espacios de múltiples partes interesadas para la discusión de temas de gobernanza de internet.
Desarrollo Internacional: Fortalecimiento de	Proporcionar los conocimientos, la capacitación y otros recursos necesarios a los países que buscan crear capacidad técnica y de ciberseguridad. Desarrollar y compartir regularmente las mejores prácticas internacionales de seguridad cibernética. Mejorar la capacidad de los Estados para combatir la ciberdelincuencia -incluyendo capacitación para la

Capacidad, Seguridad y Prosperidad.	aplicación de la ley, especialistas forenses, juristas y legisladores. Desarrollar relaciones con los encargados de formular políticas para mejorar la creación de capacidad técnica, proporcionando un contacto regular y permanente con los expertos y sus homólogos del gobierno de los Estados Unidos.
Libertad de Internet: Apoyo a las libertades fundamentales y la privacidad.	Apoyar a los actores de la sociedad civil en el logro de plataformas seguras para las libertades de expresión y asociación. Colaborar con la sociedad civil y las organizaciones no gubernamentales para establecer salvaguardas que protejan su actividad en Internet de intrusiones digitales ilegales. Fomentar la cooperación internacional para proteger eficazmente la privacidad de los datos comerciales. Asegurar la interoperabilidad de extremo a extremo de un internet accesible para todos.

Elaboración propia con información de White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World,* [en línea], 2011. Dirección URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

El Departamento de Defensa por su parte difundió la Estrategia para la Operación en el Ciberespacio del 2011, en el que se exponían cinco iniciativas estratégicas[106]:

1. Tratar el ciberespacio como un dominio operativo para organizar, entrenar y equipar a las fuerzas armadas estadounidenses para que el Departamento de Defensa pueda aprovechar al máximo el potencial del ciberespacio.
2. Emplear nuevos conceptos operativos de defensa para proteger las redes y sistemas del DoD.
3. Asociarse con otros departamentos y agencias del gobierno de los Estados Unidos y con el sector privado para permitir una estrategia de ciberseguridad integral.
4. Construir relaciones sólidas con los aliados de EE.UU. y socios internacionales para fortalecer la ciberseguridad colectiva.
5. Aprovechar el ingenio de la nación a través de una fuerza laboral cibernética excepcional y una rápida innovación tecnológica.

En la siguiente Revisión Cuadrienal de Seguridad Nacional de 2014 se dio a conocer la continuación de los esfuerzos para hacer frente al creciente número de amenazas cibernéticas tanto a infraestructuras públicas como privadas. Además, se

[106] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,* [en línea], 2011. Dirección URL: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. [Fecha de consulta: 16 de julio de 2017].

expresó que se continuaría con la investigación, el desarrollo y el despliegue rápido de soluciones y servicios de ciberseguridad para tratar de seguir el mismo ritmo de evolución de las amenazas cibernéticas.

De la misma manera se tomaron en cuenta los temas de la aplicación de la ley cibernética, la respuesta a incidentes y la capacidad de informar mediante el aumento de las investigaciones sobre delitos cibernéticos, el compartir información sobre tácticas y métodos de ciberdelincuentes y asegurando que los incidentes se denuncien a cualquier departamento federal de Estados Unidos.

La siguiente tabla, también expuesta en la Revisión Cuadrienal del año 2014, muestra cómo las áreas prioritarias de énfasis para salvaguardar y asegurar el ciberespacio se corresponden con las misiones de seguridad nacional.

Tabla 2.3. Áreas prioritarias de énfasis para salvaguardar y asegurar el ciberespacio que corresponden con las misiones de seguridad nacional.

Proteger y asegurar el ciberespacio					
Área prioritaria de énfasis	Prevenir el terrorismo y mejorar la seguridad	Asegurar y administrar nuestras fronteras	Aplicar y administrar nuestras leyes de inmigración	Proteger y asegurar el ciberespacio	Fortalecer la preparación nacional y la resiliencia
Fortalecer la seguridad y la resistencia de las infraestructuras críticas	✓	✓		✓	✓
Asegurar la Empresa de Tecnología de la Información del Gobierno Civil Federal	✓			✓	✓
Aplicación anticipada de la ley, respuesta a incidentes y capacidad de presentación de informes	✓	✓		✓	
Fortalecer el ecosistema				✓	✓

Tabla obtenida de Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review,* [en línea], p. 41.

Traducción propia. Dirección URL: https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

En la última Estrategia de Seguridad Nacional de Estados Unidos adoptada a principios de 2015, se reconoce el progreso de los últimos 6 años en los que se ha

recuperado de una crisis económica mundial y se han fortalecido alianzas para combatir los amenazas emergentes:

> Hoy, Estados Unidos está más fuerte y mejor posicionado para aprovechar las oportunidades de un nuevo siglo y salvaguardar nuestros intereses contra los riesgos de un mundo inseguro.
>
> [...] Ahora, en este momento crucial, seguimos enfrentando serios desafíos a nuestra seguridad nacional, aun cuando estamos trabajando para dar forma a las oportunidades de mañana. El extremismo violento y una amenaza terrorista en evolución plantean un riesgo persistente de ataques contra Estados Unidos y nuestros aliados. La escalada de los desafíos a la ciberseguridad, la agresión por parte de Rusia, los impactos acelerados del cambio climático y el brote de enfermedades infecciosas generan ansiedades sobre la seguridad global. Debemos ser claros acerca de estos y otros desafíos y reconocer que Estados Unidos tiene una capacidad única para movilizar y dirigir a la comunidad internacional para hacerles frente [...][107].

Se habla también de logros como el retiro de tropas en Medio Oriente, el apoyo a Afganistán para una transición pacífica y democrática del poder, la ayuda en desastres naturales como el terremoto en Haití, el terremoto y tsunami en Japón y el tifón en Filipinas para salvar vidas, evitar mayores daños y lograr la reconstrucción. De igual forma se habla de las acciones para evitar y detener la proliferación de armas nucleares con medidas como las sanciones internacionales aplicadas a Irán.

En el ámbito cibernético se le adjudica a Estados Unidos la responsabilidad de liderar un mundo en red ya que fue el lugar de nacimiento de internet. Por ello en esta estrategia se habla del aumento de inversión en capacidades en el ciberespacio y de inteligencia, debido a la dependencia de la economía y la seguridad de la nación de la infraestructura en red. Para asegurar estas redes se trabaja en conjunto con el sector privado y la sociedad civil.

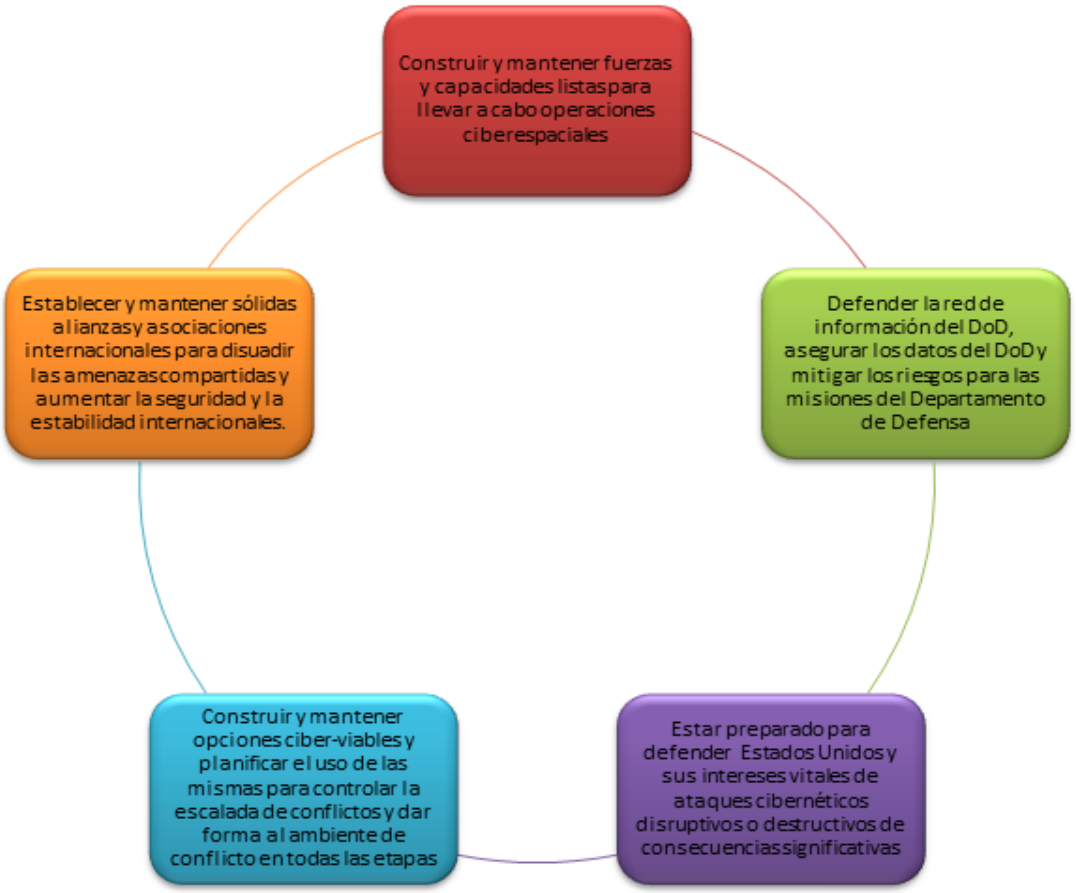
El Departamento de Defensa también en el año 2015, publicó el documento *La CiberEstrategia del Departamento de Defensa* (The DoD Cyber Strategy) que se basa en la *Estrategia para la Operación en el Ciberespacio* del 2011 y proporciona una guía

[107] National Security Strategy Archive, *National Security Strategy 2015,* [en línea]. Dirección URL: http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf. [Fecha de consulta: 18 de julio de 2017].

nueva y específica para mitigar los riesgos previstos y captar oportunidades para fortalecer la seguridad nacional de los Estados Unidos.

El DoD a partir de esta ciberestrategia establece cinco objetivos para sus misiones en el ciberespacio.

Esquema 2.2. Objetivos estratégicos del DoD para sus misiones en el ciberespacio.



Elaboración propia con información de Department of Defense, *The DoD Cyber Strategy,* [en línea], 2015. Dirección URL: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

Ésta, ha sido la última ciberestrategia presentada de manera formal por el gobierno estadounidense. Cuando Donald Trump se encontraba en su campaña presidencial el tema de la ciberseguridad sólo era tocado de una manera superficial y un tanto populista, puesto que tan pronto atacaba a Apple llamando a boicotear sus productos por no permitir el acceso a los datos de sus clientes, como atacaba a China afirmando que se dedicaban a atacar a Estados Unidos.

Cuando Donald Trump llegó a la presidencia, el Centro de Estudios Estratégicos e Internacionales (CSIS, por sus siglas en inglés) publicó una serie de recomendaciones para su administración en cuestiones de ciberseguridad. Este reporte llamado *De la conciencia a la acción. Un programa de ciberseguridad para el 45º Presidente* (From Awareness to Action. A Cybersecurity Agenda for the 45th President) pretende crear un entorno digital seguro y estable que apoye el crecimiento económico continuo, protegiendo al mismo tiempo las libertades personales y la seguridad nacional.

Según el mismo, la administración de Trump se enfrenta a cinco cuestiones principales[108]:

1. Debe decidir sobre una nueva estrategia internacional para dar cuenta de un entorno de seguridad mundial muy diferente y peligroso.
2. Debe hacer un mayor esfuerzo para reducir y controlar el delito cibernético.
3. Debe acelerar los esfuerzos para asegurar infraestructuras y servicios críticos. Como parte de esto, debe desarrollar un nuevo enfoque para asegurar las agencias y servicios gubernamentales y mejorar la autenticación de la identidad.
4. Debe identificar dónde es necesaria la participación federal en temas de recursos tales como la investigación o el desarrollo de la fuerza de trabajo, y dónde dichos esfuerzos se dejan mejor al sector privado.
5. Debe considerar cómo organizar a los Estados Unidos para defender el ciberespacio. Clarificar el papel del Departamento de Seguridad Nacional (DHS) es crucial, además debe fortalecerlo o crear una nueva agencia de ciberseguridad.

Mientras el CSIS daba estas recomendaciones, la Agencia de Seguridad Nacional en conjunto con la CIA y el FBI publicaron un informe acusando a Rusia de haber orquestado una campaña para ayudarlo a llegar a la Casa Blanca mediante la

[108] CSIS, *From Awareness to Action. A Cybersecurity Agenda for the 45th President,* [en línea]. Dirección URL: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf. [Fecha de consulta: 18 de julio de 2017].

filtración de documentos perjudiciales para la candidata demócrata, Hillary Clinton. Esta campaña de influencia, según el informe, habría sido aprobada al más alto nivel e incluyó *hackeos*, filtraciones y uso de medios de información y redes sociales pero no repercutió en el conteo de votos.

Tanto el Kremlin como el Ministerio de Exteriores ruso negaron la implicación de Rusia en los supuestos ciberataques en las elecciones en EE.UU. En medio de esta controversia surgió también el rumor de la creación de una unidad de ciberseguridad en cooperación con los rusos, no obstante el mismo Trump a través de su cuenta de *Twitter* rechazó la idea de que esto ocurriera.

Lo cierto es que ante todo esto, la única y primera acción importante de Donald Trump sobre política cibernética ha sido el firmar el once de mayo de 2017, una orden ejecutiva para el fortalecimiento de la ciberseguridad de las redes federales y la infraestructura crítica, misma que se abordará en el punto 2.3 de este capítulo.

A través de esta sección de la investigación, se ha visto la evolución de las estrategias de seguridad nacional de Estados Unidos. Muchas de ellas, no presentan cambios sustanciales de una a otra, y en esencia mantienen los mismos objetivos a menos de que haya sucedido un parteaguas en la historia como lo fue el fin de la Guerra Fría o los ataques terroristas del once de septiembre del 2001. Hoy en día, las ciberamenazas son consideradas como parte de los retos a uno de sus principales intereses nacionales, su seguridad. Véase la tabla que muestra esta evolución:

Tabla 2.4. Evolución de las Estrategias de Seguridad Nacional de Estados Unidos.

Año	Título	Presidente	Objetivos	Amenazas
1987	Estrategia de Seguridad Nacional de Estados Unidos.	Ronald Reagan	• Supervivencia de Estados Unidos como una nación libre e independiente. • Mantener la política económica internacional de EE.UU. • Contener a la Unión Soviética. • Libre mercado. • Asegurar el acceso al mar y al espacio. • Promoción de la democracia y los Derechos Humanos.	➢ Unión Soviética y el comunismo. ➢ Proliferación de armas nucleares. ➢ Terrorismo.
1988	Estrategia de Seguridad Nacional de Estados Unidos.	Ronald Reagan		
1990	Estrategia de Seguridad Nacional de Estados Unidos.	George H. W. Bush	• Supervivencia de Estados Unidos como una nación libre e independiente. • Proteger a los ciudadanos y a la nación. • Integración de la Unión Soviética al sistema internacional. • Promoción de la democracia y los valores estadounidenses. • Proporcionar estabilidad económica, política y social a Europa del Este y África. • Liderar al mundo en su camino a la paz. • Liderar el libre comercio. • Asegurar recursos naturales.	➢ Tráfico de drogas y armas convencionales y químicas. ➢ Conflictos en el "Tercer Mundo". ➢ Proliferación de armas de destrucción masiva. ➢ Transferencia de tecnologías militares a países o grupos hostiles. ➢ Crisis del Golfo.
1991	Estrategia de Seguridad Nacional de Estados Unidos.	George H. W. Bush		
1993	Estrategia de Seguridad Nacional de Estados Unidos.	George H. W. Bush		
1994	Estrategia de Seguridad Nacional de Compromiso y Ampliación.	Bill Clinton	• Proteger a los ciudadanos, el *American way of life* y a la nación. • Fortalecimiento de la democracia en el extranjero. • Mantener la seguridad a través de las fuerzas militares. • Fortalecer la revitalización económica. • Cooperación económica con Asia Pacífico, la Ronda de Uruguay del Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT) y el TLCAN. • Expansión del libre comercio. • Seguridad energética.	➢ Proliferación de armas de destrucción masiva. ➢ Terrorismo. ➢ Tráfico de drogas. ➢ Conflictos étnicos. ➢ Degradación ambiental. ➢ Estados bribón.
1995	Estrategia de Seguridad Nacional de Compromiso y Ampliación.	Bill Clinton		
1996	Estrategia de Seguridad Nacional de Compromiso y Ampliación.	Bill Clinton		

			• Preparación de las instituciones económicas internacionales para el siglo XXI.	
1997	Estrategia de Seguridad Nacional para un Nuevo Siglo.	Bill Clinton	• Proteger a los ciudadanos, el *American way of life* y a la nación. • Promoción de la democracia. • Expansión del libre comercio. • Mantener una economía sana y en crecimiento.	➢ Estados que amenazan intereses de Estados Unidos. ➢ Terrorismo. ➢ Delincuencia transnacional. ➢ Tráfico de drogas y de armas. ➢ Daño ambiental. ➢ Proliferación de armas de destrucción masiva. ➢ Adopción de nuevas tecnologías en servicios de inteligencia extranjeros. ➢ Estados fallidos.
1998	Estrategia de Seguridad Nacional para un Nuevo Siglo.	Bill Clinton	• Proteger a los ciudadanos, el *American way of life* y a la nación. • Promoción de la democracia. • Expansión del libre comercio. • Mantener una economía sana y en crecimiento. • **Protección a las infraestructuras críticas.**	➢ Estados que amenazan intereses de Estados Unidos. ➢ Terrorismo. ➢ Delincuencia transnacional. ➢ Tráfico de drogas y de armas. ➢ Daño ambiental. ➢ Proliferación de armas de destrucción masiva. ➢ Adopción de nuevas tecnologías en servicios de inteligencia extranjeros. ➢ Estados fallidos.
2000	Estrategia de Seguridad Nacional para un Nuevo Siglo.	Bill Clinton	• Proteger a los ciudadanos, el *American way of life* y a la nación. • Promoción de la democracia y de los Derechos Humanos. • Fortalecer la prosperidad económica de Estados Unidos.	➢ Terrorismo. ➢ Daño ambiental. ➢ Desastres naturales. ➢ Violaciones a los Derechos Humanos. ➢ Proliferación de armas de destrucción masiva.
2001	Estrategia de Seguridad Nacional para una Era Global.	Bill Clinton	• Proteger a los ciudadanos, el *American way of life* y a la nación. • Promover los Derechos Humanos. • Apoyar la democratización y la adhesión al estado de Derecho. • Control civil de los militares.	➢ Desastres naturales o provocados por el hombre. ➢ Terrorismo. ➢ Violaciones a los Derechos Humanos. ➢ Proliferación de armas de destrucción masiva.

			• Promover el desarrollo sostenible.	
2002	Estrategia de Seguridad Nacional de Estados Unidos.	George W. Bush	• Proteger a los ciudadanos, el *American way of life* y a la nación. • Defender la dignidad humana. • Fortalecer las alianzas para derrotar al terrorismo global y trabajar para prevenir los ataques contra EE.UU. y sus aliados. • Comenzar una nueva era de crecimiento económico mundial mediante mercados libres. • Desarrollar agendas de acción cooperativa con otros centros principales de poder global. • Transformar las instituciones de seguridad nacional de Estados Unidos para hacer frente a los desafíos y oportunidades del siglo XXI. • Protección a la infraestructura crítica.	➢ Terrorismo. ➢ Proliferación de armas de destrucción masiva. ➢ Conflictos regionales. ➢ Armas biológicas y químicas.
2006	Estrategia de Seguridad Nacional de Estados Unidos.	George W. Bush		
2010	Estrategia de Seguridad Nacional de Estados Unidos.	Barack Obama	• Proteger a los ciudadanos, el *American way of life* y a la nación. • Promoción de la democracia y de los Derechos Humanos. • Prosperidad económica. • Protección a la infraestructura crítica. • Fortalecimiento de alianzas a nivel mundial. • **Ciberseguridad. Salvaguardar y asegurar el ciberespacio.**	➢ Terrorismo: Al Qaeda. ➢ Extremismo. ➢ Migración. ➢ Desastres naturales. ➢ Proliferación de armas de destrucción masiva. ➢ Armas biológicas y químicas. ➢ Conflictos en Medio Oriente. ➢ Tráfico ilícito de drogas y delincuencia transnacional. ➢ Ciberamenazas. ➢ Disrupciones a las infraestructuras críticas.
2015	Estrategia de Seguridad Nacional de Estados Unidos.	Barack Obama	• Proteger a los ciudadanos, el *American way of life* y a la nación. (Seguridad nacional). • Promoción de la democracia y la paz mundial. • Promoción de los valores nacionales. • Prosperidad económica. • Seguridad espacial, aérea	➢ Terrorismo: Al Qaeda y Estado Islámico. ➢ Extremismo. ➢ Proliferación de armas nucleares. ➢ Disrupciones a las infraestructuras críticas. ➢ Ataques cibernéticos. ➢ Enfermedades infecciosas.

			y marítima. • Ciberseguridad. • Protección de infraestructuras críticas.	➢ Cambio climático. ➢ Estados fallidos. ➢ Corea del Norte.
2017	Estrategia de Seguridad Nacional de Estados Unidos.	Donald J. Trump	• Proteger a los ciudadanos, el *American way of life* y a la nación. (Seguridad nacional). • Promoción de la democracia y la paz. • Promoción de relaciones libres y recíprocas en lo económico. • Liderar en cuestiones de investigación, tecnología e innovación. • Avance de la influencia estadounidense. • Protección de infraestructuras críticas. • Proteger y promover los valores estadounidenses.	➢ Terrorismo: Al Qaeda y el Estado Islámico. ➢ Extremismo. ➢ Proliferación de armas de destrucción masiva. ➢ Pandemias. ➢ Migración ilegal. ➢ Organizaciones criminales transnacionales. ➢ Ciberamenazas. ➢ Corea del Norte.

Elaboración propia con información de National Security Strategy Archive, *Reports,* [en línea]. Dirección URL: http://nssarchive.us/.

La ciberseguridad es considerada como uno de los más complejos desafíos para la estabilidad interna de Estados Unidos pues las ciberamenazas ponen en riesgo la seguridad nacional, pública y hasta la económica. La infraestructura digital se vuelve la columna vertebral de las economías prósperas, de gobiernos fuertes y transparentes y de sociedades libres. Es por esto, que Estados Unidos en cada una de sus estrategias declara que enfrentará a todas aquellas personas, grupos delictivos organizados, redes terroristas y/o Estados que representen una amenaza a su seguridad nacional.

Asimismo, se destaca la intención del gobierno estadounidense de cooperar con otros países para desarrollar normas internacionales que permitan una decidida acción contra las ciberamenazas. Estas acciones tienen por objeto que el internet se gestione como una responsabilidad compartida entre los Estados, el sector privado, la sociedad civil y usuarios de internet como las principales partes interesadas.

2.2. El papel de los actores no estatales en cuestiones de ciberseguridad.

El ciberespacio es un *global common* sin fronteras que todos los actores, desde Estados hasta Organizaciones Internacionales, empresas privadas, grupos delictivos y personas comparten. Como consecuencia, la ciberseguridad se ve afectada debido a que la mayoría de las veces es extremadamente difícil identificar con precisión a los autores de un ataque o incluso su ubicación, facilitando al o a los perpetradores de los mismos enmascarar su participación o disfrazarse de otro modo como otro usuario.

Un gran número de actores estatales, privados, internacionales y otros no estatales están involucrados en la seguridad cibernética. Del mismo modo, una gran diversidad de actores participan en la generación de ciberataques. La siguiente tabla muestra las fuentes más comunes de donde pueden provenir los ciberataques.

Tabla 2.5. Fuentes de ciberamenazas.

Fuente de amenaza	Descripción de la amenaza
Estados/Gobiernos	Los servicios de inteligencia extranjeros utilizan herramientas informáticas para la reunión de información y el espionaje. Esto puede estar dirigido a otros Estados o a amenazas no estatales. Los Estados también pueden atacar a los adversarios extranjeros con fines de desinformación, desestabilización, intimidación o incluso ciberguerras a gran escala. Desde el punto de vista de la seguridad humana, los Estados también pueden constituir una amenaza a través de la captura y uso de datos personales, en algunos casos sin orden judicial o supervisión democrática adecuada.
Corporaciones	Las empresas y las corporaciones (a veces en colaboración con grupos del crimen organizado o hackers individuales) conducen al espionaje industrial y/o sabotaje. Las corporaciones también pueden amenazar los derechos humanos recolectando y analizando grandes cantidades de datos personales y, en algunos casos, compartiendo estos datos con gobiernos y otros actores privados.
Crackers[109]	Individuos que aprovechan vulnerabilidades o comprometen sistemas informáticos de manera ilegal, su objetivo es obtener algún beneficio económico o reconocimiento personal.
Hacktivistas	*Hacktivismo* se refiere a ataques motivados políticamente en páginas web o servidores de correo electrónico. Los *hacktivistas* buscan interrumpir o

[109] En el documento original se manejaba el concepto de *hackers*, sin embargo, se optó por cambiarlo por el de *cracker* debido a que existe una confusión y mal interpretación del significado del primero. Un hacker es aquella persona experta en tecnología capaz de identificar fallas o explotar vulnerabilidades de sistemas pero lo hacen con un fin académico, educativo o de investigación. Los hackers cuentan con un código de ética que no les permite utilizar sus conocimientos para causar algún daño.

	destruir sitios web para lograr objetivos políticos.
Miembros descontentos de empresas o gobiernos	Los miembros insatisfechos de empresas o gobiernos son una amenaza importante dado que su conocimiento a menudo detallado de un sistema de la víctima puede permitirles ganar el acceso sin restricciones. Pueden estar motivados para causar daño al sistema o para robar datos confidenciales. La Oficina Federal de Investigaciones (FBI) de los Estados Unidos informa que los ataques de parte de personas de dentro pueden ser dos veces más probables que los de foráneos.
Terroristas	Los terroristas buscan destruir, incapacitar o explotar infraestructuras críticas, amenazar la seguridad nacional, provocar bajas masivas, debilitar las economías y dañar la moral pública y la confianza.
Operadores de Botnet	Los operadores de *Botnet* son *hackers* que se apoderan de un gran número de ordenadores, que luego se utilizan para coordinar ataques y para distribuir esquemas de *phishing*, ataques de *spam* y malware. Los servicios de estas redes a veces se ponen a disposición en mercados subterráneos.
Phishers	Los *phishers* son individuos o grupos pequeños que usan el fraude en un intento de robar identidades o información para ganar dinero. Los *phishers* a menudo usan *spam* y *spyware/malware* para lograr sus objetivos.
Spammers	Los *spammers* son individuos u organizaciones que distribuyen correos electrónicos no solicitados (a menudo con información oculta o falsa) con el fin de vender productos, realizar esquemas de *phishing*, distribuir *spyware/malware* o para atacar a organizaciones.
Autores de spyware y malware	Las personas u organizaciones con intenciones maliciosas llevan a cabo ataques contra los usuarios produciendo y distribuyendo *spyware* y *malware*.

Tabla obtenida de Benjamin S., Buckland; Fred, Schreier; Theodor H., Winkler, *Democratic Governance Challenges of Cyber Security,* [en línea], 2015, p. 14. Traducción propia. Dirección URL: http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security.

Ante esto, los Estados y actores no estatales están por supuesto preocupados por la posibilidad de que otros Estados o actores o grupos no estatales roben, modifiquen, alteren o destruyan y pongan en peligro sus infraestructuras críticas de información y a su vez, esté amenazada su seguridad. Es por esto que la protección de las redes implica la cooperación entre los gobiernos, el sector privado, las organizaciones no gubernamentales y las organizaciones internacionales permitiendo a los actores aprovechar los recursos geográficos, tecnológicos y de conocimiento que no podrían reunir solos.

Tabla 2.6. Actores que responden a las Ciberamenazas.

Tipo	Ejemplo
Organizaciones Internacionales y Regionales	Foro de Gobernanza de Internet (IGF, por sus siglas en inglés), Unión Internacional de Telecomunicaciones (UIT), *Internet Society* (ISOC, por sus siglas en inglés), Corporación de Internet para Nombres y Números Asignados (ICANN, por sus siglas en inglés), Meridian CIIP, Grupo G8, Agencia Europea para la Seguridad de las Redes y de la Información (ENISA), OTAN, ONU.
Organizaciones No Gubernamentales	Organizaciones de derechos humanos (como la Unión Americana de Libertades Civiles, *Human Rights Watch*, Amnistía Internacional, Reporteros sin Fronteras, la Iniciativa *OpenNet*), fundaciones (como la Fundación *World Wide Web*, la Fundación *Shadowserver*), *think tanks* (como el CSIS, RAND), entre muchos otros.
Organismos de la Industria	Grupo de Trabajo *Anti-Phishing* (APWG, por sus siglas en inglés), Centro de Análisis e Investigación de Operaciones del Sistema de Nombres de Dominio (DNS-OARC, por sus siglas en inglés), Grupo de Trabajo Anti-Abuso de Mensajería (MAAWG, por sus siglas en inglés), Consejo de Investigación de Infosec Research Science (ISTSG, por sus siglas en inglés), el Grupo de Trabajo de Ingeniería de Internet (IETF), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), organismos relacionados con el transporte (especialmente seguridad aeroportuaria/control de tráfico aéreo), otros organismos relacionados con la infraestructura crítica.
Estados	Ministerios de Justicia, Equipos de Preparación para Emergencias Informáticas (CERT), oficinas de seguridad de operaciones, oficinas especializadas de seguridad cibernética.
Sector privado	Empresas especializadas en seguridad de internet, desarrolladores de *software*, fabricantes de *hardware*, proveedores de pagos en línea, servidores de correo electrónico, bancos y actores del sector financiero, actores del comercio en línea.
Individuales	Usuarios y propietarios de PC individuales

Tabla obtenida de Benjamin S., Buckland; Fred, Schreier; Theodor H., Winkler, *Democratic Governance Challenges of Cyber Security,* [en línea], 2015, p. 14. Traducción propia. Dirección URL: http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security.

2.3. Las acciones en el marco de la estrategia de ciberseguridad para la protección de la infraestructura crítica de Estados Unidos.

La *Estrategia de Seguridad Nacional para un Nuevo Siglo* de 1998 fue la primera en incluir la protección a las infraestructuras críticas, en ese mismo año el entonces presidente Bill Clinton firmó la Directiva Presidencial de Decisión 63 en la que expresa que el gobierno tomará las medidas necesarias para eliminar cualquier vulnerabilidad significativa a ataques físicos o de información sobre las infraestructuras críticas estadounidenses.

En este documento se reconoce la alta dependencia del poder militar y económico de Estados Unidos de ciertas infraestructuras críticas y de sistemas de información basados en el ciberespacio. Ahí mismo, se definen las infraestructuras críticas como aquellos sistemas físicos y cibernéticos que son esenciales para las operaciones mínimas de la economía y el gobierno. Incluyen, pero no se limitan a, telecomunicaciones, energía, banca y finanzas, transporte, sistemas de agua y servicios de emergencia tanto gubernamentales como privados[110].

Como resultado de los rápidos avances en la tecnología de la información y la necesidad de mejorar la eficiencia, estas infraestructuras se han automatizado y están cada vez más interrelacionadas. Esto a su vez ha provocado que surjan nuevas vulnerabilidades a fallas de equipos, errores humanos, ataques físicos y/o cibernéticos por lo que el gobierno de EE.UU. afirma que para enfrentarlos es necesario tomar medidas que abarquen tanto el sector público como el privado.

Asimismo, Clinton ordena al FBI la creación de un Centro Nacional de Protección de Infraestructura (National Infrastructure Protection Center (NIPC, por sus siglas en inglés)) que servirá como "una entidad nacional de evaluación de amenazas de infraestructura crítica, alerta, vulnerabilidad y aplicación de la ley"[111]. Este Centro incluye investigadores con experiencia en delitos informáticos y protección de infraestructura, así como representantes del Departamento de Defensa, la Comunidad de Inteligencia y el sector privado.

Además, se conectará electrónicamente con el resto del gobierno federal, incluidos otros centros de alerta y operaciones, así como con los centros de análisis del sector privado para proporcionar advertencias oportunas sobre las amenazas a las infraestructuras coordinando la respuesta del gobierno a un incidente, incluyendo mitigación, investigación y monitoreo de esfuerzos de reconstrucción.

En la misma decisión presidencial, se pide la creación de un *Plan Nacional de Aseguramiento de la Infraestructura* (National Infrastructure Assurance Plan) para llevar a cabo las siguientes tareas[112]:

[110] Federation of American Scientists, *Protecting America's Critical Infrastructures: PDD 63,* [en línea], 1998. Dirección URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm. [Fecha de consulta: 19 de julio de 2017].
[111] *Ídem.*
[112] *Ídem.*

1. Análisis de Vulnerabilidad: Para cada sector de la economía y cada sector del gobierno que pudiera ser un objetivo de ataque de infraestructura destinado a dañar significativamente a los Estados Unidos, habrá una evaluación inicial de vulnerabilidad seguida de actualizaciones periódicas. Según proceda, estas evaluaciones incluirán también la determinación de la infraestructura mínima indispensable en cada sector.
2. Plan de Remedio: Basado en la evaluación de la vulnerabilidad, habrá un plan de remediación recomendado. El plan identificará los plazos, la implementación, las responsabilidades y la financiación.
3. Advertencia: Se pondrá en marcha un sistema mejorado para detectar y analizar tales ataques, con la máxima participación posible del sector privado.
4. Respuesta: Se desarrollará un sistema para responder a un ataque a la infraestructura significativo mientras está en marcha, con el objetivo de aislar y minimizar el daño.
5. Reconstitución: Para diversos niveles de ataques de infraestructura exitosos, se tendrá un sistema para reconstituir las capacidades mínimas requeridas de forma rápida.
6. Educación y sensibilización: Dentro del sector público y del sector privado, habrá un programa de concientización y educación sobre la vulnerabilidad para sensibilizar a las personas sobre la importancia de la seguridad y capacitarlas en las normas de seguridad, especialmente en lo que respecta a los sistemas cibernéticos.
7. Investigación y desarrollo: La investigación y el desarrollo auspiciados por el gobierno federal en apoyo de la protección de las infraestructuras se coordinarán, se someterán a una planificación plurianual, se tendrán en cuenta las investigaciones del sector privado y se financiarán adecuadamente para minimizar las vulnerabilidades en un calendario rápido pero alcanzable.
8. Inteligencia: La Comunidad de Inteligencia desarrollará e implementará un plan para mejorar la recolección y el análisis de la amenaza extranjera a la infraestructura nacional, incluyendo, pero no limitándose a, la amenaza extranjera de la guerra cibernética/ informativa.
9. Cooperación internacional: Habrá un plan para expandir la cooperación en protección de infraestructura crítica con naciones de ideas afines y amistosas, Organizaciones Internacionales y corporaciones multinacionales.

10. Requisitos Legislativos y Presupuestarios: Habrá una evaluación de las autoridades legislativas del Poder Ejecutivo y las prioridades presupuestarias con respecto a las infraestructuras críticas, y se harán recomendaciones de mejoramiento según sea necesario.

Como resultado de lo anterior, en el año 2000 surgió el *Plan Nacional para la Protección de Sistemas de Información: Una invitación al diálogo* (National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue), el primer intento por parte de cualquier gobierno nacional de diseñar una forma de proteger su ciberespacio. En él se consideran las infraestructuras críticas como "aquellos sistemas y activos -tanto físicos como cibernéticos- tan vitales para la nación que su incapacidad o destrucción tendrían un impacto debilitante sobre la seguridad nacional, la seguridad económica nacional y/o la salud y seguridad pública nacional"[113].

Este *Plan Nacional para la Protección de Sistemas de Información* tenía tres objetivos generales:

1. Preparar y prevenir: los pasos necesarios para minimizar la posibilidad de un ataque significativo y exitoso a las redes críticas de información y construir una infraestructura que siga siendo efectiva frente a tales ataques.
2. Detectar y Responder: las acciones necesarias para identificar y evaluar un ataque de manera oportuna, y luego para contener el ataque, recuperarse de forma rápida de él y reconstituir los sistemas afectados.
3. Construir bases sólidas: las cosas que se debe hacer como nación para crear y nutrir a las personas, organizaciones, leyes y tradiciones que harán a la misma más capaz de preparar y prevenir, detectar y responder a los ataques a las redes de información crítica.

En el mismo, se identifica para cada sector de infraestructura que pudiera ser un blanco para ataques cibernéticos o físicos significativos, un único Departamento u Organismo del gobierno de Estados Unidos que fungirá como el organismo principal para el enlace; a su vez, estas agencias trabajarán con líderes y organizaciones clave del sector privado y del gobierno local y estatal:

[113] Federation of American Scientists, *National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue,* [en línea], 2000. Dirección URL: https://fas.org/irp/offdocs/pdd/CIP-plan.pdf. [Fecha de consulta: 19 de julio de 2017].

Tabla 2.7. Organización Federal para una Asociación Público-Privada para la protección de las infraestructuras críticas.

Sector de Infraestructura Crítica	Coordinador del Sector Privado	Agencia federal líder y enlace sectorial
Información y comunicaciones	Asociación de Tecnología de la Información de América; Asociación de la Industria de Telecomunicaciones; Asociación Telefónica de los Estados Unidos	Departamento de Comercio Subsecretario de Comunicaciones e Información
Bancos y finanzas	Comité de Coordinación Bancaria y Financiera	Departamento del Tesoro Subsecretario Adjunto
Suministro de agua	Asociación de Agencias Metropolitanas del Agua	Agencia de Protección Ambiental Administrador Auxiliar, Oficina de Agua
Aviación, autopistas (incluyendo camiones y sistemas de transporte inteligentes), transporte público, oleoductos, ferrocarriles y transporte marítimo	Por determinarse	Departamento de Transporte Director de la Oficina de Inteligencia y Seguridad
Servicios de policía de emergencia	Comité de Aplicación de la Ley Estatal y Local	FBI Director del Centro Nacional de Protección de Infraestructura
Servicio de bomberos de emergencia; Continuidad de los servicios gubernamentales	Asociación Nacional de Comisarios de Bomberos del Estado	Agencia Federal para el Manejo de Emergencias Academia Nacional del Fuego Directora de la Oficina de Asuntos de Seguridad Nacional
Servicios de salud pública	Por determinarse	Departamento de Salud y Servicios Humanos Secretario Adjunto
Sector Federal	/	Agencia de Servicios Generales Comisionado Auxiliar de la Oficina de Seguridad de la Información
Energía eléctrica; Producción y almacenamiento de petróleo y gas	Consejo de Confiabilidad Eléctrica de América del Norte; Consejo Nacional del Petróleo	Departamento de Energía Director de la Oficina de Seguridad y Operaciones de Emergencia

Tabla obtenida de Federation of American Scientists, *National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue,* [en línea], 2000, p. 109. Dirección URL: https://fas.org/irp/offdocs/pdd/CIP-plan.pdf. Traducción propia.

Por otro lado, en la siguiente gráfica se muestran los fondos para la protección de las infraestructuras críticas por sector, la financiación de iniciativas para comprender mejor las interdependencias entre sectores y los esfuerzos por establecer Centros de Información Compartida y Análisis.

Gráfica 2.1. Financiamiento para la Protección de la Infraestructura Crítica por sector.

Elaboración propia con datos de Federation of American Scientists, *National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue,* [en línea], 2000, p. 123. Dirección URL: https://fas.org/irp/offdocs/pdd/CIP-plan.pdf.

Es de esta manera como el entonces presidente Bill Clinton genera los primeros esfuerzos para proteger la infraestructura crítica de ataques físicos y/o cibernéticos de Estados Unidos. Más tarde con la llegada de George Bush al poder y la creación del Departamento de Seguridad Nacional a raíz del 11-S, el Centro Nacional de Protección de Infraestructura quedó bajo su dirección.

En la Ley de Seguridad Nacional de 2002, se señala al Secretario del Departamento de Seguridad nacional como el responsable de coordinar el esfuerzo nacional general para mejorar la protección de la infraestructura crítica y los recursos clave de los Estados Unidos. “El Secretario servirá como principal funcionario federal para dirigir, integrar y coordinar la implementación de esfuerzos entre los departamentos

y agencias federales, los gobiernos estatales y locales y el sector privado para proteger la infraestructura crítica y los recursos clave"[114].

Dentro del mismo departamento se crea la Oficina de Protección de la Infraestructura (IP) que dirige y coordina los programas y políticas nacionales sobre la seguridad y la resiliencia de las infraestructuras críticas y ha establecido alianzas sólidas entre el gobierno y el sector privado.

La oficina lleva a cabo y facilita evaluaciones de vulnerabilidad y consecuencias para ayudar a propietarios y operadores de infraestructuras críticas, así como a socios estatales, locales, tribales y territoriales a comprender y abordar los riesgos de la infraestructura crítica. "Proporciona información sobre amenazas y peligros emergentes para que se puedan tomar las medidas apropiadas y también ofrece herramientas y capacitación a los socios para ayudarles a manejar los riesgos de sus activos, sistemas y redes"[115].

Es hasta el siguiente año, 2003, cuando se lanza la *Estrategia Nacional para la Protección Física de Infraestructuras Críticas y Activos Clave* (National Strategy for the Physical Protection of Critical Infrastructures and Key Assets). Este documento identifica las metas y objetivos para asegurar las infraestructuras y activos vitales para la seguridad nacional, también proporciona una estructura unificadora y define roles y responsabilidades para los mismos fines.

Esta estrategia reconoce trece sectores de infraestructuras críticas: agricultura, comida, agua, salud pública, servicios de emergencia, gobierno, base industrial de defensa, información y telecomunicaciones, energía, transporte, bancos y finanzas, la industria química y materiales peligrosos, y el servicio postal y de envío. No obstante, el mismo documento no descarta que esta lista se amplíe conforme las amenazas aumentan.

Son tres los objetivos que se plantea la *Estrategia Nacional para la Protección Física de Infraestructuras Críticas y Activos Clave*. El primero es identificar y asegurar la protección de aquellos activos, sistemas y funciones que se consideran más "críticos" en

[114] DHS, *Homeland Security Act of 2002,* [en línea]. Dirección URL: https://www.dhs.gov/homeland-security-act-2002. [Fecha de consulta: 19 de julio de 2017].
[115] DHS, *Office of Infrastructure Protection,* [en línea]. Dirección URL: https://www.dhs.gov/office-infrastructure-protection. [Fecha de consulta: 19 de julio de 2017].

términos de salud pública y seguridad pública a nivel nacional, gobernabilidad, seguridad económica y nacional y confianza pública[116].

El segundo objetivo principal es asegurar la protección de las infraestructuras y los bienes que se enfrentan a una amenaza específica e inminente. Y por último, el tercero es perseguir medidas e iniciativas de colaboración para asegurar la protección de otros objetivos potenciales que puedan convertirse en atractivos para atacar a lo largo del tiempo[117].

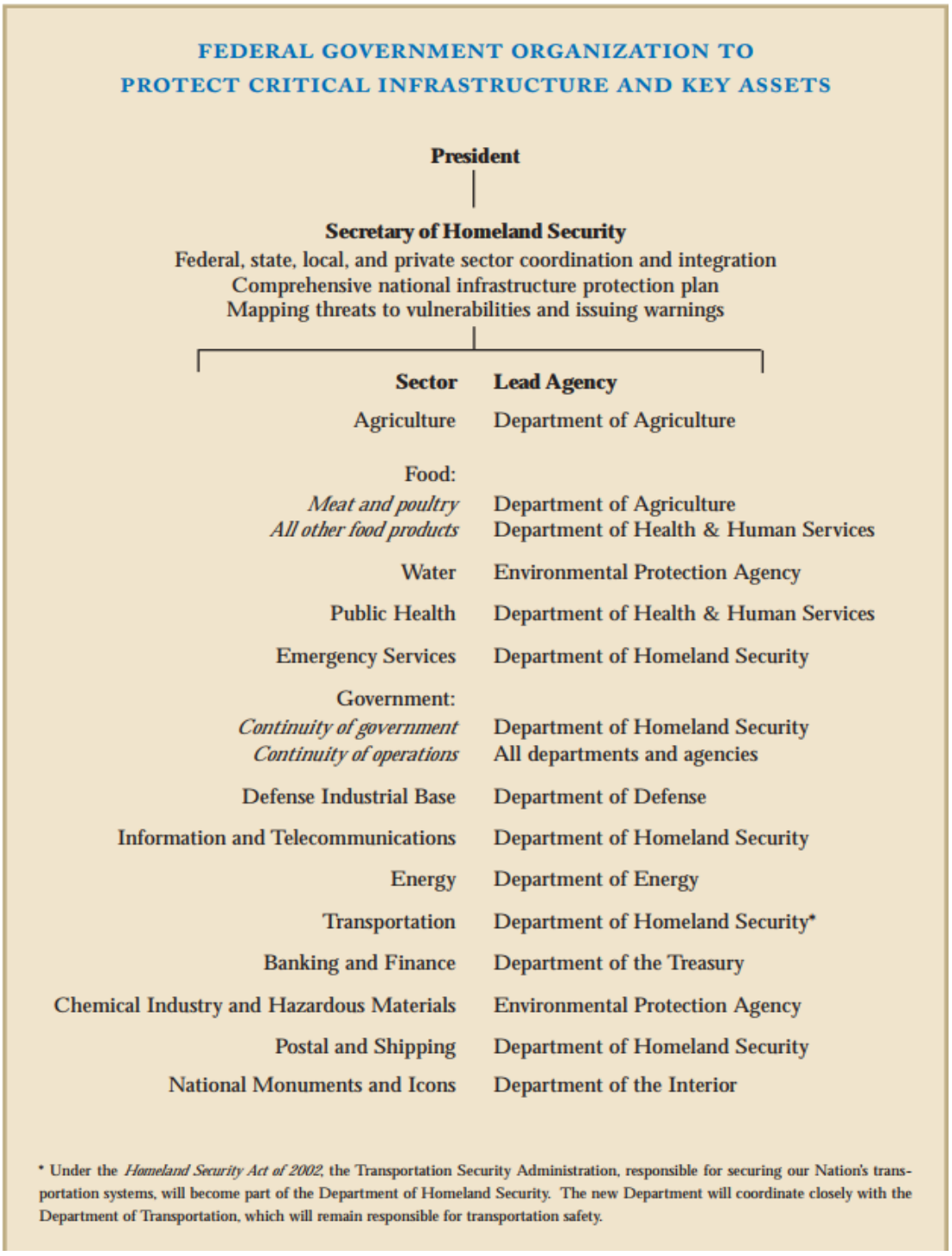
Incluso la estrategia proporciona para cada sector crítico las características únicas del propio sector y de la industria que lo apoya, los esfuerzos que están en marcha para proteger bienes y servicios específicos del sector y los activos, sistemas y funciones críticos asociados, los desafíos de protección y las áreas de acción de protección prioritaria.

Además de los sectores ya mencionados, la estrategia incluye "la protección de los activos clave, mismos que representan una amplia gama de instalaciones, sitios y estructuras únicas cuya interrupción o destrucción podría tener consecuencias significativas en múltiples dimensiones"[118]. Comprenden la diversidad de monumentos nacionales, símbolos e iconos que representan el patrimonio, las tradiciones y los valores de la nación, y el poder político. También se toman en cuenta una gran variedad de sitios y estructuras, tales como importantes atracciones históricas, monumentos, iconos culturales y centros de gobierno y comercio.

Para concluir con el análisis de esta estrategia se proporciona un esquema en el que se pueden observar cada una de las agencias y departamentos que participan en la protección de infraestructuras críticas.

[116] DHS, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* [en línea], 2003. Dirección URL:https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf. [Fecha de consulta: 20 de julio de 2017].
[117] *Ídem.*
[118] *Ídem.*

Esquema 2.3. Organización del Gobierno Federal para Proteger la Infraestructura Crítica y Activos Clave.



FEDERAL GOVERNMENT ORGANIZATION TO
PROTECT CRITICAL INFRASTRUCTURE AND KEY ASSETS

President

Secretary of Homeland Security
Federal, state, local, and private sector coordination and integration
Comprehensive national infrastructure protection plan
Mapping threats to vulnerabilities and issuing warnings

Sector	Lead Agency
Agriculture	Department of Agriculture
Food:	
Meat and poultry	Department of Agriculture
All other food products	Department of Health & Human Services
Water	Environmental Protection Agency
Public Health	Department of Health & Human Services
Emergency Services	Department of Homeland Security
Government:	
Continuity of government	Department of Homeland Security
Continuity of operations	All departments and agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy	Department of Energy
Transportation	Department of Homeland Security*
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

* Under the *Homeland Security Act of 2002*, the Transportation Security Administration, responsible for securing our Nation's transportation systems, will become part of the Department of Homeland Security. The new Department will coordinate closely with the Department of Transportation, which will remain responsible for transportation safety.

Esquema obtenido de DHS, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* [en línea], 2003, p. 18. Dirección URL:https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

En el 2009 se publica el *Plan Nacional de Protección de la Infraestructura: Asociarse para mejorar la protección y la resiliencia* (National Infrastructure Protection Plan. Partnering to enhance protection and resiliency), que tuvo como meta:

> Construir una América más segura y más resistente al prevenir, disuadir, neutralizar o mitigar los efectos de los esfuerzos deliberados de los terroristas para destruir, incapacitar o explotar elementos de la infraestructura crítica y recursos clave de nuestra Nación y fortalecer la preparación nacional oportuna, respuesta y recuperación rápida de la infraestructura crítica y los recursos clave en caso de un ataque, desastre natural u otra emergencia[119].

Para lograr esta meta se establecen una serie de objetivos en los que se debe tener la colaboración entre los gobiernos federal, estatal y local, el sector privado, entidades internacionales y organizaciones no gubernamentales[120]:

- ➢ Entender e intercambiar información sobre las amenazas terroristas y otros peligros con la infraestructura crítica y los socios clave de los recursos;
- ➢ Establecer alianzas para compartir información e implementar programas de protección de infraestructuras críticas y de recursos clave;
- ➢ Implementar un programa de gestión de riesgos a largo plazo; y
- ➢ Maximizar el uso eficiente de los recursos para la infraestructura crítica y la protección, restauración y recuperación de los recursos clave.

La piedra angular de este *Plan Nacional de Protección de la Infraestructura* es su marco de gestión de riesgos. Dándole esta importancia a los riesgos debido a que están influenciados por la naturaleza y magnitud de una amenaza, las vulnerabilidades a esa amenaza y las consecuencias que podrían resultar. “Este marco de gestión de riesgos integra y coordina estrategias, capacidades y gobernabilidad para permitir la toma de decisiones con conocimiento de riesgo relacionada con la infraestructura crítica y los recursos clave de la nación”[121].

El marco que se puede observar en la siguiente figura es aplicable a amenazas tales como desastres naturales o peligros de seguridad causados por el hombre.

---

[119] DHS, *National Infrastructure Protection Plan,* [en línea], 2009. Dirección URL: https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. [Fecha de consulta: 19 de julio de 2017].
[120] *Ídem.*
[121] *Ídem.*

Figura 2.1. Marco de Gestión de Riesgos del Plan Nacional de Protección de Infraestructura.

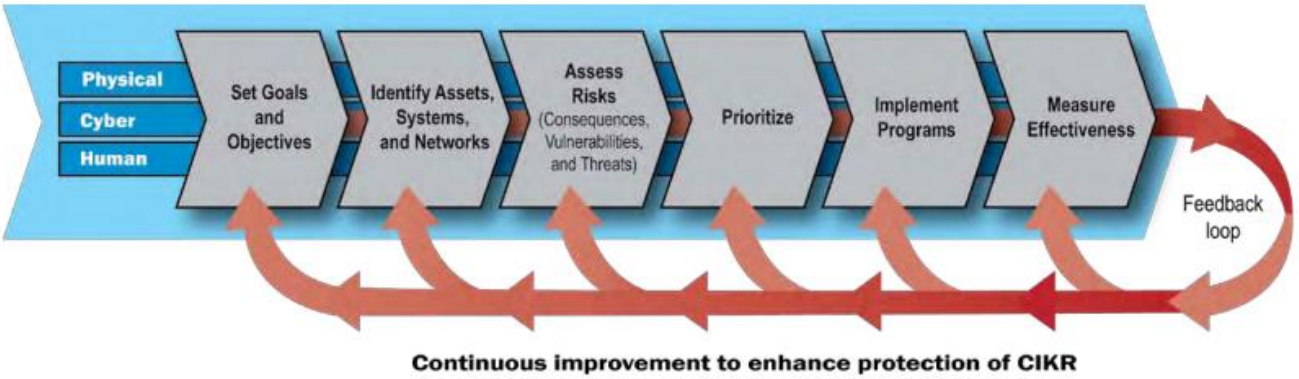


Imagen obtenida de DHS, *National Infrastructure Protection Plan,* [en línea], 2009. Dirección URL: https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Para el año 2012, la Oficina de Protección de Infraestructuras publica su *Plan Estratégico: 2012-2016* en el que se proponen cuatro metas a cumplir durante el tiempo designado en el nombre del plan: "apoyar y mejorar las actividades de gestión de riesgos; asegurar una coordinación e intercambio de información eficaces con los socios de la infraestructura crítica para mejorar las actividades de protección y resiliencia durante las operaciones normales y los incidentes; aumentar la concientización e implementar programas regulatorios para mejorar la protección de la infraestructura crítica y la resiliencia; y mantener un ambiente de trabajo positivo que promueva el logro de los objetivos de la organización"[122].

No obstante, la acción más importante después del *Plan Nacional de Protección de la Infraestructura* del 2009, se presentó en el año 2013 con la firma de la *Directiva de Política Presidencial - Seguridad y Resiliencia de la Infraestructura Crítica* (Presidential Policy Directive--Critical Infrastructure Security and Resilience) la cual se unía a los esfuerzos para fortalecer y mantener una infraestructura crítica segura, funcional y resiliente.

Esta Directiva identifica 16 sectores de infraestructura crítica y designa Agencias Sectoriales Específicas asociadas para colaborar con su protección:

[122] DHS, *Office of Infrastructure Protection Strategic Plan: 2012–2016,* [en línea]. Dirección URL: https://www.dhs.gov/sites/default/files/publications/IP-Strategic-Plan-FINAL-508.pdf. [Fecha de consulta: 19 de julio de 2017].

Tabla 2.8. Sectores de infraestructura crítica y sus Agencias Sectoriales Específicas.

Sector de infraestructura crítica	Agencia Sectorial Específica
Químico	Departamento de Seguridad Nacional
Instalaciones comerciales	Departamento de Seguridad Nacional
Comunicaciones	Departamento de Seguridad Nacional
Fabricación crítica	Departamento de Seguridad Nacional
Represas	Departamento de Seguridad Nacional
Base Industrial de Defensa	Departamento de Defensa
Servicios de emergencia	Departamento de Seguridad Nacional
Energía	Departamento de Energía
Servicios financieros	Departamento de Hacienda
Alimentación y agricultura	Departamento de Agricultura de los Estados Unidos y Departamento de Salud y Servicios Humanos.
Instalaciones gubernamentales	Departamento de Seguridad Nacional y Administración de Servicios Generales
Salud y Salud Pública	Departamento de Salud y Servicios Humanos
Tecnología de Información	Departamento de Seguridad Nacional
Reactores nucleares, materiales y residuos:	Departamento de Seguridad Nacional
Sistemas de transporte	Departamento de Seguridad Nacional y Departamento de Transporte
Sistemas de agua y alcantarillado	Agencia de Protección Ambiental

Elaboración propia con información obtenida de The White House, *Presidential Policy Directive--Critical Infrastructure Security and Resilience,* [en línea], 2013. Dirección URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Tres metas son las que se identifican por parte de todos los actores y departamentos que participan en la protección de las infraestructuras críticas en esta Directiva[123]:

1) Refinar y clarificar las relaciones funcionales en todo el Gobierno Federal para avanzar en la unidad nacional de esfuerzos para fortalecer la seguridad y la resiliencia de las infraestructuras críticas;
2) Hacer posible un intercambio efectivo de información mediante la identificación de los datos básicos y los requisitos de sistemas para el Gobierno Federal; e
3) Implementar una función de integración y análisis para informar las decisiones de planificación y operaciones sobre infraestructura crítica.

Pocos días después de la firma de esta Directiva, surgió la Orden Ejecutiva 13636 para mejorar la seguridad cibernética de las infraestructuras críticas debido a que se reconoce que las ciberamenazas a las mismas continúan creciendo y representan uno de los desafíos de seguridad nacional más serios que se deben enfrentar.

Además, se establece la obligación de Estados Unidos de "mejorar la seguridad y la resistencia de la infraestructura crítica de la nación y mantener un entorno cibernético que fomente la eficiencia, la innovación y la prosperidad económica, al tiempo que promueve la seguridad, la confidencialidad empresarial, la privacidad y las libertades civiles"[124].

Se ordena también al Secretario de Comercio para que dirija al Director del Instituto Nacional de Imprenta y Tecnología para dirigir el desarrollo de un marco para reducir los riesgos cibernéticos a la infraestructura crítica: el Marco de Seguridad Cibernética. Este Marco debía incluir un conjunto de normas, metodologías, procedimientos y procesos que alinearan los enfoques de política, negocios y tecnología para abordar los riesgos cibernéticos.

Durante el mismo año, 2013, se publicó el *Plan Nacional de Protección de la Infraestructura* con el fin de "fortalecer la seguridad y la resistencia de la infraestructura crítica de la nación, mediante la gestión de riesgos físicos y cibernéticos a través de los

[123] The White House, *Presidential Policy Directive--Critical Infrastructure Security and Resilience,* [en línea], 2013. Dirección URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. [Fecha de consulta 20 de julio de 2017].

[124] Office of the Federal Register, *Improving Critical Infrastructure Cybersecurity,* [en línea], Executive Order 13636. Dirección URL: https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity. [Fecha de consulta: 20 de julio de 2017].

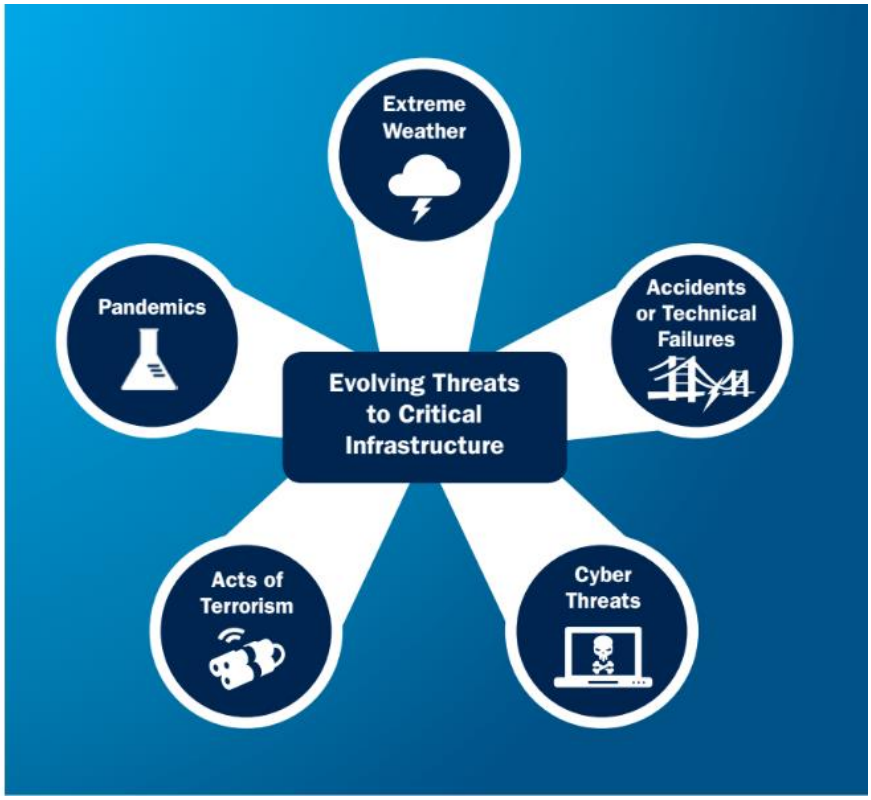
esfuerzos de colaboración e integrados de la comunidad de infraestructura crítica"[125]. Este plan a su vez se plantea diversas metas[126]:

- ➔ Evaluar y analizar las amenazas, vulnerabilidades y consecuencias de la infraestructura crítica para informar las actividades de gestión de riesgos;
- ➔ Asegurar la infraestructura crítica contra las amenazas humanas, físicas y cibernéticas mediante esfuerzos sostenibles para reducir el riesgo, al mismo tiempo que se contabilizan los costos y beneficios de las inversiones en seguridad;
- ➔ Mejorar la resiliencia de las infraestructuras críticas minimizando las consecuencias adversas de los incidentes mediante la planificación anticipada y los esfuerzos de mitigación, y empleando respuestas eficaces para salvar vidas y asegurar la rápida recuperación de los servicios esenciales;
- ➔ Compartir información útil y pertinente en toda la comunidad de infraestructura crítica para crear conciencia y permitir una toma de decisiones basada en el riesgo; y
- ➔ Promover el aprendizaje y la adaptación durante y después de los ejercicios e incidentes.

En este plan se acepta que el entorno de riesgo que afecta a la infraestructura crítica es complejo e incierto pues las amenazas, vulnerabilidades y consecuencias han evolucionado en los últimos 10 años. Por ejemplo, la infraestructura crítica que durante mucho tiempo estuvo sujeta a riesgos asociados con amenazas físicas y desastres naturales ahora está cada vez más expuesta a ciberataques derivados de la creciente integración de las tecnologías de la información y las comunicaciones con las operaciones de infraestructura crítica.

[125] DHS, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience,* [en línea]. Dirección URL: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience. [Fecha de consulta: 20 de julio de 2017].
[126] *Ídem.*

Figura 2.2. Amenazas a la infraestructura crítica.



Tomada de DHS, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience,* [en línea]. Dirección URL: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

Como en el *Plan Nacional de Protección de la Infraestructura* del año 2009, en este también se establecen los departamentos encargados de cada uno de los sectores de infraestructura crítica. Esto se puede observar en la siguiente tabla.

Tabla 2.9. Estructuras Coordinadoras Sectoriales y Transectoriales.

		Critical Infrastructure Partnership Advisory Council		
Critical Infrastructure Sector	Sector Specific Agency	Sector Coordinating Councils (SCCs)	Government Coordinating Councils (GCCs)	Regional Consortia
Chemical	Department of Homeland Security	✓	✓	
Commercial Facilities ⓘ		✓	✓	
Communications ⓘ		✓	✓	
Critical Manufacturing		✓	✓	
Dams		✓	✓	
Emergency Services ⓘ		✓	✓	
Information Technology ⓘ		✓	✓	
Nuclear Reactors, Materials & Waste		✓	✓	
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	✓	✓	
Defense Industrial Base ⓘ	Department of Defense	✓	✓	
Energy ⓘ	Department of Energy	✓	✓	
Healthcare & Public Health ⓘ	Department of Health and Human Services	✓	✓	
Financial Services ⓘ	Department of the Treasury	Uses separate coordinating entity	✓	
Water & Wastewater Systems ⓘ	Environmental Protection Agency	✓	✓	
Government Facilities	Department of Homeland Security, General Services Administration	Sector does not have an SCC	✓	
Transportation Systems ⓘ	Department of Homeland Security, Department of Transportation	Various SCCs are broken down by transportation mode or subsector.	✓	

Critical Infrastructure Cross-Sector Council

Federal Senior Leadership Council

State, Local, Tribal, and Territorial Government Coordinating Council

Regional Consortium Coordinating Council

ⓘ Indicates that a sector (or a subsector within the sector) has a designated information-sharing organization.

Tabla obtenida de DHS, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience,* [en línea]. Dirección URL: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

Para comprender mejor la tabla, se tiene que aclarar que los Consejos Sectoriales de Coordinación son "consejos del sector privado autogestionados, autogenerados y autogobernados, compuestos por propietarios y operadores y sus representantes, que interactúan en una amplia gama de estrategias, políticas, actividades y temas específicos del sector"[127].

Estos consejos "sirven como principales puntos de colaboración entre el gobierno y los propietarios y operadores del sector privado para la coordinación y planificación de la seguridad de las infraestructuras críticas y la resiliencia y una serie de actividades relacionadas con sectores específicos"[128].

Los Consejos de Coordinación Gubernamental son representantes de varios niveles de gobierno según sea apropiado para el panorama operativo de cada sector individual, estos consejos permiten la coordinación interinstitucional, intergubernamental e intercomunitaria dentro y entre sectores. Por último, el Consejo Coordinador del Consorcio Regional comprende grupos regionales y coaliciones alrededor del país que participan en diversas iniciativas para avanzar en la seguridad y resistencia de las infraestructuras críticas en los sectores público y privado[129].

Este *Plan Nacional de Protección de la Infraestructura de Estados Unidos* 2013, es el último plan que está disponible por el momento. En el 2016 se publicaron algunas hojas informativas sobre ciertas acciones a seguir en temas como la resiliencia, la gestión de riesgos y objetivos a cumplir en sectores como el de la salud y la energía pero en realidad nada que fuera muy relevante.

Aunque el gobierno ya presentó el llamado *Desafío de Seguridad y Resistencia del Plan Nacional de Protección de Infraestructura* (NIPP) 2017, aún no se encuentra disponible para el público en general. En cambio, una de las acciones más recientes e importantes de la administración de Donald Trump ha sido la firma del Decreto Ejecutivo Presidencial sobre el *Fortalecimiento de la Ciberseguridad de las Redes Federales y la Infraestructura Crítica*.

---

[127] HS, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience,* [en línea]. Dirección URL: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience. [Fecha de consulta: 20 de julio de 2017].

[128] *Ídem.*

[129] *Ídem.*

En esta Orden Ejecutiva se establece que el Presidente asumirá la responsabilidad de los jefes de los departamentos y agencias ejecutivas (jefes de agencia) por gestionar el riesgo de ciberseguridad para sus empresas. Además, debido a que las decisiones de gestión de riesgos tomadas por los jefes de agencia pueden afectar el riesgo para el ejecutivo en su conjunto y para la seguridad nacional, también "es política de los Estados Unidos manejar el riesgo de seguridad cibernética como una empresa del poder ejecutivo"[130].

A partir de ahora, de acuerdo con esta orden, cada jefe de agencia proporcionará un informe de gestión de riesgos al Secretario de Seguridad Nacional y al Director de la Oficina de Gestión y Presupuesto. Dicho informe deberá: "documentar las opciones de mitigación y aceptación del riesgo tomadas por cada jefe de agencia a la fecha de esta orden, incluyendo las consideraciones estratégicas, operativas y presupuestarias que informaron esas elecciones y cualquier riesgo aceptado, incluyendo desde vulnerabilidades no mitigadas; y describir el plan de acción de la agencia"[131].

Por último, se les solicita al Secretario de Estado, el Secretario de Hacienda, el Secretario de Defensa, el Procurador General, el Secretario de Comercio, el Secretario de Seguridad Nacional, el Representante de Comercio de los Estados Unidos y al Director de Inteligencia Nacional, presentar conjuntamente al Presidente a través del Asistente del Presidente para Asuntos de Seguridad Nacional y el Asistente del Presidente para la Seguridad Interna y el Contraterrorismo, las opciones estratégicas de la nación para disuadir a los adversarios y proteger mejor a los estadounidenses de las amenazas cibernéticas[132].

Como se pudo observar durante el desarrollo de este punto de la investigación la complejidad de la red ocasiona que surjan un gran número de áreas dedicadas a la supervisión y actividades de inteligencia en el ciberespacio por lo que para obtener los resultados esperados es necesario que exista una gran comunicación entre las diferentes agencias o departamentos gubernamentales. Por otro lado la cooperación público-privada relacionada con la ciberseguridad atraviesa los límites de las agencias,

[130] The White House, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* [en línea]. Dirección URL: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal. [Fecha de consulta: 21 de julio de 2017].
[131] *Ídem.*
[132] *Ídem.*

por lo que la creación de estrategias que permitan saber cómo comunicarse, qué información compartir y qué uso darle a la misma es indispensable.

En cada una de las estrategias de seguridad nacional de Estados Unidos en el ámbito de ciberseguridad, se destaca la cooperación del gobierno federal con el sector privado. La burocracia del gobierno estadounidense es vasta y complicada pues cuenta con numerosas agencias, oficinas, juntas y comisiones. Todos los departamentos y agencias federales están a cargo de la protección de sus propios sistemas de TIC y muchos tienen responsabilidades sectoriales específicas para la infraestructura crítica de la que son responsables.

III. La ciberseguridad en el Sistema de Posicionamiento Global (GPS).

> La respuesta de los Estados Unidos a los desafíos y oportunidades de la era cibernética determinará nuestra prosperidad y seguridad futuras. Internet es una invención estadounidense, y debe reflejar nuestros valores a medida que continúa transformando el futuro para todas las naciones y todas las generaciones. Una infraestructura cibernética sólida y defendible fomenta el crecimiento económico, protege nuestras libertades y mejora nuestra seguridad nacional.
>
> -Estrategia de Seguridad Nacional de Estados Unidos 2017.

3.1. El Sistema de Posicionamiento Global (GPS).

La era espacial comenzó como una carrera por la seguridad y el prestigio entre dos superpotencias. Las oportunidades en ese momento se limitaban a Estados Unidos y la Unión Soviética sin embargo, las décadas que siguieron han visto una transformación radical en las actividades de la vida diaria en gran parte debido al uso y aprovechamiento del espacio por parte de una enorme variedad de actores incluidos aquellos no estatales.

Los vehículos espaciales han permitido viajar a otros cuerpos celestes y el desarrollo de distintas tecnologías como los Sistemas Mundiales de Navegación por Satélite han revolucionado el funcionamiento de todas las infraestructuras que proporcionan servicios fundamentales y básicos para cualquier sociedad. No obstante toda ventaja trae su contraparte y el crecimiento del nuevo dominio, el ciberespacio, y el fácil acceso a éste han multiplicado los riesgos y las amenazas poniendo en peligro la seguridad nacional de los Estados.

3.1.1. Fundamentos y funciones.

Con el lanzamiento del *Sputnik*[133] en el año 1957 por la Unión Soviética, se descubrió que este satélite podía ser utilizado como una herramienta de navegación. Los investigadores

[133] Sputnik 1 fue lanzado el 4 de octubre de 1957, convirtiéndose en el primer satélite artificial colocado con éxito en la órbita de la Tierra. El satélite medía 58 centímetros de diámetro y pesaba 83.6 kilogramos. Tenía cinco objetivos científicos primarios: probar el método de colocar un satélite artificial en la órbita terrestre; proporcionar información sobre la densidad de la atmósfera calculando su vida útil en órbita; prueba de radio y métodos ópticos de seguimiento orbital; determinar los efectos de la propagación de ondas de radio a través de la atmósfera; y, comprobar los principios

del laboratorio Lincoln del Instituto Tecnológico de Massachusetts (MIT, por sus siglas en inglés) pudieron determinar con precisión la órbita del satélite al observar cómo la frecuencia aparente de la señal de radio aumentaba al acercarse y disminuía al alejarse, hecho que se conoce como efecto *Doppler*. Fue así, como se dio el primer paso para establecer la posibilidad de determinar las posiciones en la Tierra mediante la localización de señales emitidas por satélites[134].

Durante los años siguientes, la marina estadounidense realizó experimentos con una serie de sistemas de navegación por satélite, que comenzó en 1965 con el sistema *Transit*, desarrollado para satisfacer las necesidades de navegación de los submarinos que transportaban misiles nucleares. El sistema *Transit* estaba formado por seis satélites que giraban alrededor de la Tierra, al analizar las señales de radio transmitidas por los satélites es decir, al medir el efecto *Doppler* de las señales, un submarino podía determinar su ubicación con precisión en un período de diez o quince minutos.

En 1973, el Departamento de Defensa desarrolló el concepto de Sistema de Posicionamiento Global (Global Positioning System o GPS, por sus siglas en inglés), basado en la experiencia del departamento con todos los satélites anteriores. Los componentes esenciales del GPS son los 24 satélites *Navstar* fabricados por *Rockwell International*[135]. Cada uno de estos satélites tiene el tamaño de un vehículo de gran tamaño y pesa alrededor de 1,900 libras (900 kilogramos). Todos los satélites giran alrededor de la Tierra cada doce horas en una formación tal que cada punto del planeta siempre se encontrará en contacto por radio con 4 satélites como mínimo. El primer

---

de presurización utilizados en los satélites. El exitoso lanzamiento sacudió al mundo, dando a la Unión Soviética la distinción de poner el primer objeto hecho por el hombre en el espacio y otorgándole la victoria sobre Estados Unidos, la carrera espacial había comenzado.

Como respuesta Estados Unidos se vio obligado a acelerar el programa espacial que estaba llevando a cabo, lo que resultó en el lanzamiento del satélite Explorer 1 el 31 de enero de 1958. El satélite tenía 203 centímetros (80 pulgadas) de largo y 15,9 centímetros (6,25 pulgadas) de diámetro y pesaba 14 kilogramos.

[134] National Academy of Sciences, *The Global Positioning System,* [en línea], Beyond Discovery. The Path from Research to Human Benefit, 1997, p.4. Dirección URL: http://www.nasonline.org/publications/beyond-discovery/the-global-positioning-system.pdf. [Fecha de consulta: 13 de agosto de 2017].

[135] *Rockwell International Corporation*, anteriormente (1967-1973) *North American Rockwell Corporation*, es una corporación estadounidense que por años fue uno de los principales contratistas aeroespaciales del país, fabricando vehículos de lanzamiento y naves espaciales para el programa espacial estadounidense. Después de la fusión con *Rockwell-Standard Corporation*, la empresa continuó siendo un contratista importante del gobierno, haciendo los motores del cohete de *Saturn V* que levantaron los astronautas de Apolo a la luna y los orbitadores del transbordador espacial por ejemplo. A pesar de estos éxitos, Rockwell en la década de 1980 se diversificó en campos como la electrónica y los productos automotrices en un esfuerzo por reducir su dependencia de los sistemas y armas espaciales contratados por el gobierno estadounidense. Rockwell se había convertido en un importante fabricante de chips de módem, aviónica comercial y equipo de automatización de fábricas cuando vendió sus productos electrónicos de defensa y negocios aeroespaciales a *The Boeing Company* en 1996.

satélite GPS en funcionamiento se lanzó en 1978 y el sistema alcanzó su capacidad completa de 24 satélites en 1995[136].

Hoy en día el Sistema de Posicionamiento Global “es un sistema de radionavegación de los Estados Unidos de América basado en el espacio, que proporciona servicios fiables de posicionamiento, navegación, y cronometría en todo el mundo. La Fuerza Aérea gestiona la constelación para garantizar la disponibilidad de al menos 24 satélites GPS, el 95% del tiempo”[137].

Este sistema se compone de tres segmentos: a) los satélites en órbita alrededor de la Tierra, b) las estaciones terrestres de seguimiento y control, y c) los receptores del GPS propiedad de los usuarios. El primer segmento, el espacial, consiste en una constelación de satélites que transmite señales de radio a los usuarios, los satélites están posicionados dentro de seis planos orbitales igualmente espaciados que rodean la Tierra, vuelan a una altitud de aproximadamente 20,200 km, cada uno rodea el planeta dos veces al día y están diseñados para tener una vida útil de 7 a 12 años[138].

En junio de 2011, la Fuerza Aérea completó con éxito una expansión de constelación de GPS conocida como la configuración "*Expandable 24*". Tres de las 24 franjas horarias se expandieron y seis satélites fueron reposicionados, de modo que tres de los satélites adicionales pasaron a formar parte de la línea de base de la constelación. Como resultado, el GPS comenzó a funcionar como una constelación de 27 satélites con una mejor cobertura alrededor del mundo.

Durante los últimos años, la Fuerza Aérea ha estado volando 31 satélites GPS operativos, más 3-5 satélites desactivados ("residuos") que pueden reactivarse si es necesario. Al 25 de agosto de 2017, siguen existiendo un total de 31 satélites operacionales en la constelación del GPS, no incluyendo los que se encuentran desactivados. La constelación del GPS es una mezcla de viejos y nuevos satélites.

[136] National Academy of Sciences, *Op. cit.*
[137] GPS, *¿Qué es el GPS?*, [en línea]. Dirección URL: http://www.gps.gov/spanish.php. [Fecha de consulta: 18 de agosto de 2017].
[138] GPS, *Space Segment,* [en línea]. Dirección URL: http://www.gps.gov/systems/gps/space/. [Fecha de consulta: 18 de agosto de 2017].

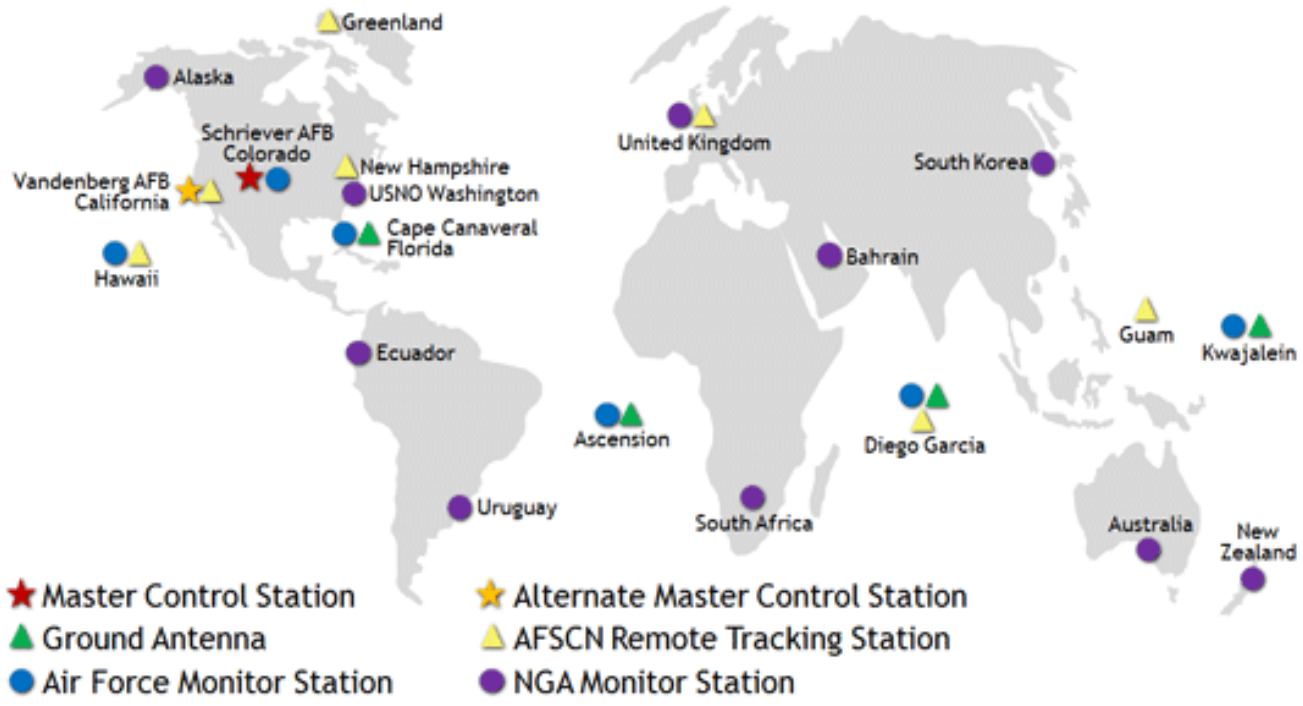
Imagen 3.1. Constelación de satélites GPS

Tomada de Schriever Air Force Base, *50 SW completes GPS constellation expansion,* [en línea]. Dirección URL: http://www.schriever.af.mil/News/Article-Display/Article/277054/50-sw-completes-gps-constellation-expansion/.

Por otro lado, el segmento de control GPS consiste en una red global de instalaciones terrestres que rastrea los satélites GPS, monitorea sus transmisiones, realiza análisis y envía comandos y datos a la constelación. El segmento de control operacional actual incluye una estación de control maestra, una estación de control maestra alternativa, 11 antenas de mando y control y 16 sitios de monitoreo[139]. Las ubicaciones de estas instalaciones se muestran en el siguiente mapa:

[139] GPS, *Control Segment,* [en línea]. Dirección URL: http://www.gps.gov/systems/gps/control/. [Fecha de consulta: 18 de agosto de 2017].

Mapa 3.1. Ubicación de las instalaciones de control del GPS.



Obtenido de GPS, *Control Segment,* [en línea]. Dirección URL: http://www.gps.gov/systems/gps/control/.

La constelación de GPS ofrece un rendimiento consistentemente alto gracias a los operadores pertenecientes a la Segunda Escuadrilla de Operaciones Espaciales de la Fuerza Aérea de los Estados Unidos (2SOPS, por sus siglas en inglés) y el 19° Escuadrón de Operaciones Espaciales de la Fuerza Aérea (19SOPS, por sus siglas en inglés) en la Base Aérea Schriever, Colorado. Juntos, forman el llamado *Team Blackjack* y se encargan de mantener los satélites GPS volando las 24 horas del día los 7 días de la semana, con disponibilidad continua y alta precisión para miles de millones de usuarios civiles y militares.

El segmento de control está compuesto por diversos elementos[140]:

1. Estación de Control Principal o Maestra (MCS).

[140] GPS, *Control Segment, Op. cit.*

Se encuentra ubicada en Colorado y es donde el 2SOPS realiza las funciones de segmento de control primario, proporcionando el comando y control de la constelación de GPS. Esta estación genera y carga mensajes de navegación, y asegura el buen funcionamiento, la integridad y la precisión de la constelación de satélites. Además, recibe información de navegación de las estaciones de monitoreo y la utiliza para calcular las ubicaciones precisas de los satélites GPS en el espacio para después cargar estos datos en los satélites.

También en esta estación de control principal se realiza el mantenimiento de satélites así como la resolución de anomalías, en caso de que falle algún satélite, se puede reposicionar los demás satélites para mantener una óptima constelación de GPS.

El Centro de Operaciones GPS (GPSOC) en la Base Aérea de Schriever, Colorado, es el punto focal en el Departamento de Defensa para cuestiones operacionales y preguntas relacionadas con el uso militar del GPS. Este centro es parte del Comando Espacial de la Fuerza Aérea y proporciona al Departamento de Defensa y a los usuarios de GPS aliados (de Estados Unidos) en todo el mundo, informes de anomalías e información general las 24 horas del día, los siete días de la semana. El GPSOC es responsable de[141]:

- Recepción de informes y respuestas coordinadas a la interferencia de radiofrecuencia en el uso del GPS en operaciones militares;
- Proporcionar respuestas rápidas a los problemas del usuario del Departamento de Defensa o preguntas concernientes al GPS;
- Proporcionar el control oficial del Comando Estratégico de los Estados Unidos (USSTRATCOM) del rendimiento del GPS proporcionado a los usuarios del Departamento de Defensa a nivel mundial;
- Proporcionar apoyo táctico para la planificación y evaluación de misiones militares que impliquen el uso del GPS.

Además, el GPSOC interactúa con la comunidad civil a través del Centro de Navegación de la Guardia Costera de Estados Unidos (NAVCEN, por sus siglas en inglés) y la Administración Federal de Aviación (FAA, por sus siglas inglés).

[141] GPS, *GPS Service Outages & Status Reports,* [en línea]. Dirección URL: http://www.gps.gov/support/user/. [Fecha de consulta: 8 de septiembre de 2017].

2. Estaciones de monitoreo.

Estas estaciones rastrean los satélites GPS cuando pasan por encima de las mismas y canalizan sus observaciones de vuelta a la Estación de Control Maestra. Recogen datos atmosféricos, mediciones de rango/portador y señales de navegación. Los sitios utilizan receptores GPS sofisticados y son operados por la MCS. Hay 16 estaciones de monitoreo ubicadas en todo el mundo, incluyendo seis de la Fuerza Aérea y 10 de la Agencia Nacional de Inteligencia Geoespacial (NGA, por sus siglas en inglés).

3. Antenas terrestres.

Las antenas terrestres se utilizan para comunicarse con los satélites GPS para fines de mando y control. Estas antenas soportan enlaces de comunicaciones de *banda-S*[142] que envían/transmiten cargas de datos de navegación y cargas de programas de procesador, y recogen la telemetría[143]. También son responsables de las transmisiones de comandos normales a los satélites.

Hay cuatro antenas terrestres GPS ubicadas en las estaciones de monitoreo en Kwajalein (atolón en las Islas Marshall), en la Isla Ascensión, en el atolón Diego García (ubicado en el Archipiélago de Chagos, situado en el territorio británico del Océano Índico) y en Cabo Cañaveral (Florida). Además, el segmento de control está conectado a las siete estaciones de localización remota de la Red de Control de Satélite de la Fuerza Aérea (AFSCN, por sus siglas en inglés) en todo el mundo, aumentando la visibilidad, flexibilidad y robustez para la telemetría, el seguimiento y el mando.

Por último se encuentra el segmento del usuario, que consiste en el equipo receptor del GPS que recibe las señales de los satélites del GPS y las procesa para calcular la posición tridimensional y la hora, servicio que está disponible de manera

[142] La banda-S está comprendida en un rango de frecuencias que van desde los 2.0 a los 4.0 Ghz y su longitud de onda es de 8-15 cm y parte de la banda de microondas del espectro electromagnético. Es utilizada con mayor frecuencia por radares meteorológicos pues son la mejor opción para obtener imágenes claras y fieles de fenómenos meteorológicos intensos a largo alcance. El rango de banda-S permite que el 2SOPS pueda resolver cualquier anomalía en los satélites.

[143] Se conoce como telemetría al sistema que permite la monitorización, mediación y/o rastreamiento de magnitudes físicas o químicas a través de datos que son transferidos a una central de control. Se realiza normalmente mediante comunicación inalámbrica pero también se puede realizar a través de otros medios como: teléfono, redes de ordenadores, enlace de fibra óptica, entre otros. La telemetría tiene como objetivo permitir la mediación de magnitudes físicas o químicas, conocer los estados de los procesos y sistema, así como controlar de manera remota el funcionamiento, corregir los errores y enviar la información recabada hacia un sistema de información para su uso y provecho. La telemetría espacial permite obtener desde la tierra mediciones efectuadas a bordo del satélite, lo cual es de suma importancia para la seguridad del hombre. Por otro lado, permite controlar pruebas de vuelos y verificar aviones, sondas, misiles, entre otros.

gratuita y permanente. En 1983 por órdenes del entonces presidente Ronald Reagan[144], el Sistema de Posicionamiento Global se puso a disposición para los usuarios civiles[145].

En el año 2000 Bill Clinton ya reconocía el GPS como un sistema dual de uso militar-civil y por razones de seguridad nacional el segmento civil contaba con "Disponibilidad Selectiva", "una degradación intencional de la calidad de la señal de GPS que introducía errores de hasta 50 a 100 metros al proporcionar la ubicación. Sin embargo, en dicho año fue suspendida para hacer que el sistema fuera de mayor utilidad en cuestiones civiles y comerciales"[146]. El Centro de Navegación de la Guardia Costera de los EE.UU. es el punto de contacto designado para brindar apoyo operacional al usuario GPS de la comunidad civil.

También, se encuentra el Comité de Interconexión de Servicios del Sistema de Posicionamiento Global Civil (CGSIC, por sus siglas en inglés), establecido por el Departamento de Transporte de los Estados Unidos. Está compuesto por representantes de grupos de usuarios privados, gubernamentales e industriales relevantes, tanto de los EE.UU. como internacionales. La estructura del Comité consta de un presidente, dos vicepresidentes, una Secretaría Ejecutiva y un Panel Ejecutivo.

El Comité está presidido por el Director de Radionavegación y Posicionamiento. El primer Vicepresidente es Comandante del Centro de Navegación de la Guardia de los Estados Unidos, cuenta con el apoyo de una Secretaría Ejecutiva, administra el Comité, coordina las reuniones del mismo, representa al Presidente del Comité en las reuniones relacionadas con el GPS y coordina las respuestas a los temas presentados.

El segundo Vicepresidente es el Vicepresidente de Asuntos Internacionales y es un representante no estadounidense designado por el Presidente con la aprobación del

[144] Reagan Library, *Statement by Deputy Press Secretary Speakes on the Soviet Attack on a Korean Civilian Airliner,* [en línea]. Dirección URL: https://reaganlibrary.archives.gov/archives/speeches/1983/91683c.htm. [Fecha de consulta: 8 de septiembre de 2017].

[145] En 1983 el vuelo 007 de *Korean Air Lines* que partió de Nueva York con destino a Corea del Sur perdió su ruta y se desvió al espacio aéreo soviético, razón por la cual fue derribado. El saldo fueron 269 víctimas y el aumento de las tensiones entre Estados Unidos y la Unión Soviética en plena Guerra Fría. Para que este suceso no se repitiera, el presidente Ronald Reagan decidió poner a disposición de las aeronaves civiles las instalaciones del Sistema de Posicionamiento Global que permitiría a los aviones obtener información de su posición tridimensional.
Aunque en 1983 el presidente Reagan toma la decisión de que el GPS esté disponible para los usuarios civiles hay que recordar que éste fue operativo hasta 1995, y un año después para reafirmar la postura de Reagan el Departamento de Defensa y el de Transportes firmaron un Memorándum de Acuerdo para el uso civil del GPS.

[146] White House, *U.S. GLOBAL POSITIONING SYSTEM POLICY,* [en línea]. Dirección URL: https://clintonwhitehouse3.archives.gov/WH/EOP/OSTP/NSTC/html/pdd6.html. [Fecha de consulta: 8 de septiembre de 2017].

Panel Ejecutivo. Este último está compuesto por el Presidente, los Vicepresidentes, los Presidentes de los Subcomités, un representante del Comité Interinstitucional del Sistema Global de Observación Geodésica (GIAC, por sus siglas en inglés)[147] y representantes de tres áreas:

1. Aviación: un representante designado por la Administración Federal de Aviación
2. Tierra: un representante designado por la Administración Federal de Carreteras
3. Mar: un representante designado por la Guardia Costera de los Estados Unidos.

Entre los objetivos del Comité de Interconexión de Servicios del Sistema de Posicionamiento Global Civil se encuentran[148]:

- Proporcionar un foro para intercambiar información técnica y recopilar información sobre las necesidades GPS de la comunidad civil.
- Identificar los requisitos y métodos de información para distribuir esta información a los usuarios GPS.
- Llevar a cabo estudios de información GPS sobre las necesidades de los usuarios civiles según lo solicitado por el Departamento de Transporte o identificado por el Comité.
- Identificar cualquier problema de GPS y someterlo a las autoridades apropiadas para su consideración.

Por otra parte, el Sistema de Posicionamiento Global recibe atención y orientación a nivel nacional de un órgano civil/militar conjunto denominado Comité Ejecutivo Nacional de Posicionamiento Espacial, Navegación y Tiempo (PNT, por sus siglas en inglés). Establecido por una directiva presidencial, este Comité coordina los asuntos relacionados con el GPS en varias agencias federales para asegurar que el sistema responde a las prioridades nacionales así como a los requisitos militares.

El Comité Ejecutivo Nacional es presidido conjuntamente por los Subsecretarios de Defensa y Transporte. Además, incluye altos líderes de los Departamentos de

[147] El Sistema Global de Observación Geodésica es el sistema de observación de la Asociación Internacional de Geodesia (IAG, por sus siglas en inglés) que proporciona las observaciones necesarias para monitorear, mapear y comprender los cambios en la forma, rotación y distribución masiva de la Tierra.

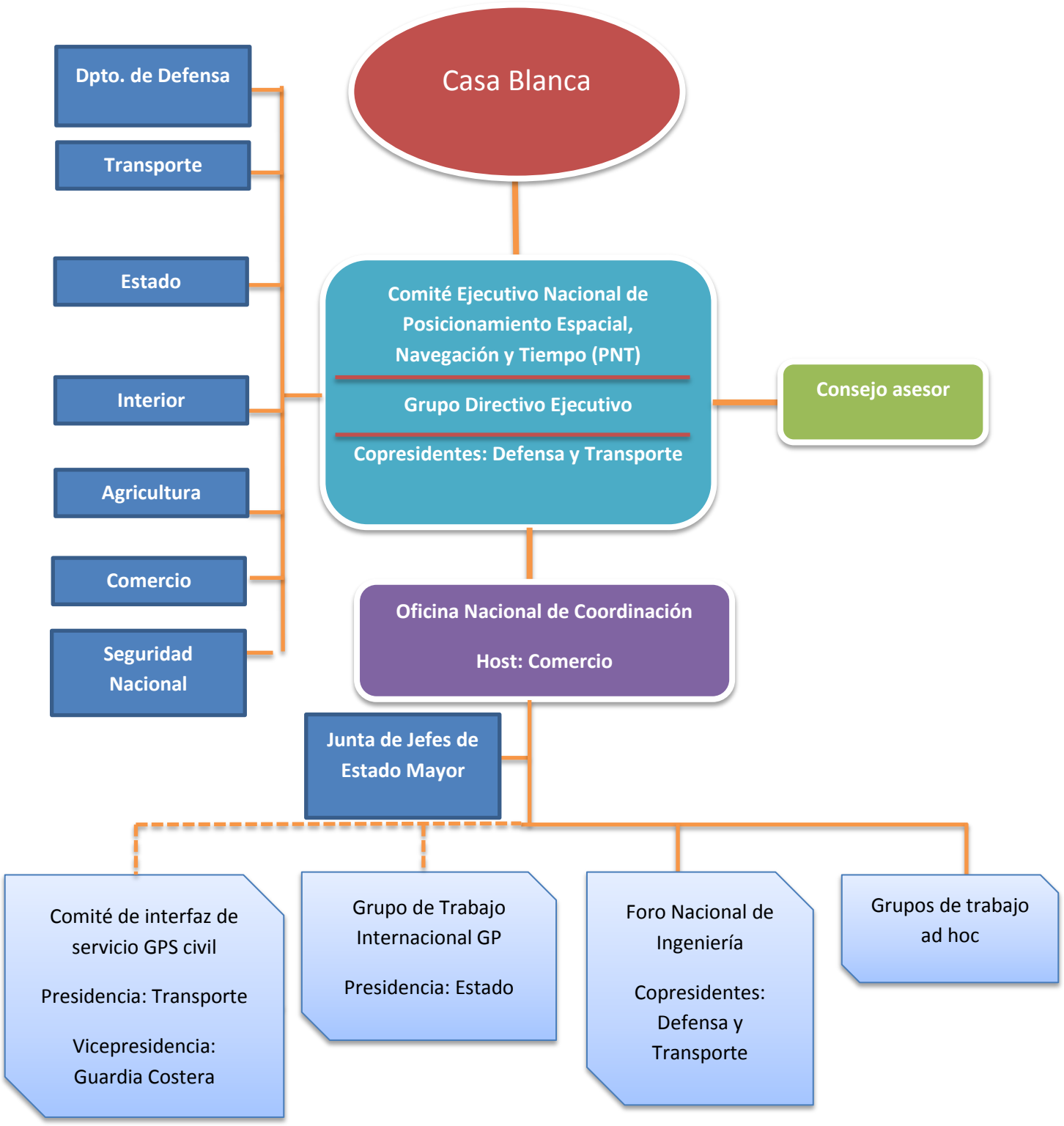
[148] GPS, *Civil Global Positioning System (GPS) Service Interface Committee Charter,* [en línea]. Dirección URL: http://www.gps.gov/cgsic/charter/. [Fecha de consulta: 8 de septiembre de 2017].

Estado, el Interior, Agricultura, Comercio y Seguridad Nacional, los Jefes de Estado Mayor Conjunto y la Administración Nacional de la Aeronáutica y del Espacio (NASA, por sus siglas en inglés). Como se puede ver, son numerosos los departamentos y agencias del gobierno de Estados Unidos los que participan en la operación, administración y/o uso del GPS como un activo nacional.

El personal permanente del Comité Ejecutivo Nacional de Posicionamiento Espacial, Navegación y Tiempo conforma la Oficina Nacional de Coordinación (NCO, por sus siglas en inglés), que es responsable de recopilar información relacionada con el GPS de múltiples agencias federales, del desarrollo del consenso interinstitucional y la resolución de problemas. La oficina está dirigida por un director y subdirector e incluye un cuadro de asesores superiores de las agencias del Comité Ejecutivo Nacional. Además, mantiene el sitio web *GPS.gov* como el pilar central de la campaña de alcance GPS de los Estados Unidos y desarrolla y difunde otros materiales educativos relativos al GPS[149].

[149] GPS, *National Coordination Office for Space-Based Positioning, Navigation, and Timing,* [en línea]. Dirección URL: http://www.gps.gov/governance/excom/nco/. [Fecha de consulta: 9 de septiembre de 2017].

Esquema 3.1. Estructura Organizacional de los Estados Unidos para la gobernanza del GPS.



Obtenido de GPS, *Organization,* [en línea]. Dirección URL: http://www.gps.gov/governance/excom/. Traducción propia.

3.1.2. Legislación del GPS.

En la parte legal, el Código de los Estados Unidos es una compilación de estatutos federales permanentes, organizados en varios títulos, en dos de los cuales se aborda el tema del Sistema de Posicionamiento Global: el Título 10 (Fuerzas Armadas) y el Título 51 (Programas de Espacios Nacionales y Comerciales). El sistema de aumento[150] de GPS a escala nacional se trata en el Título 49 (Transporte).

En el Título 10 de la sección 2281 del Código de los Estados Unidos asigna al Secretario de Defensa autoridad legal para sostener y operar GPS con fines militares y civiles. Además, le ordena que proporcione servicio GPS civil en forma continua, en todo el mundo, sin cargos directos por parte de los usuarios y debe desarrollar medidas para prevenir el uso hostil del GPS en un área particular sin obstaculizar el uso civil pacífico del sistema en otros lugares.

El Secretario de Defensa y el Secretario de Transporte según el mismo estatuto, deben preparar conjuntamente el Plan Federal de Radionavegación, mismo que debe publicarse cada dos años[151]. Mientras que el Secretario de la Fuerza Aérea presentará al Contralor General de los Estados Unidos un informe[152] y documentación de apoyo sobre el segmento espacial del Sistema de Posicionamiento Global III[153], el segmento de control operacional del GPS y los programas de adquisición de equipos de usuario del mismo pero en su uso militar.

Asimismo, esta sección 2281 establece que “el presidente no podrá autorizar ni permitir la construcción de una estación de monitoreo terrestre del sistema mundial de navegación por satélite controlada directa o indirectamente por un gobierno extranjero en el territorio de Estados Unidos, a menos que el Secretario de Defensa y el Director de Inteligencia Nacional certifiquen conjuntamente a los comités del Congreso apropiados

[150] Un sistema de aumento del GPS es cualquier sistema que lo ayuda proporcionando exactitud, integridad, disponibilidad o cualquier otra mejora al posicionamiento, navegación y sincronización que no es inherentemente parte del propio GPS, más adelante en este capítulo se hablará de ellos.

[151] El Plan Federal de Radionavegación es la fuente oficial de la política y planificación de radionavegación para el gobierno federal de los Estados Unidos. Abarca tanto los sistemas de radionavegación de uso terrestre como los espaciales, de uso común y de uso federal, incluidos los sistemas de GPS y los sistemas de aumento del mismo. El plan destaca la importancia de la infraestructura de posicionamiento espacial, navegación y tiempo y realiza estudios, análisis y evaluaciones para el desarrollo, demostración e implementación de tecnología en la misma.

[152] Cada informe debe incluir una declaración de la situación con respecto al segmento del GPS y su funcionamiento, una descripción de cualquier cambio, de cualquier riesgo técnico que afecte el costo, y/o desempeño y una evaluación de cómo se deben abordar estos riesgos y los costos asociados con los mismos.

[153] La empresa *Lockheed Martin* tiene una fuerte herencia en la construcción y mantenimiento del GPS de la Fuerza Aérea de los Estados Unidos, por lo que ahora está trabajando para ampliar las capacidades de éste con la próxima generación de satélites GPS III. De esta modernización se hablará en el punto 3.3 de esta investigación.

que dicha estación de monitoreo terrestre no poseerá la capacidad o potencial para ser utilizado con el propósito de recolectar inteligencia en los Estados Unidos o mejorar cualquier sistema de armas extranjero"[154].

El Secretario de Defensa y el Director de Inteligencia Nacional también deben cerciorarse de que[155]:

- Todos los datos recopilados o transmitidos desde estaciones de monitoreo en tierra cubiertas por la exención no estén encriptados.
- Todas las personas que participan en la construcción, operación y mantenimiento de esas estaciones de vigilancia en tierra sean personas de Estados Unidos.
- Esas estaciones de observación del terreno no se encuentran en la proximidad geográfica de lugares sensibles para la seguridad nacional de Estados Unidos.
- Se adopten medidas apropiadas para garantizar que dichas estaciones de vigilancia terrestre no supongan un espionaje cibernético u otra amenaza, incluida la inteligencia o la contrainteligencia, para la seguridad nacional de Estados Unidos.
- Cualquier mejora a tales estaciones de monitoreo terrestre no reduzca ni compita con las ventajas de la tecnología del Sistema de Posicionamiento Global para los usuarios.

Por otro lado, el Título 51 del Código de los Estados Unidos, sección 50112, establece que con el fin de apoyar y sostener el Sistema de Posicionamiento Global de una manera efectiva para la seguridad nacional, seguridad pública, los intereses científicos y económicos de Estados Unidos, se debe asegurar el funcionamiento del mismo en forma continua en todo el mundo sin cobro directo a los usuarios; celebrar acuerdos internacionales que promuevan la cooperación con gobiernos extranjeros y Organizaciones Internacionales para establecer el GPS y sus aumentos como una norma internacional aceptable; y por último, lograr y mantener una gestión eficiente del

[154] USCode, *10 USC 2281: Global Positioning System,* [en línea]. Dirección URL: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section2281&num=0&edition=prelim. [Fecha de consulta: 12 de septiembre de 2017].
[155] *Ídem.*

espectro electromagnético utilizado por el Sistema de Posicionamiento Global y a su vez, protegerlo de la interrupción y la interferencia[156].

El Título 49 del Código de los Estados Unidos, sección 301, autoriza el establecimiento del Sistema de Posicionamiento Global Diferencial a Nivel Nacional (NDGPS, por sus siglas en inglés). Este programa se implementa conjuntamente con la Administración Federal de Carreteras del Departamento de Transporte, la Administración Federal de Ferrocarriles y la Oficina del Secretario de Transporte; la Guardia Costera de los EE.UU. del Departamento de Seguridad Nacional; el Departamento de Comercio, el Laboratorio de Sistemas de Pronósticos y el Departamento de Defensa de la Fuerza Aérea y el Cuerpo de Ingenieros del Ejército.

El propósito del Sistema de Posicionamiento Global Diferencial a Nivel Nacional es proveer información precisa de posicionamiento y localización a viajeros, a unidades de respuesta de emergencias y a otros usuarios. El servicio de GPS ofrece sólo una precisión de navegación de entre 4 y 20 metros, lo que resulta insuficiente para muchos usos del transporte terrestre, es por esto, que el NDGPS ofrece un servicio de radio-navegación de uno a tres metros que satisface las necesidades de muchos más usuarios de transporte[157].

Al mejorar la precisión, la disponibilidad y la integridad del GPS, vigilando y emitiendo constantemente correcciones al servicio del mismo, el Sistema de Posicionamiento Global Diferencial a Nivel Nacional enriquece los sistemas de notificación de colisiones para evitar éstas entre vehículos y además, proporciona sistemas de guiado de ruta más precisos en medios de transporte. Todo esto se logra a través de una red de instalaciones terrestres llamadas estaciones de referencia[158].

---

[156] USCode, *51 USC 50112: Promotion of United States Global Positioning System standards,* [en línea]. Dirección URL: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title51-section50112&num=0&edition=prelim. [Fecha de consulta: 12 de septiembre de 2017].

[157] U.S. Department of Transportation, *Nationwide Differential Global Positioning System Program Fact Sheet,* [en línea]. Dirección URL: https://www.fhwa.dot.gov/publications/research/operations/02072/index.cfm. [Fecha de consulta: 14 de septiembre de 2017].

[158] El GPS diferencial utiliza la ubicación fija de una estación de referencia para determinar la inexactitud de la señal del satélite. La ubicación derivada de la señal de satélite se compara con la estación de referencia, esa diferencia, o inexactitud, puede entonces ser transmitida a receptores no estacionarios. Comparando la inexactitud con la señal de satélite, los receptores no estacionarios pueden determinar con precisión su ubicación. Cuanto más cercano al transmisor, más exacta es la determinación.
Al determinar esta corrección, las instalaciones de NDGPS también están monitoreando GPS para comportamiento anómalo. Cuando se identifica este comportamiento, las instalaciones de NDGPS transmitirán una advertencia a los usuarios para que no utilicen ese satélite.

El Secretario de Transporte es el responsable de administrar y operar el Sistema de Posicionamiento Global Diferencial a Nivel Nacional, asegurarse de que el servicio se proporciona sin la evaluación de cualquier tarifa de usuario, y en cooperación con el Secretario de Defensa, asegurar que su uso sea negado a cualquier enemigo de Estados Unidos. Asimismo, en cooperación con representantes de industrias privadas, universidades y funcionarios de los gobiernos de los Estados, puede investigar mejoras al sistema, desarrollar nuevas aplicaciones y proveer su mejoramiento continuo para atender las necesidades del Gobierno Federal; los gobiernos estatales y locales, y el público en general[159].

3.1.3. Financiamiento.

El Sistema de Posicionamiento Global es un sistema de usos múltiples propiedad del gobierno de los Estados Unidos y por lo tanto, es pagado por los contribuyentes del mismo país. Sin embargo, es el Departamento de Defensa quien lo opera y tiene la responsabilidad de desarrollarlo, sostenerlo y modernizarlo. Asimismo, le asigna al Departamento de Transporte la responsabilidad de financiar los costos adicionales asociados con nuevas actualizaciones civiles del GPS.

El 23 de diciembre de 2016, el entonces presidente Barack Obama firmó la Ley de Autorización de Defensa Nacional para el año fiscal 2017. La ley incluyó orientación de política y financiamiento para el programa del Sistema de Posicionamiento Global. La solicitud original de Obama para financiar el GPS durante el año 2017 fue de US$847,4 millones, sin incluir US$13,171 millones solicitados para el soporte en órbita de los satélites GPS Block IIF[160].

En marzo de 2017, el presidente Donald Trump solicitó fondos adicionales para el año fiscal 2017 para el Departamento de Defensa, incluyendo un aumento de US$37,3 millones para el desarrollo de los satélites GPS III y otro de US$120 millones para el Sistema de Control Operacional de Próxima Generación (OCX). La solicitud de presupuesto GPS total se convirtió en US$1,004.66 millones.[161]

---

[159] USCode, *49 USC 301: Leadership, consultation, and cooperation,* [en línea]. Dirección URL: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title49-section301&num=0&edition=prelim. [Fecha de consulta: 12 de septiembre de 2017].

[160] GPS, *Fiscal Year 2017 Program Funding,* [en línea]. Dirección URL: http://www.gps.gov/policy/funding/2017/. [Fecha de consulta: 13 de septiembre de 2017].

[161] *Ídem.*

El 5 de mayo de 2017, el Presidente Trump firmó la *Ley de Asignaciones o Apropiaciones Consolidadas* (Consolidated Appropriations Act) 2017[162], una medida de financiación que logró que el Congreso proporcionara US$908.262 millones[163] para financiar el programa GPS básico en el año fiscal 2017, finalizando éste el 30 de septiembre.

La solicitud de presupuesto del presidente Donald Trump para el año fiscal 2018 del Departamento de Defensa es de US$208.6 mil millones, de los cuales US$9.8 mil millones son destinados a los activos espaciales[164], es decir a todas aquellas herramientas que apoyan a las fuerzas estadounidenses desplegadas mediante la prestación de servicios de comunicaciones, capacidades de navegación e información recolectada por sensores remotos tales como satélites meteorológicos y sistemas de recolección de inteligencia.

Las fuerzas espaciales contribuyen a la efectividad general de las fuerzas militares estadounidenses actuando como un multiplicador de fuerza que potencia el poder de combate. Dentro de estos activos espaciales, se encuentra el Sistema de Posicionamiento Global, al que se le pretende atribuir US$1.1 mil millones para el año 2018[165].

3.1.4. Sistemas de aumento del GPS.

Un aumento del Sistema de Posicionamiento Global se refiere a "cualquier sistema que lo ayude proporcionando exactitud, integridad, disponibilidad o cualquier otra mejora al posicionamiento, navegación y sincronización que no es inherentemente parte del propio GPS"[166]. Los sectores público y privado han desarrollado una amplia gama de diferentes sistemas de aumento, para cumplir con requisitos específicos el gobierno de los Estados Unidos ha presentado varios sistemas de estos disponibles públicamente además del ya mencionado Sistema de Posicionamiento Global Diferencial a Nivel Nacional.

[162] Esta Acta tiene el fin de hacer las adecuaciones monetarias necesarias en los diferentes programas y departamentos del gobierno, desde la defensa, la agricultura, el comercio, la ciencia, tecnología, energía, salud, educación, trabajo, etc., para el año fiscal 2017.
[163] *Ídem.*
[164] GPS, *Fiscal Year 2018 Program Funding,* [en línea]. Dirección URL: http://www.gps.gov/policy/funding/2018/. [Fecha de consulta: 13 de septiembre de 2017].
[165] *Ídem.*
[166] GPS, *Augmentation Systems,* [en línea]. Dirección URL: http://www.gps.gov/systems/augmentations/. [Fecha de consulta: 13 de septiembre de 2017].

➢ Sistema de Ampliación de Área (WAAS, por sus siglas en inglés)[167].

Es un sistema regional de aumento basado en el espacio operado por la Administración Federal de Aviación y apoya la navegación de aviones en toda América del Norte. Este sistema de navegación es muy preciso y fue desarrollado para la aviación civil ya que proporciona servicio para todas las clases de aeronaves en todas las fases del vuelo, incluyendo la navegación en ruta, las salidas y las llegadas al aeropuerto.

Antes de este sistema, el Sistema Nacional de Espacio Aéreo de Estados Unidos no tenía el potencial de proporcionar navegación horizontal y vertical para operaciones de aproximación para todos los usuarios en todos los lugares, con el Sistema de Ampliación de Área esta capacidad es una realidad. Además, el servicio de este sistema es interoperable con otros servicios regionales basados en el espacio como los operados por Japón, Europa e India.

➢ Estaciones de Referencia de Operación Continua (CORS, por sus siglas en inglés)[168].

El Estudio Geodésico Nacional, una oficina del Servicio Nacional de Oceanografía, administra una red de Estaciones de Referencia de Operación Continua que proporcionan datos del Sistema Global de Navegación por Satélite (GNSS, por sus siglas en inglés) que consisten en mediciones y códigos de apoyo del posicionamiento tridimensional, meteorología, tiempo espacial y aplicaciones geofísicas en los Estados Unidos, sus territorios y algunos países extranjeros.

Los topógrafos, los ingenieros, los científicos y el público en general que recopilan datos GPS pueden utilizar los datos de las Estaciones de Referencia de Operación Continua para mejorar la precisión de sus posiciones. La red de estas estaciones es un esfuerzo cooperativo multiusos que involucra a organizaciones gubernamentales, académicas y privadas. Los sitios son de propiedad y operación independientes y cada agencia comparte sus datos y a su vez los analiza y distribuye de forma gratuita.

➢ Sistema de GPS Global Diferencial (GDGPS, por sus siglas en inglés)[169].

---

[167] Federal Aviation Administration, *Satellite Navigation - Wide Area Augmentation System (WAAS),* [en línea]. Dirección URL: https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/waas/. [Fecha de consulta: 14 de septiembre de 2017].

[168] National Geodetic Survey, *Continuously Operating Reference Station (CORS),* [en línea]. Dirección URL: https://www.ngs.noaa.gov/CORS/. [Fecha de consulta: 14 de septiembre de 2017].

El Sistema de GPS Global Diferencial es un Sistema Global de Navegación por Satélite de monitoreo y aumento completo, altamente preciso y extremadamente robusto en tiempo real. Fue desarrollado por la NASA para soportar los requisitos de posicionamiento y determinación en tiempo real de las misiones científicas y ha proporcionado servicios de datos de posicionamiento, navegación y temporización a las operaciones de la industria y el gobierno desde el año 2000, con una fiabilidad del 99,99%.

El sistema emplea una gran red terrestre de receptores de referencia en tiempo real, una arquitectura de red innovadora y un software de procesamiento de datos en tiempo real proporcionando una precisión de posicionamiento de subdímetro (<10 cm) y una precisión de transferencia de tiempo inferior al nanosegundo en cualquier parte del mundo, en tierra, en aire y en el espacio, independientemente de la infraestructura local. Los servicios de este sistema están disponibles para el GPS, el GLONASS[170], Galileo[171] y BeiDou[172].

- ➢ Servicio Internacional del Sistema Mundial de Navegación por Satélite (IGS, por sus siglas en inglés)[173].

El Servicio Internacional del Sistema Mundial de Navegación por Satélite es una red de más de 350 estaciones de monitoreo GPS de 200 organizaciones, universidades e instituciones de investigación contribuyentes en 80 países. Su misión es proporcionar datos y productos de la más alta calidad para los Sistemas Mundiales de Navegación por Satélite en apoyo de la investigación científica, la educación y el comercio.

3.1.5. Cooperación Internacional.

La *Política Nacional del Espacio* de 2010 lanzada por el gobierno de Barack Obama establece que Estados Unidos debe mantener su liderazgo en el servicio, suministro y uso de los Sistemas Mundiales de Navegación por Satélite[174]. No obstante, también fomenta

[169] NASA, *The Global Differential GPS System,* [en línea]. Dirección URL: http://www.gdgps.net/. [Fecha de consulta: 17 de septiembre de 2017].
[170] Las siglas GLONASS provienen de las palabras rusas *Global'naya Navigatsionnaya Sputnikovaya Sistema*, que traducidas al español se refieren al Sistema de Navegación Global por Satélite. Este sistema es el homólogo ruso del GPS.
[171] Galileo es el Sistema de Navegación Global por Satélite de Europa, sus primeros servicios se activaron en diciembre del año 2016 pero será hasta el año 2020 cuando esté plenamente operativo.
[172] Es el Sistema de Navegación Global por Satélite desarrollado por China, operativo desde el año 2000 y da servicio sólo a China y a sus países vecinos.
[173] IGS, *About,* [en línea]. Dirección URL: http://www.igs.org/about. [Fecha de consulta: 17 de septiembre de 2017].
[174] NASA, *National Space Policy of the United States of America,* [en línea], p.5. Dirección URL: https://www.nasa.gov/sites/default/files/national_space_policy_6-28-10.pdf. [Fecha de consulta: 17 de septiembre 2017].

la cooperación internacional relacionada con dichos sistemas y en especial con el Sistema de Posicionamiento Global:

"Se debe colaborar con proveedores extranjeros de Sistemas Mundiales de Navegación por Satélite para fomentar la compatibilidad y la interoperabilidad, promover la transparencia en la provisión de servicios públicos y permitir el acceso al mercado para la industria de los Estados Unidos"[175]. Entre los países y Organizaciones Internacionales que cooperan con el gobierno estadounidense se encuentran:

A. Australia.

La relación de cooperación Estados Unidos-Australia con relación al GPS y sistemas de aumento del mismo comenzó en el año 2007. Ambos países se encuentran trabajando para facilitar el uso amplio y eficaz de los sistemas de aumento que se pueden considerar como aumentos regionales civiles al GPS, la cooperación se ha centrado en los sistemas de transporte, especialmente en el campo de la aviación civil.

Los representantes de los servicios aéreos de Australia han desarrollado un Sistema de Aumento Regional Basado en Tierra (GBAS, por sus siglas en inglés) de la Organización de Aviación Civil Internacional (OACI, por sus siglas en inglés) para mejorar la gestión del tráfico aéreo y las operaciones regionales de aeronaves, así como otras aplicaciones civiles y comerciales. Estados Unidos a través de su Administración Federal de Aviación y Australia, a través de *Airservices Australia*, están coordinando esfuerzos para asegurar la interoperabilidad entre el GPS y el Sistema de Aumento Basado en Tierra de Australia.

B. Comité Internacional de Sistemas Globales de Navegación por Satélite (ICG, por sus siglas en inglés).

El Comité Internacional de Sistemas Globales de Navegación por Satélite creado en 2005 bajo la égida de las Naciones Unidas, promueve la coordinación entre los proveedores de Sistemas Mundiales de Navegación por Satélite, los sistemas regionales y las ampliaciones a fin de garantizar una mayor compatibilidad, interoperabilidad y transparencia y promover la introducción y utilización de estos servicios y sus mejoras

[175] *Ídem.*

futuras, incluso en los países en desarrollo mediante la asistencia y si es necesario, con la integración en sus infraestructuras[176].

El ICG también sirve para ayudar a los usuarios de Sistemas Mundiales de Navegación por Satélite con sus planes y aplicaciones de desarrollo, alentando la coordinación y sirviendo como un punto focal para el intercambio de información. Además, tiene como misión "asegurar el mejor posicionamiento basado en satélites, la navegación y el tiempo para usos pacíficos para todo el mundo, en cualquier lugar y en cualquier momento"[177]. El Comité Internacional está abierto a los Estados miembros de las Naciones Unidas, Organizaciones Internacionales o Entidades internacionales responsables de Sistemas Mundiales de Navegación por Satélite y sus aumentos.

Hay tres categorías de participantes en el Comité: Miembros, Miembros Asociados y Observadores. Entre los miembros se encuentran los proveedores actuales y futuros de sistemas básicos, entre ellos China (Sistema de Satélite de Navegación Beidou), la Unión Europea (Sistema Europeo de Navegación por Satélite Galileo), Rusia (GLONASS) y Estados Unidos de América (Sistema de Posicionamiento Global), además de los Estados miembros de Naciones Unidas con un programa activo de aplicación o promoción de una amplia gama de servicios y aplicaciones de los Sistemas Mundiales de Navegación por Satélite (Italia, Malasia y Emiratos Árabes Unidos por ejemplo).

Entre los miembros asociados se encuentran Organizaciones y Asociaciones Internacionales y regionales que se ocupan de los servicios y aplicaciones de los Sistemas Mundiales de Navegación por Satélite como la Oficina de Asuntos del Espacio Ultraterrestre de la Secretaría de las Naciones Unidas, el Sistema Europeo de Determinación de la Posición (EUPOS, por sus siglas en inglés) y la Federación Aeronáutica Internacional, la Asociación Internacional de Geodesia (IAG, por sus siglas en inglés), la Asociación Cartográfica Internacional (ICA, por sus siglas en inglés), el Servicio Internacional de Rotación de Tierra y Sistemas de Referencia (IERS, por sus siglas en inglés) y la Sociedad Internacional de Fotogrametría y Teledetección (ISPRS, por sus siglas en inglés).

[176] United Nations Office for Outer Space Affairs, *International Committee on Global Navigation Satellite Systems (ICG),* [en línea]. Dirección URL: http://www.unoosa.org/oosa/en/ourwork/icg/icg.html. [Fecha de consulta: 18 de septiembre de 2017].
[177] *Ídem.*

Mientras que dentro de los observadores se encuentra el Instituto Árabe de Navegación (AIN, por sus siglas en inglés), el Comité de Investigaciones Espaciales (COSPAR, por sus siglas en inglés), la Oficina Internacional de Pesos y Medidas (BIPM, por sus siglas en inglés), el Instituto Europeo de Políticas Espaciales (ESPI, por sus siglas en inglés), la Asociación Internacional de Institutos de Navegación (IAIN, por sus siglas en inglés), la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), el Grupo Consultivo Interinstitucional de Operaciones (IOAG, por sus siglas en inglés) y la Unión Radio-Científica Internacional (URSI, por sus siglas en inglés).

C. China.

Desde 2006 Estados Unidos y la República Popular China han estado discutiendo asuntos de interés mutuo relacionados con el Sistema de Posicionamiento Global y el Sistema de Navegación por Satélite Compass/BeiDou (BDS), un proyecto desarrollado de manera independiente por China con miras a satisfacer las necesidades de seguridad nacional del país y de desarrollo económico y social.

En el año 2014, se iniciaron consultas bilaterales sobre cooperación civil en relación con el GPS y BeiDou. Ambas partes discutieron la cooperación en materia de desarrollo, compatibilidad e interoperabilidad de señales civiles entre BeiDou y GPS, sus respectivos sistemas de aumento y aplicaciones de aviación civil, monitoreo y evaluación, protección del espectro, detección y mitigación de interferencias, y actividades relacionadas a la OACI, la Organización Marítima Internacional, la UIT y otros foros internacionales multilaterales conexos.

Además, se acordó establecer un intercambio regular, con la cooperación continua a través de reuniones periódicas. No obstante, es necesario destacar que aunque BeiDou está operativo desde el año 2000 y se pretende que para el 2020 pueda proveer servicios a nivel mundial, hoy en día sólo provee servicios a la región de Asia Pacífico.

Para finales de 2012 se habían lanzado un total de 14 satélites (5 satélites de órbita terrestre geoestacionaria, 5 satélites de órbita de geosincrónica inclinada y 4 satélites de órbita terrestre media) esto quiere decir que su segmento espacial es una constelación híbrida que consta de satélites en tres tipos de órbitas, mejorando así la

precisión del servicio mediante el uso de señales combinadas de múltiples frecuencias. Se espera que para el año 2020 BeiDou cuente con 35 satélites.

A pesar de que el gobierno chino ha destacado la cooperación internacional entre ambos Sistemas Mundiales de Navegación por Satélite y la compatibilidad e interoperabilidad de su sistema con los demás, no hay que dejar de lado que en realidad lo que se busca es contar con una industria de navegación por satélite independiente e innovadora que permita colocar a BeiDou como un competidor fuerte frente al GPS e incluso, llegar a superarlo.

D. Unión Europea.

Galileo es el sistema mundial de navegación por satélite europeo y empezó a ofrecer sus servicios avanzados de posicionamiento, navegación y temporización a las autoridades públicas, las empresas y los ciudadanos europeos el 15 de diciembre de 2016. En la actualidad, la constelación Galileo ya tiene 18 satélites, todos los cuales están en órbita, se prevé que toda la constelación tenga 30 satélites y esté completa en el año 2020. Los servicios iniciales de Galileo los gestiona la Agencia de los Sistemas Mundiales de Navegación por Satélite Europea (GSA, por sus siglas en inglés).

Estados Unidos y la Unión Europea han sido socios estrechos en el ámbito de la navegación por satélite desde 2004 cuando firmaron el Acuerdo sobre la Promoción, Disposición y Uso de Sistemas de Navegación basados en los Satélites de Galileo y GPS y Aplicaciones Relacionadas. La cooperación tiene por objeto garantizar que el GPS y Galileo sean interoperables a nivel de usuario para beneficio de los usuarios civiles de todo el mundo.

Ambas partes en dicho acuerdo se comprometen a trabajar conjuntamente tanto en los foros bilaterales como multilaterales para promover y facilitar el uso de estas señales, servicios y equipos para usos civiles, comerciales y científicos pacíficos, compatibles con la seguridad e intereses mutuos. El Acuerdo GPS-Galileo estableció grupos de trabajo para la cooperación sobre:

- Compatibilidad e interoperabilidad de radiofrecuencias
- Aplicaciones comerciales y civiles
- Diseño y desarrollo de la próxima generación de sistemas

En el artículo 7 del acuerdo, se establece que excepto por razones de seguridad nacional, tanto Estados Unidos como la Unión Europea no deben restringir ni el uso ni el acceso a la información de posicionamiento, navegación y temporización de sus respectivos servicios abiertos por parte de los usuarios finales[178]. El último informe (2016) sobre la cooperación identifica tres áreas principales de trabajo para el período 2016-2018: contribuciones a las actividades de desarrollo de normas, desarrollo de prototipos y pruebas para algoritmos terrestres y aéreos y desarrollo de requisitos de proveedores de compatibilidad.

El conjunto del programa Galileo es gestionado por la Comisión Europea, que ha transferido a la Agencia Espacial Europea la responsabilidad del despliegue del sistema y del apoyo técnico a las tareas operativas. La interoperabilidad de Galileo con GPS es total, pero Galileo ofrecerá un posicionamiento más preciso y fiable a los usuarios finales, asimismo, también se pretende que sea compatible con el sistema ruso y chino. Como BeiDou, Galileo es el intento de Europa por contar con su sistema de navegación por satélite independiente, y aunque hoy en día depende del GPS se espera que en el futuro también llegue a superarlo.

E. Japón.

Los Estados Unidos y Japón han tenido una relación exitosa con la navegación por satélite desde 1998, cuando los jefes de ambas naciones firmaron una Declaración Conjunta que establecía una cooperación en el uso del GPS. A través de esta relación, las dos naciones han logrado la interoperabilidad entre el GPS y el Sistema de Aumento de Satélites basado en Satélites de Transporte Multifuncional de Japón (MTSAT, por sus siglas en inglés), un satélite geoestacionario similar al Sistema de Ampliación de Área.

Las naciones también han tomado medidas para asegurar la interoperabilidad entre la constelación de GPS de próxima generación y el Sistema de Satélites *Quasi-Zenith* de Japón (QZSS), una constelación regional de satélites diseñada para complementar el GPS en Asia Oriental. Hay que destacar que Japón es uno de los países con los que el gobierno estadounidense ha tenido un mayor número de reuniones

[178] GPS, *Agreement on the Promotion, Provision and Use of Galileo and GPS Satellite-Based Navigation Systems and Related Applications,* [en línea], p. 14. Dirección URL: http://www.gps.gov/policy/cooperation/europe/2004/gps-galileo-agreement.pdf. [Fecha de consulta: 18 de septiembre de 2017].

para dialogar sobre la cooperación en temas no sólo relacionados al GPS, si no en cuanto a políticas espaciales en general.

F. India.

Estados Unidos y la India emitieron una declaración conjunta en 2007 que establecía la cooperación en GPS y aumentos de GPS. India está desarrollando su propia plataforma de aumento basado en el espacio denominada Sistema de Navegación Aumentada por GPS y GEO (GAGAN, por sus siglas en inglés), la cual mejorará significativamente la gestión del tráfico aéreo y las operaciones de aviones regionales en el sur de Asia, así como otras aplicaciones civiles y comerciales.

Los dos gobiernos trabajan en estrecha colaboración para facilitar el uso amplio y efectivo del Sistema de Ampliación de Área y el Sistema de Navegación Aumentada por GPS y GEO como sistemas regionales de aumento civiles basados en el espacio para el GPS. También cooperan en el establecimiento de mecanismos internacionales como el Comité Internacional de Sistemas Globales de Navegación por Satélite para promover el uso de los mismos especialmente en los países en desarrollo.

Por otro lado, India se encuentra desarrollando hoy en día su propio sistema de navegación por satélite regional conocido como *IRNSS,* por sus siglas en inglés, es decir Sistema de Navegación por Satélite Regional de la India o también conocido como Constelación India de Navegación (NavIC, por sus siglas en inglés) conformado por siete satélites. Está diseñado para proporcionar un servicio preciso de información de posición a los usuarios en la India y en la región que se extiende hasta 1500 km de su límite, que es su área de servicio principal. NavIC proporcionará dos tipos de servicios, el Servicio de Posicionamiento Estándar (SPS, por sus siglas en inglés) que se proporciona a todos los usuarios y el Servicio Restringido, que es un servicio encriptado proporcionado sólo a los usuarios autorizados.[179]

G. Rusia.

Estados Unidos y Rusia iniciaron la cooperación en 2004, con el objetivo principal de permitir la interoperabilidad civil a nivel de usuario entre el GPS y el sistema GLONASS

[179] Indian Space Research Organisation, *Indian Regional Navigation Satellite System (IRNSS):NavIC,* [en línea], Department of Space. Dirección URL: https://www.isro.gov.in/irnss-programme. [Fecha de consulta: 21 de septiembre de 2017].

de Rusia. Aunque ambas partes reiteraron su compromiso de proseguir estas conversaciones para seguir proporcionando las señales civiles GPS y GLONASS apropiadas para el uso comercial y científico, a partir de abril de 2014, toda la cooperación entre Estados Unidos y Rusia en esta área está en suspenso sin exponer los motivos públicamente.

Las pruebas de vuelo del sistema ruso de navegación por satélite de alta órbita, llamado GLONASS, se iniciaron en octubre de 1982 con el lanzamiento del satélite *Kosmos-1413*. El sistema GLONASS fue oficialmente declarado operativo en 1993 y dos años después se declaró una constelación completamente operativa que contaba con 24 satélites GLONASS de la primera generación[180].

La reducción de los fondos para la industria espacial en 1990 llevó a la degradación de la constelación GLONASS. En 2002 la constelación de GLONASS consistió en 7 satélites que eran insuficientes para el apoyo de la navegación del territorio ruso incluso con disponibilidad limitada. Las cosas mejoraron cuando el programa federal *Sistema Global de Navegación para 2002-2011* fue adoptado y lanzado en 2002 ya que el sistema GLONASS se conservó, se modernizó y comenzó a funcionar con los satélites *GLONASS-K*.

Hoy en día GLONASS cuenta con 26 satélites en su constelación y el gobierno ruso trabaja en la mejora de su capacidad con el fin de lograr la paridad con los Sistemas Internacionales de Navegación por Satélite y conseguir el liderazgo en la navegación por satélite en beneficio de la defensa, la seguridad y el desarrollo social y económico del país, dando a notar a su vez, la gran rivalidad con Estados Unidos y el GPS.

3.1.6. Usos y aplicaciones.

Los satélites del Sistema de Posicionamiento Global proporcionan servicios a usuarios civiles y militares. Como se ha mencionado a lo largo de esta investigación, el servicio a civiles es gratuito y está a disposición de todos los usuarios de manera permanente y global. Al igual que internet, el GPS es un elemento esencial de la infraestructura mundial de la información.

[180] Information and Analysis Center for Positioning, Navigation and Timing, *GLONASS History,* [en línea]. Dirección URL: https://www.glonass-iac.ru/en/guide/index.php. [Fecha de consulta: 21 de septiembre de 2017].

La naturaleza libre y confiable del GPS ha llevado al desarrollo de cientos de aplicaciones que afectan a todos los aspectos de la vida moderna, la tecnología GPS está ahora en todo, desde teléfonos celulares hasta cajeros automáticos, aviones, contenedores de envío y armas. El GPS aumenta la productividad en una amplia franja de la economía en sectores como la agricultura, construcción, minería, topografía, navegación marítima, aviación, las redes de comunicaciones, sistemas bancarios, mercados financieros y redes eléctricas dependen en gran medida del GPS.

La combinación del GPS con los sistemas de información geográfica ha desarrollado la "agricultura de precisión" en la que la tecnología se aplica en la planificación de cultivos, el levantamiento de mapas topográficos, muestreo de los suelos, la orientación de tractores, exploración de cultivos y mapas de rendimiento. Además, el GPS permite "determinar el posicionamiento exacto de infestaciones de plagas, insectos y malezas y ayuda a que los agricultores puedan trabajar en condiciones de baja visibilidad en los campos (con lluvia, polvo, niebla o penumbra)"[181].

En la aviación, los pilotos utilizan el Sistema de Posicionamiento Global para "elevar la seguridad y la eficiencia de sus vuelos, el posicionamiento y la navegación hacen posible la determinación tridimensional de la posición para todas las fases del vuelo, desde el despegue, el vuelo en ruta y el aterrizaje, hasta el movimiento sobre la superficie del aeropuerto"[182].

Vía terrestre, la disponibilidad y precisión del GPS ayuda a la eficiencia y seguridad de los vehículos ya que permite conocer su ubicación, información que en casos de emergencia o simplemente en servicios al cliente como la hora de llegada de un autobús, es de mucha utilidad. Además, el GPS puede ser empleado en la inspección del estado de las redes de carreteras y autopistas mediante la identificación de ciertas facilidades en ellas o en las proximidades, incluidas gasolineras, servicios y suministros de mantenimiento y de emergencias, y rampas de entrada y salida, los daños al sistema de viales, etc.

En la navegación marítima el GPS les permite a los marineros navegar de forma segura, medir su velocidad y determinar su posición con mayor eficiencia. Marineros y

[181] GPS, *Agricultura,* [en línea]. Dirección URL: http://www.gps.gov/applications/agriculture/spanish.php. [Fecha de consulta: 22 de septiembre de 2017].
[182] GPS, *Aviación,* [en línea]. Dirección URL: http://www.gps.gov/applications/aviation/spanish.php. [Fecha de consulta: 22 de septiembre de 2017].

oceanógrafos emplean la información obtenida con el GPS para la topografía submarina, la colocación de boyas y la localización de peligros para la navegación y su señalamiento en cartas náuticas.

En los puertos la tecnología del GPS en colaboración con sistemas de información geográfica (GIS, por sus siglas en inglés) es clave para la gestión y operación eficientes de la ubicación automática de contenedores. El Sistema de Posicionamiento Global "permite seguir éstos desde su entrada en el puerto hasta su salida, lo que facilita la automatización del proceso de recogida, transferencia y colocación de los contenedores"[183].

El GPS apoya también a la cartografía y la modelización del mundo físico, desde montañas, bosques y ríos, hasta calles, edificios, cables y tuberías de los servicios públicos y otros recursos. Las superficies medidas con esta tecnología se pueden visualizar en mapas y en sistemas de información geográfica que almacenan, manipulan y visualizan los datos obtenidos. Los gobiernos, las organizaciones científicas y las operaciones comerciales de todo el mundo utilizan la combinación de estos elementos para facilitar la toma oportuna de decisiones y el uso racional de los recursos.

De igual modo, el medio ambiente se ve beneficiado por el uso del GPS al poder llevar a cabo estudio aéreos de las zonas más impenetrables para evaluar su flora y fauna, topografía e infraestructura humana, permitiendo a su vez la planificación de estrategias para la conservación.

En un ámbito más recreativo, el Sistema de Posicionamiento Global ha eliminado muchos de los peligros asociados con actividades como el senderismo, ciclismo y todo tipo de deportes al aire libre, ya que ha ido desplazando los mapas impresos, la brújula y los puntos de referencia, al permitir al usuario saber con precisión dónde se encuentra en todo momento.

Las labores de rescate en caso de emergencia ya sea por las actividades descritas anteriormente o por cualquier otro motivo, son beneficiadas por el uso del GPS ya que el conocimiento de la ubicación exacta desde calles, edificios, carreteras,

[183] GPS, *Navegación marítima,* [en línea]. Dirección URL: http://www.gps.gov/applications/agriculture/spanish.php. [Fecha de consulta: 22 de septiembre de 2017].

bosques, etc., permite a los servicios de emergencia y a los centros de rescate reducir el tiempo del mismo y así proteger y salvar vidas.

Además de la longitud, latitud y altitud, el Sistema de Posicionamiento Global proporciona una cuarta dimensión: la cronometría. Cada satélite de la constelación GPS contiene múltiples relojes atómicos que contribuyen con datos horarios muy precisos a las señales del GPS, estos datos horarios son vitales para toda una serie de actividades económicas alrededor del mundo.

Los sistemas de comunicación, redes de distribución eléctrica y redes financieras dependen de la hora precisa para sincronizarse y operar con eficiencia. "Negocios grandes y pequeños están recurriendo a sistemas automatizados capaces de rastrear, actualizar y gestionar transacciones múltiples realizadas por una red mundial de clientes, que necesitan información exacta de la hora que es posible obtener con el GPS"[184].

Si el GPS es imprescindible y de mucha ayuda en tierra, mar y aire, no podía dejar de serlo en su ubicación principal: el espacio. El Sistema de Posicionamiento Global "está revolucionando y revitalizando la forma como las naciones operan en el espacio, desde los sistemas de orientación para vehículos tripulados pasando por la gestión, seguimiento y control de constelaciones de satélites de comunicaciones, hasta la observación de la Tierra desde el espacio"[185].

Para concluir pero no menos importante, el Sistema de Posicionamiento Global es un sistema crítico para la seguridad nacional de Estados Unidos, no sólo porque está presente en diferentes infraestructuras críticas y es *per sé* una de ellas, sino porque sus aplicaciones están integradas en prácticamente todas las facetas de las operaciones militares de los Estados Unidos, pues la mayoría de los nuevos activos militares desde vehículos hasta municiones, vienen equipados con GPS.

3.2. La Seguridad Nacional de Estados Unidos en riesgo: la vulnerabilidad del GPS.

La utilización del espacio ha desaparecido fronteras, creado nuevos mercados y operaciones financieras, ha ayudado a recopilar información geoespacial, a facilitar el pronóstico del tiempo, a prever desastres naturales, a agilizar operaciones de búsqueda y

[184] GPS, *Cronometría,* [en línea]. Dirección URL: http://www.gps.gov/applications/timing/spanish.php. [Fecha de consulta: 23 de septiembre de 2017].
[185] GPS, *Espacio,* [en línea]. Dirección URL: http://www.gps.gov/applications/space/spanish.php. [Fecha de consulta: 23 de septiembre de 2017].

rescate, a mejorar la gestión de los recursos naturales, a aumentar el conocimiento en muchos campos científicos y a ampliar y mejorar las comunicaciones. También, se ha vuelto un campo de batalla al permitir la modernización de armas y el uso de avanzada tecnología en ellas.

Es decir gracias a la infraestructura espacial se desarrollan decenas de actividades en todo el mundo, su naturaleza interconectada y la creciente dependencia de ella significa que actos irresponsables en el espacio pueden tener consecuencias perjudiciales para todos. El espacio puede dar la impresión de ser un reino intocable y 100% seguro pero a medida que los sistemas y las redes que dependen de él van en aumento también crecen los riesgos[186] en cuestiones de ciberseguridad, los posibles impactos de la pérdida de capacidades espaciales serían fatales para cualquier gobierno, empresa u organización internacional.

Estados Unidos de acuerdo con su *Política Espacial Nacional* del año 2010 considera la sostenibilidad, la estabilidad y el libre acceso y uso del espacio, vital a sus intereses nacionales. Reconoce también que "todas las naciones tienen derecho a explorar y utilizar el espacio con fines pacíficos y en beneficio de toda la humanidad de conformidad con el derecho internacional, y que respetando el mismo principio, se permite utilizar el espacio para actividades de seguridad nacional"[187].

Es por lo anterior que el gobierno estadounidense considera la interferencia intencional con los sistemas espaciales incluida la infraestructura de apoyo como una violación a los derechos de una nación. Asimismo, declara en su *Política Espacial Nacional* que "utilizará una serie de medidas para garantizar el uso responsable del espacio y de acuerdo con el derecho inherente a la autodefensa, disuadir a otros de la interferencia y el ataque, además de defender sus sistemas espaciales y contribuir a la defensa del espacio aliado, y si la disuasión fracasa, atacarlos"[188].

La vulnerabilidad a los ciberataques de los satélites y otros activos que forman parte de la infraestructura crítica espacial no es un terreno que se haya explorado de manera profunda en los debates acerca de las amenazas cibernéticas a la infraestructura nacional crítica; ejemplo de ello son los pocos documentos existentes de

[186] El riesgo se define como la posibilidad de un resultado no deseado resultante de un incidente, evento u ocurrencia, según lo determinen su probabilidad y las consecuencias asociadas.
[187] NASA, *National Space Policy of the United States of America,* Op. Cit.
[188] *Ídem.*

análisis al respecto. La intersección entre seguridad espacial y ciberseguridad es una preocupación de seguridad nacional, regional e internacional y su análisis es fundamental para comprender esta amenaza de seguridad no tradicional y en evolución.

Desde 1998 se formó una Comisión que recibió instrucciones de evaluar la organización y la gestión de las actividades espaciales en apoyo de la seguridad nacional de los Estados Unidos. Los miembros de la Comisión fueron nombrados por los presidentes y los miembros de los Comités de Servicios Armados de la Cámara y el Senado y por el Secretario de Defensa en consulta con el Director de la Central de Inteligencia.

La Comisión emitió el *Informe de la Comisión para Evaluar la Gestión y Organización de la Seguridad Nacional del Espacio de Estados Unidos* en el que concluyó que "la seguridad y el bienestar del país, sus aliados y amigos dependían de la capacidad de la nación para operar en el espacio por lo que era de interés nacional el promover el uso pacífico del espacio; el utilizar el potencial de la nación en el espacio para apoyar sus objetivos de seguridad nacional, económica, diplomática y nacional; y desarrollar y desplegar los medios para disuadir y defenderse contra los actos hostiles dirigidos a los activos espaciales de Estados Unidos"[189].

Además, se incluyeron hechos considerados como "señales de advertencia" de la vulnerabilidad de Estados Unidos entre ellos:

1. En 1998, el satélite *Galaxy IV* funcionó mal y apagó el 80% de los *buscapersonas* de Estados Unidos así como las transmisiones de televisión por cable, las redes de autorización de tarjetas de crédito y los sistemas de comunicaciones corporativos. Para restaurar el servicio satelital, los satélites tuvieron que ser movidos y miles de antenas de tierra tuvieron que ser reposicionadas manualmente, lo que llevó semanas en algunos casos.
2. A principios del año 2000 Estados Unidos perdió toda la información de varios de sus satélites durante tres horas cuando las computadoras de las estaciones terrestres no funcionaban correctamente.

[189] Defense Technical Information Center, *Report to the Commission to Assess United States National Security Space Management and Organization,* [en línea], 11 de enero de 2001, p. XV. Dirección URL: http://www.dtic.mil/docs/citations/ADA404328. [Fecha de consulta: 20 de octubre de 2017].

3. También en el 2000 la agencia de noticias *Xinhau* informó que el ejército de China estaba desarrollando métodos y estrategias para derrotar al ejército de Estados Unidos en una guerra futura de alta tecnología y espacio. Señaló que para los países que nunca podrían ganar una guerra utilizando el método de tanques y aviones, atacar el sistema espacial de EE.UU. podía ser una opción irresistible y más tentadora.

En el mismo documento se destaca que si el Sistema de Posicionamiento Global experimentara fallas o interrupciones generalizadas, el impacto podría ser grave. La pérdida del tiempo del GPS podría desactivar las comunicaciones de la policía, los bomberos y las ambulancias en todo el mundo; perturbar el sistema bancario y financiero mundial que depende de la sincronización del GPS para mantener conectados a los centros financieros mundiales; e interrumpir el funcionamiento de los sistemas de distribución de energía eléctrica[190].

En el año 2001 fue la primera vez que se reconoció que Estados Unidos dependía más del espacio que cualquier otra nación por lo que sus activos espaciales eran candidatos atractivos para atacar. No obstante, la evaluación de los riesgos y las amenazas a las capacidades espaciales de los Estados Unidos carecían de prioridad por parte de los departamentos y agencias del gobierno encargados de las responsabilidades de la seguridad nacional.

Esta serie de hechos y preocupaciones sobre el futuro de los satélites también se vieron reflejadas cuando el Departamento de Transporte de Estados Unidos publicó en agosto de 2001 la *Evaluación de Vulnerabilidad de la Infraestructura de Transporte basándose en el Sistema de Posicionamiento Global*, un informe elaborado por su Centro Nacional de Sistemas de Transporte John A. Volpe.

En este informe el Departamento de Defensa reconoce que existen vulnerabilidades en el GPS y que a medida que el conocimiento de los usos militares del mismo y sus vulnerabilidades se generaliza cada vez más, la milicia está implementando

[190] Defense Technical Information Center, *Op. Cit.*

capacidades para proteger sus sistemas críticos y para cumplir su mandato de protegerse a sí mismo y a los Estados Unidos de cualquier tipo de fuerza hostil[191].

El informe del Centro Volpe identifica vulnerabilidades en el sistema de GPS en ese momento como el empleo de señales de muy baja potencia y analiza su interrupción involuntaria como la interferencia ionosférica, la actividad solar y la interferencia de radiofrecuencia de la televisión abierta, dispositivos electrónicos personales, sistemas de comunicaciones móviles por satélite, entre otros. También discute interrupciones intencionales en cada uno de los diferentes sistemas de transporte como el "apagado" a través de ataques a los satélites, la interferencia, la suplantación y la interferencia de señales.

El informe al final recomienda continuar la modernización del GPS y los esfuerzos para su protección reconociendo a su vez que a medida que la penetración del GPS en la infraestructura civil es mayor, se convierte en un objetivo cada vez más tentador que podría ser explotado por personas o países. Esta Evaluación de Vulnerabilidad de la Infraestructura de Transporte basándose en el Sistema de Posicionamiento Global fue un evento decisivo para el futuro del GPS pues se convirtió en una llamada de atención para los usuarios del mismo y de los Sistemas Globales de Navegación por Satélite a nivel mundial.

El alto grado de interconexión entre los satélites y la infraestructura crítica terrestre plantea serios riesgos para ambos y a su vez para la sociedad que requiere de los servicios que éstos proporcionan para el desarrollo de su vida diaria. Es por esto que un ataque cibernético a las infraestructuras espaciales que provoque una interrupción en su funcionamiento se convierte en una nueva clase de riesgo potencialmente catastrófico.

Las consecuencias de un ciberataque a los satélites son diversas, lo que forza a que los mecanismos de respuesta sean lo suficientemente flexibles y capaces para

[191] Coast Guard Navigation Center, *Vulnerability Assessment of the Transportation Infrastructure relying on the Global Positioning System,* [en línea], John A. Volpe National Transportation Systems Center, August 29, 2001, p. 2. Dirección URL: https://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf. [Fecha de consulta 19 de octubre de 2017].

hacer frente a la naturaleza impredecible de los mismos, entre las más importantes se encuentran[192]:

- Reducción de la seguridad nacional o capacidad de defensa.
- Reducción de la capacidad de las comunicaciones, la capacidad de observación o la precisión de la navegación.
- Corrupción de las comunicaciones, incluidos los sistemas de cronometraje precisos, que llevan a la falta de confianza.
- Destrucción de un vehículo espacial.
- Corrupción o eliminación de datos que se transmiten desde satélites.
- Intercepción de comunicaciones que incluye información sensible.
- Cambio de ruta de las comunicaciones para permitir una intercepción más fácil.

El ciclo de vida de la tecnología en satélites es completamente diferente al de la mayoría de las utilizadas en la infraestructura crítica. Generalmente la tecnología empleada en su creación está diseñada para que puedan tener vidas útiles muy largas lo que ocasiona que la misma se vuelva obsoleta con el paso del tiempo aumentando así su exposición a riesgos de tipo cibernético. El ritmo al que evoluciona la tecnología hace que sea difícil o incluso imposible, idear una respuesta oportuna y capaz de combatir al 100% las ciberamenazas espaciales.

Los ataques cibernéticos en satélites pueden ser de diferentes tipos, como[193]:

➔ Interferencia.

Es un intento de degradar e interrumpir la conectividad al interferir con las señales que son los medios para la comunicación. Normalmente se asocia con interferencia intencional en la transmisión y recepción de señales, y se ha utilizado durante muchas décadas mediante el uso deliberado del ruido de radio y las señales electromagnéticas en un intento de interrumpir las comunicaciones. Un dispositivo de interferencia normalmente transmite energía electromagnética en las mismas bandas de frecuencia de radio que la

[192] David, Livingstone; Patricia, Lewis, *Space, the Final Frontier for Cybersecurity?,* [en línea], Chatham House, The Royal Institute of International Affairs, September 2016, p. 13. Dirección URL: https://www.chathamhouse.org/publication/space-final-frontier-cybersecurity. [Fecha de consulta: 30 de septiembre de 2017].

[193] *Ibídem,* p. 16.

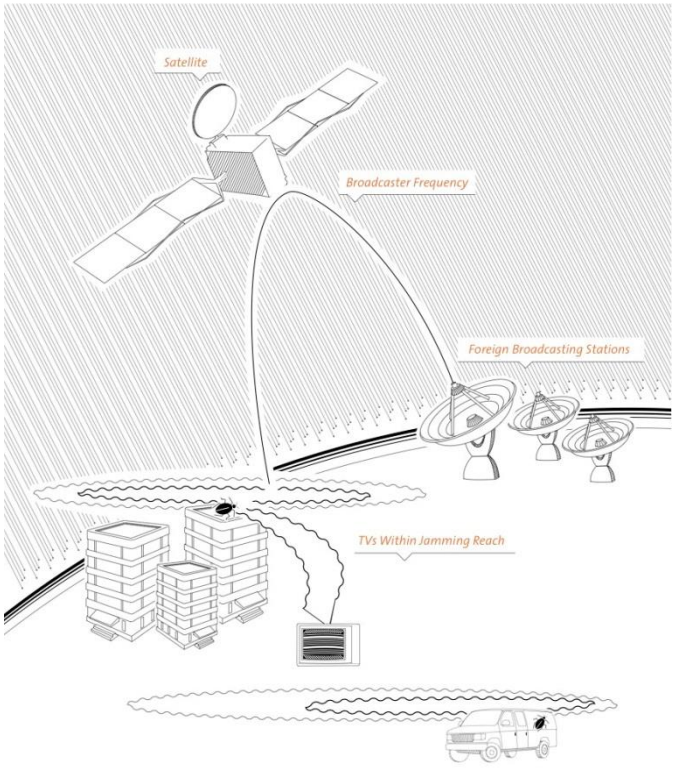
señal transmitida deseada, interrumpiendo la capacidad de un receptor para recuperar con precisión la señal transmitida.

En el caso específico de los servicios satelitales las señales pueden bloquearse en el "enlace descendente" entre satélites y receptores conocida como interferencia terrestre, o en el "enlace ascendente" es decir entre estaciones terrestres transmisoras y satélites llamada interferencia orbital. La primera afecta la capacidad operativa de los receptores ubicados en regiones geográficas específicas y es una técnica que se ha utilizado durante muchos años, por ejemplo, por gobiernos autoritarios que intentan evitar que las personas accedan a transmisiones de radio o televisión no autorizadas.

Durante los períodos de inquietud y control político, la recepción de radio y televisión y en tiempos más recientes el acceso a las redes de telefonía móvil e internet se ha bloqueado en varios países a través de la interferencia terrestre permitiendo que los gobiernos mantengan el control sobre la información disponible y la comunicación. Los aparatos utilizados para interferir las señales pueden ser económicos, fáciles de usar y de conseguir pues se pueden comprar en internet por menos de 50 dólares.

El alcance de uno de estos aparatos (conocidos como *jammer*) depende de su potencia, las condiciones atmosféricas, la topografía y el rendimiento de los receptores. El bloqueo de señales de Sistemas Globales de Navegación por Satélite es también uno de los usos más frecuentes de los *jammers* pues pueden interferir con los sistemas de informe de posición de las unidades de respuesta de servicio de emergencia por ejemplo.

Imagen 3.2. Interferencia terrestre.

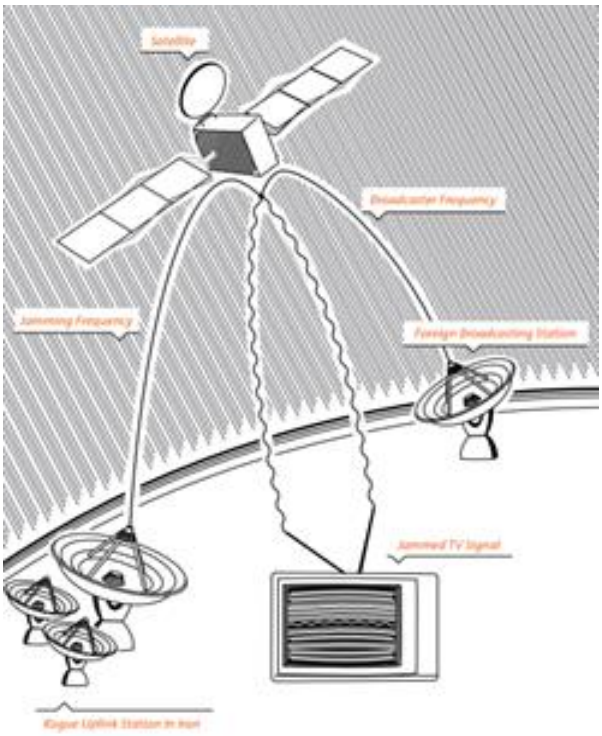


Tomada de Infosec Institute, *Hacking Satellites … Look Up to the Sky,* [en línea]. Dirección URL: http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref.

Por otra parte, la interferencia orbital degrada la calidad de la señal que se transmite por una estación terrestre hacia un satélite. El perturbador no necesariamente tiene que estar cerca del transmisor sino que podría ubicarse en cualquier lugar dentro del área de la Tierra que cubre el satélite, asimismo, la extensión geográfica de la interferencia orbital no se limita a la ubicación física del bloqueador, sino que afecta a toda la región geográfica en la que el satélite está destinado a ofrecer servicio.

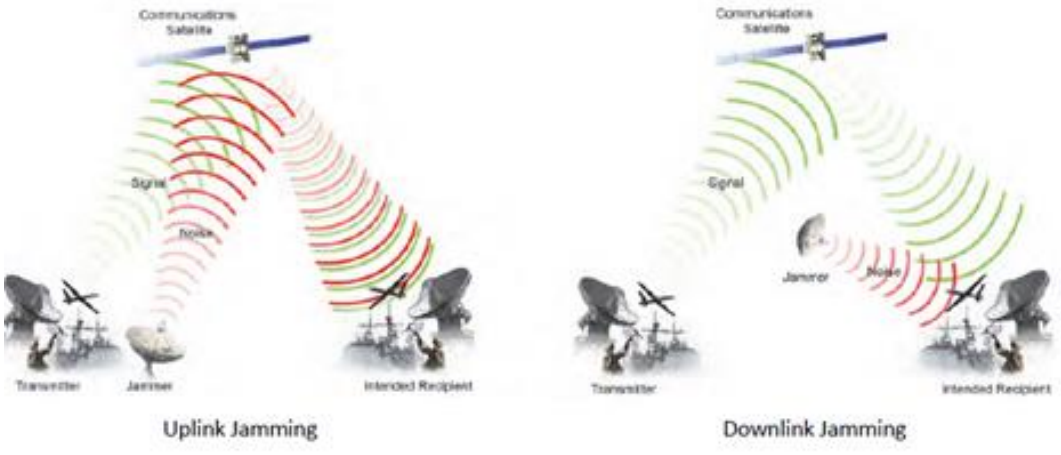
Además, dependiendo de la naturaleza de la señal de interferencia, podría haber consecuencias colaterales involuntarias si otras señales transmitidas por el mismo satélite también se ven afectadas. Por ejemplo, si un presentador de un canal de televisión asiático está sujeto a un ataque de interferencia orbital, los posibles televidentes en América del Norte tampoco pueden recibir las señales de transmisión.

Imagen 3.3. Interferencia orbital.



Tomada de Infosec Institute, *Hacking Satellites … Look Up to the Sky,* [en línea]. Dirección URL: http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref.

Imagen 3.4. Interferencia satelital.



Tomada de Infosec Institute, *Hacking Satellites … Look Up to the Sky,* [en línea]. Dirección URL: http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref.

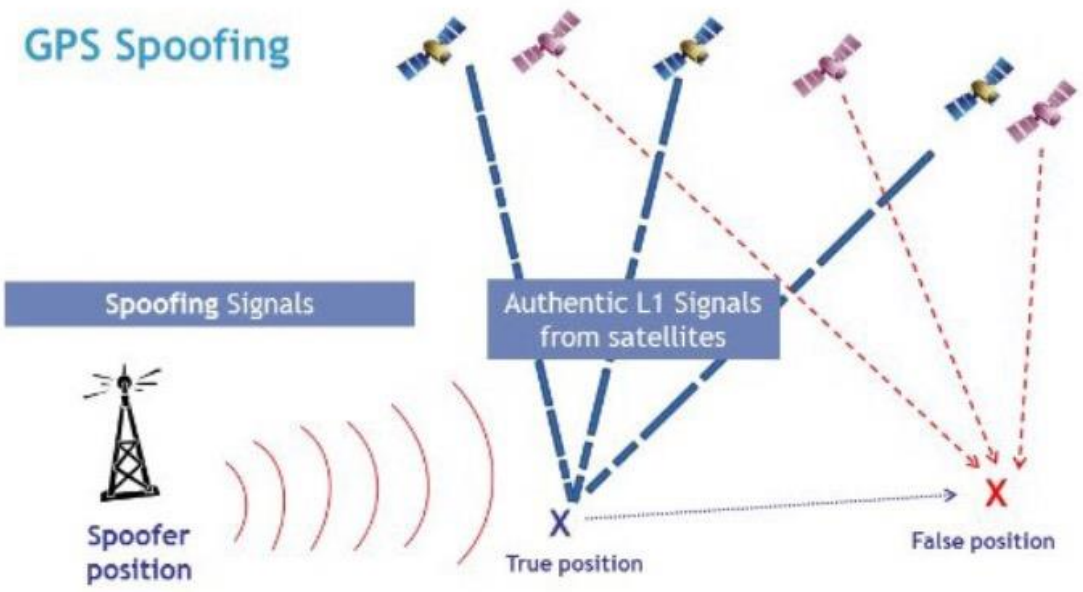
➔ Spoofing.

Este tipo de ataque manipula la información que se intercambia en las comunicaciones y por lo tanto, reduce su integridad. La suplantación va más allá de la interferencia para distorsionar o reemplazar la señal deseada con una señal falsa. Para que el ataque sea exitoso el receptor debe seguir funcionando correctamente y las señales de *spoofing* deben atascar la señal deseada y ser indistinguibles de ella, conteniendo información falsa pero aparentemente verdadera.

Al igual que con la interferencia, la suplantación se puede aplicar tanto en el receptor como en el transmisor (satélite). En una demostración en el año 2013 el Dr. Todd Humphreys, al frente de un equipo de científicos de la Universidad de Texas, utilizó un dispositivo construido en laboratorio para emitir señales de GPS falsificadas que eran ligeramente más fuertes que las reales. Bajo condiciones controladas tomó el control del sistema de navegación de un yate de lujo, reiniciando el sistema de navegación por satélite del barco de una manera que no era visible para el capitán.

El sistema de navegación del yate se fijó en la señal falsa y el capitán sin darse cuenta de que la señal del GPS era incorrecta, ajustó el rumbo de modo que la verdadera huella del barco fuera inexacta unos pocos grados. Las implicaciones de esta forma de ataque sobre un transportador de carga muy grande y cargado que maniobra en aguas confinadas, son muy claras.

Imagen 3.5. GPS Spoofing.



Tomada de Política y otras cosas, *¿Cómo se engaña a un GPS?,* [en línea]. Dirección URL: https://mrjaen.com/2017/05/21/como-se-engana-a-un-gps/.

➔ Secuestro de satélites para destruirlos o desactivarlos.

Los desafíos técnicos asociados con los ataques cibernéticos que apuntan a tomar el control físico de los satélites pueden resultar muy atractivos para los atacantes, que probablemente se centrarán en los sistemas de control industrial (ICS, por sus siglas en inglés) y específicamente en los sistemas de control y adquisición de datos (SCADA, por sus siglas en inglés). Hay tres componentes de sistemas SCADA: computadoras que controlan y monitorean las operaciones de la planta, y envían señales que controlan físicamente el sistema; dispositivos de campo tales como controladores lógicos programables que controlan los sensores, motores y otros componentes físicos; y computadoras de interfaz hombre-máquina (HMI, por sus siglas en inglés), que muestran datos sobre las operaciones.

La mayoría de los satélites lanzados en los últimos años se basan en computadoras que están instaladas en el satélite y que requieren actualizaciones regulares a través del acceso remoto. Además, al igual que con todos los dispositivos electrónicos una "puerta trasera" podría estar presente en uno de los muchos miles de componentes en un solo satélite, lo que permite el acceso oculto de los piratas informáticos.

Es posible que un ataque sofisticado pueda maniobrar un satélite para colisionar con otro satélite u objeto espacial. Los peligros de los ataques cibernéticos que apuntan a tomar el control físico de los satélites han recibido muy poca atención, a pesar de que tales ataques serían de gran importancia estratégica global. El principal foco de preocupación han sido las redes en lugar de los satélites. En consecuencia, los expertos y los responsables de la formulación de políticas no han entendido todas las implicaciones y el alcance de las posibles consecuencias de una toma de control por satélite.

➔ Ataques a la infraestructura terrestre.

Las vulnerabilidades de los satélites a ataques cibernéticos incluyen ataques dirigidos a estaciones terrestres. Un ataque podría llegar a través de una estación terrestre con la intención de hacer que un satélite maniobre, "decaiga" o baje su órbita para que vuelva a entrar en la atmósfera de la Tierra y se incendie. También, pueden existir ataques a la infraestructura terrestre como los centros de control de satélites, las redes y los centros de datos asociados causando impactos globales potenciales por ejemplo, alteraciones en los sistemas de predicción meteorológica.

➔ Espionaje “Escuchando a escondidas”[194].

A diferencia de la interferencia, “escuchar a escondidas” una transmisión permite a un atacante acceder a los datos transmitidos. A pesar de que casi todas las comunicaciones satelitales están encriptadas, es bastante fácil leer publicaciones en internet que describen cómo usar productos disponibles para interceptar transmisiones satelitales, ya sea información que transmitan medios, conversaciones vía satélite o el tráfico de datos en internet.

Uno de los casos más populares de espionaje satelital fue el protagonizado por piratas informáticos en Iraq y Afganistán para acceder a datos transmitidos por satélites gracias a la utilización del *software SkyGrabber*, producido por la firma rusa *Sky Software* y vendido por 26 dólares en internet. El caso alarmó al ejército ya que es normal esperar el más alto nivel de seguridad en equipos militares, incluida la encriptación de comunicaciones. La solución de la falla agregó costos al programa militar, pero la mayor amenaza fue la revelación de ubicaciones áreas militares y de los

[194] Infosec Institute, *Hacking Satellites … Look Up to the Sky,* [en línea]. Dirección URL: http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref. [Fecha de consulta: 15 de octubre de 2017].

patrones seguidos por aviones no tripulados utilizados para actividades de reconocimiento.

Todas estas formas de ataque a los satélites pueden ser llevadas a cabo por distintos actores desde Estados que se proponen crear ventajas militares en el espacio, o que buscan robar cantidades estratégicas de propiedad intelectual y que tienen suficiente poder de cómputo para descifrar códigos de cifrado; organizaciones criminales con recursos suficientes que buscan ganancias financieras; grupos terroristas que desean promover sus causas; hasta crackers individuales que simplemente quieren probar sus habilidades y/o cualquier combinación de las organizaciones e individuos anteriores.

Las vulnerabilidades cibernéticas en la infraestructura crítica espacial nacional e internacional podrían ser un conducto para ataques con consecuencias sumamente peligrosas. En caso de una escalada de una crisis internacional, las debilidades es cuestiones de ciberseguridad pueden explotarse como parte de las campañas diplomáticas, de inteligencia o militares.

Las tecnologías militares se basan en satélites y la infraestructura espacial para la navegación y la orientación, el mando y el control, la supervisión operativa y otras funciones por lo que los ataques cibernéticos en los satélites "socavarían la integridad de los sistemas de armas estratégicas, desestabilizarían las relaciones de disuasión y ofuscarían al autor del ataque"[195].

El hecho de que las tecnologías cibernéticas estén al alcance de la mayoría de los Estados y actores no estatales crea oportunidades hasta ahora inimaginables e incomparables para pequeños gobiernos o grupos terroristas para perpetrar ataques de alto impacto, y teniendo como consecuencia a su vez, que las capacidades en el campo de batalla no sean tan dispares.

Es por todo lo anterior que Estados Unidos en su *Política Espacial Nacional* establece como una de sus prioridades el "operar y mantener la constelación del Sistema de Posicionamiento Global para satisfacer las necesidades de seguridad civil y nacional"[196]. Debido a que las señales de GPS son la base de casi todas las tecnologías,

[195] David, Livingstone; Patricia, Lewis, *Op. Cit.*
[196] NASA, *National Space Policy of the United States of America, Op. Cit.*

los funcionarios del Departamento de Seguridad Nacional lo consideran como "un punto único de falla para la infraestructura crítica"[197].

El GPS como la constelación de satélites que es, está sujeto a los mismos tipos de ataques antes mencionados en este mismo subtítulo de la investigación no obstante, a continuación se mencionan los efectos específicos que producirían la interrupción de su funcionamiento[198]:

1. Interferencia o negación del servicio de GPS. La desactivación de la recepción GPS por interferencia es relativamente simple. Personas que buscan privacidad y hasta delincuentes en los Estados Unidos usan este tipo de interferencias para interrumpir la recepción del GPS en pequeñas áreas.
2. Desactivación de redes. Prácticamente todas las redes dependen de la señal de tiempo altamente precisa del Sistema de Posicionamiento Global. Cuando las señales GPS se interrumpen, los relojes que existen de reserva se utilizan para mantener la sincronización pero con el tiempo éstos se desvían y partes de las redes comienzan a fallar.
3. Datos e información erróneos y engañosos (*Spoofing*). Muchas aplicaciones informáticas necesitan la ubicación del GPS y la información del tiempo para funcionar correctamente. Cuando las señales GPS están atascadas, antes de que los receptores muestren fallos, a menudo aceptan la señal de interferencia como válida durante un período de tiempo y proporcionan a los usuarios información incorrecta.

Todas las técnicas mencionadas se pueden llevar a un nivel más alto de sofisticación pero se requiere *hardware* costoso. La contramedida más eficiente contra estos ataques es la adopción de encriptación de señal, donde el receptor y el transmisor utilizan procesos de autenticación mutua para evitar interferencias de fuentes externas. Desafortunadamente, aunque esta técnica es compatible con cualquier GPS, el requerimiento de sistemas más potentes y a su vez más costosos hace que el cifrado se limite al sector militar.

[197] Resilient Navigation and Timing Foundation, *Cybersecurity,* [en línea]. Dirección URL: https://rntfnd.org/cybersecurity/. [Fecha de consulta: 1° de octubre de 2017].
[198] *Ídem.*

Al igual que lo sucedido en otros entornos[199], la falta de hechos documentados, poco conocidos o reportados en el dominio cibernético espacial, conduce a una falsa sensación de seguridad aparentando que no sucede nada o que la probabilidad de que algo ocurra es poca. No obstante, los hechos que se describen a continuación demuestran lo contrario.

En 1999 el periódico *The Telegraph* publicó la historia sobre un grupo de piratas informáticos sospechosos de tomar el control de un satélite de comunicaciones militares británico usando una computadora doméstica, lo que ocasionó que se activara una alerta de seguridad. Sin embargo el hecho nunca fue confirmado y la historia se puso en duda.

La Guerra del Golfo de 1991, oficialmente denominada *Operación Tormenta del Desierto*, fue el primer conflicto en la historia en hacer uso del apoyo de los sistemas espaciales. En particular, los satélites meteorológicos, los satélites de imágenes multiespectrales, los satélites del Sistema de Posicionamiento Global, los satélites de alerta temprana y los satélites de comunicaciones. Durante los 12 años transcurridos entre la *Operación Tormenta del Desierto* y el comienzo de la *Operación Libertad Iraquí* (OIF, por sus siglas en inglés) en 2003, el apoyo que los sistemas basados en el espacio proporcionaron a las fuerzas militares de Estados Unidos se volvió cada vez más integral para las operaciones.

En consecuencia muchos analistas llegaron a considerar la *Operación Libertad Iraquí* como "la primera guerra espacial real", puesto que se hacía cada vez más difícil imaginar la realización de operaciones de combate sin activos espaciales[200]. En dicha operación, Iraq adquirió equipos de interferencia de GPS supuestamente de la compañía rusa *Aviaconversiya Ltd*, el ejército estadounidense descubrió los equipos y confirmó haber destruido seis *jammers* de GPS, sin embargo el director de la empresa rusa negó haber vendido los equipos a Iraq.

Por su parte, el entonces presidente Bush le expresó su preocupación a Vladimir Putin sobre la venta a Iraq de equipamiento militar sensible además de enseñarles a los iraquíes cómo usar *hardware* prohibido como gafas de visión nocturna, interceptores

[199] Como lo sucedido con el virus *Stuxnet* en el año 2010, siendo la primera vez que un ataque cibernético logró cruzar la frontera del software y dañar la infraestructura del "mundo real". Antes de este hecho, no se tenían contempladas y valoradas las consecuencias de un ataque de este tipo.

[200] Rick, W. Sturdevant; Haithe, Anderson, *Space Effects in Operation Iraqi Freedom,* [en línea]. Dirección URL: http://www.spacebusiness.com/sample2.pdf. [Fecha de consulta: 18 de octubre de 2017].

GPS y misiles guiados. Putin, ante esto, negó que Rusia hubiera vendido algún equipo a Iraq e insinuó que Ucrania podría haber vendido equipo que primero le compró a Rusia para posteriormente proporcionarlo a Iraq.

Los tipos de bombas cuyos cursos pueden ser alterados por estos *jammers* se denominan *J-Dams* guiadas por GPS del ejército estadounidense. Se estima que el 80%[201] de las armas estadounidenses que se usarían en una guerra con Iraq serían dirigidas a través de satélites, motivo por el cual la Fuerza Aérea probó dispositivos de interferencia similares para ver si los utilizados por Iraq realmente podían funcionar contra las armas estadounidenses.

Las consecuencias de un caso como el de Estados Unidos *vs* Iraq no sólo radican en la disminución de las capacidades de ataque o en la demostración de las capacidades de defensa que respectivamente se puedan tener, sino que si las armas inteligentes utilizadas se desvían de sus objetivos designados pueden llegar a alcanzar sitios no militares y causar víctimas civiles, agravando la situación del enfrentamiento y menoscabando a su vez la seguridad nacional de las partes desde diversas aristas.

En 2007 se presentó otro caso en el que los rebeldes tamiles que luchaban por la independencia en Sri Lanka, interfirieron los servicios de un satélite estadounidense para enviar emisiones de radio y televisión a otros países. El satélite interferido pertenecía a *Intelstat*, una compañía estadounidense. Funcionarios de *Intelstat* se reunieron con expertos técnicos y el embajador de Sri Lanka en Estados Unidos para discutir medidas que la compañía tomaría para evitar el uso no autorizado del satélite; mientras que los rebeldes sostuvieron que no habían accedido al satélite ilegalmente.

En enero de ese mismo año el periódico *New York Times* publicó esta historia:

> China realizó con éxito su primera prueba de un arma antisatélite la semana pasada, señalando su determinación de desempeñar un papel importante en las actividades espaciales militares y llevando expresiones de preocupación desde Washington y otras capitales, dijo el gobierno de Bush ayer. [...] Expertos en control de armas llamaron a la prueba, en la que el arma destruyó un viejo satélite meteorológico chino, un desarrollo preocupante que podría presagiar una carrera armamentista antisatélite.

[201] Fox News, *Military Wipes Out Iraqi GPS Jammers,* [en línea]. Dirección URL: http://www.foxnews.com/story/2003/03/25/military-wipes-out-iraqi-gps-jammers.html. [Fecha de consulta: 18 de octubre de 2017].

Jianhua Li, un portavoz de la Embajada de China en Washington, dijo que había escuchado sobre la historia antisatélite, pero que no tenía ninguna declaración o información. En un momento en que China está modernizando sus armas nucleares, ampliando el alcance de su armada y enviando astronautas a la órbita por primera vez, la prueba parece marcar una nueva esfera de competencia técnica y militar. Los funcionarios estadounidenses se quejaron ayer de que China no había hecho anuncios públicos o privados sobre su prueba, a pesar de las reiteradas solicitudes de los funcionarios estadounidenses para una mayor apertura sobre sus acciones.

[...] Los satélites presumiblemente al alcance del misil chino incluyen la mayoría de los satélites de imágenes utilizados para el reconocimiento militar básico, que son esencialmente los ojos de la comunidad de inteligencia estadounidense para los movimientos militares, posibles ensayos nucleares e incluso satélites comerciales.

A fines de agosto, el presidente Bush autorizó una nueva política espacial nacional que ignoró los llamados a una prohibición global de tales pruebas. La política decía que Estados Unidos "preservaría sus derechos, capacidades y libertad de acción en el espacio" y "disuadiría o impediría a otros de obstaculizar esos derechos o desarrollar capacidades destinadas a hacerlo". Declaró que Estados Unidos "prohibiría, si es necesario, a los adversarios el uso de capacidades espaciales hostiles a los intereses nacionales de los Estados Unidos".

"Durante varios años, los rusos y los chinos han estado tratando de impulsar un tratado para prohibir las armas espaciales. El concepto de exhibir una capacidad de poder duro para llevar a alguien a la mesa de negociaciones es una técnica clásica de Guerra Fría" dijo Theresa Hitchens, directora del Centro de Información de Defensa, un grupo privado en Washington que rastrea los programas militares.

Gary Samore, director de estudios en el Consejo de Relaciones Exteriores, dijo en una entrevista: "Creo que tiene mucho sentido para los chinos hacer esto tanto para disuadir como para cubrir sus apuestas. Ejerce presión sobre EE.UU. para que negocien acuerdos que prohíban armar el espacio".

Hitchens y otros críticos han acusado a la administración de realizar investigaciones secretas sobre armas antisatélite avanzadas que usan láser, que se consideran una forma mucho más rápida y poderosa de destruir satélites que las armas de hace dos décadas.

Michael Krepon, cofundador del Centro Henry L. Stimson, un grupo que estudia la seguridad nacional, agregó que la administración estadounidense había argumentado

> durante mucho tiempo que el mundo no necesitaba ningún tratado de armas espaciales porque no existían tales armas y porque las últimas pruebas fueron hace dos décadas. "Parece", dijo, "ese argumento ya no es operativo"[202].

Esta noticia implicó el ataque directo a un satélite chino por medio de un misil del mismo país, un tema que aunque no es abordado de manera directa en esta investigación, no se le resta importancia ya que da a notar la evolución que ha tenido este tipo de amenaza pues hoy en día atacar un satélite no requiere capacidad espacial de Estado. Debido a las herramientas utilizadas y el ahorro de costes al adquirir las mismas, la violación a la ciberseguridad espacial se ha convertido en un tema donde operan gran variedad de actores.

Por otro lado, en 2011 el gobierno de Estados Unidos registró que al menos dos de sus satélites de vigilancia del medio ambiente habían sufrido interferencias cuatro o más veces en 2007 y 2008. Un satélite *Landsat-7* de observación de la Tierra construido por la NASA experimentó 12 o más minutos de interferencia en octubre de 2007 y julio de 2008. Un satélite *Terra AM-1* de observación de la Tierra también administrado por la NASA sufrió una interferencia similar durante dos minutos en un solo día en junio de 2008, y por lo menos nueve minutos en un día en octubre de 2008[203].

En 2013, los sistemas de alerta de emergencia de las estaciones de televisión en Montana y Michigan fueron pirateados y los atacantes transmitieron un informe de una invasión zombi. No se sabe si las transmisiones ilegales fueron posibles debido a un ataque contra satélites o contra conexiones a internet, no obstante, la falta de detalles proporcionados en los informes llevó a muchos expertos en seguridad a creer que la primera hipótesis era la más probable.

Para concluir con los casos de ciberataques o ataques a satélites por distintos medios, la Administración Nacional Oceanográfica y Atmosférica de Estados Unidos informó en el año 2014 que su Sistema de Información de Datos Satelitales fue desconectado en septiembre después de un grave incidente cibernético que provocó la denegación de grandes volúmenes de datos a las agencias de pronóstico del tiempo en

[202] New York Times, *Flexing Muscle, China Destroys Satellite in Test*, [en línea], 19 de Enero de 2007. Traducción propia. Dirección URL: http://www.nytimes.com/2007/01/19/world/asia/19china.html?ex=1326862800&en=74a017e997a72c53&ei=5088&partner=rssnyt&emc=rss. [Fecha de consulta: 10 de octubre de 2017].

[203] David, Livingstone; Patricia, Lewis, *Op. Cit.*

todo el mundo durante 48 horas[204]. Con esta serie de casos se demuestra que el uso generalizado y creciente del GPS, junto con el aumento de actores que poseen tecnologías que pueden interrumpir sus servicios ahora y en el futuro, representan una amenaza a largo plazo que no se puede ignorar.

En el año 2012 el Departamento de Seguridad Nacional de Estados Unidos desclasificó un documento llamado *Estimación Nacional de Riesgos: Riesgos para la Infraestructura Crítica de los Estados Unidos por las interrupciones del Sistema de Posicionamiento Global,* documento que señala los riesgos y predice el impacto de las amenazas en los principales sectores de aplicaciones de GPS: telecomunicaciones, servicios de emergencia, energía y transporte.

El mismo reporte reconoce que los sectores de infraestructura críticos de Estados Unidos están cada vez más en riesgo debido a una dependencia creciente del Sistema de Posicionamiento Global, considerando que en el corto plazo (en ese entonces) el riesgo de un ataque al mismo es "manejable para la nación". Sin embargo, el documento hace hincapié en que si no se aborda, esta amenaza representa un riesgo creciente para la seguridad nacional y económica del país a largo plazo.

Los sectores de infraestructura crítica de los Estados Unidos actualmente dependen del GPS para aspectos de sus operaciones centrales. A medida que el Sistema de Posicionamiento Global se integra cada vez más en las operaciones de los sectores, se ha convertido en una herramienta invisible, por lo tanto es probable que la dependencia del mismo se subestime significativamente.

Tampoco hay que dejar de lado que existe una gran interdependencia entre los sectores de infraestructura críticos, por lo que una interrupción del GPS que afecte directamente a un sector puede generar efectos de cascada y expansión a otros sectores que dependen del sector afectado en un principio, lo que ocasiona daños colaterales. El informe considera las interrupciones a los servicios civiles de GPS en los Estados Unidos, los riesgos que las mismas representan para las misiones cumplidas por los sectores de infraestructura críticos y el consiguiente impacto nacional.

Empero, la *Estimación Nacional de Riesgos: Riesgos para la Infraestructura Crítica de los Estados Unidos por las interrupciones del Sistema de Posicionamiento*

[204] *Ídem.*

Global no aborda las amenazas disruptivas desde fuera de los Estados Unidos, pero reconoce su importancia y evalúa la proliferación interna de equipos fabricados fuera de sus fronteras. Además, reconoce que "las implicaciones de una interrupción del GPS doméstico podrían tener un alcance global dado la naturaleza cada vez más globalizada de algunos sectores de infraestructura críticos"[205].

El informe más reciente que se tiene sobre las vulnerabilidades del GPS fue publicado en el año 2016 por el Centro Nacional de Sistemas de Transporte John A. Volpe, y lleva por nombre *Dependencias del GPS en el Sector Transporte: Un inventario de las dependencias del Sistema de Posicionamiento Global en el Sector del Transporte, las Mejores Prácticas para Mejorar la Robustez de los Dispositivos GPS y Posibles Soluciones Alternativas para el Posicionamiento, la Navegación y el Tiempo* y como el título lo dice, se encuentra enfocado en cada uno de los diferentes medios de sector de transporte: aviación, transporte terrestre, marítimo y gasoductos.

En realidad este informe no varía mucho del que se publicó en el año 2001 pues sus contenidos son muy parecidos e incluso algunos subtítulos se mantuvieron intactos, lo que demuestra que los tipos de amenazas a la interrupción de los servicios del Sistema de Posicionamiento Global en cuanto al sector de transportes no han variado en lo esencial. La siguiente tabla, muestra una clasificación de los tipos de interrupciones al GPS.

[205] Department of Homeland Security, *National Risks Estimate: Risks to US critical infrastructure from global positioning system disruptions,* [en línea], p.59. Dirección URL: https://rntfnd.org/wp-content/uploads/DHS-National-Risk-Estimate-GPS-Disruptions.pdf. [Fecha de consulta: 20 de octubre de 2017].

Tabla 3.1. Tipos de interrupciones al GPS.

Tipos	Ejemplo
Involuntario vs Intencional	¿La interrupción es causada por un pedazo de basura espacial que deshabilita un satélite GPS o se debe a un acto intencional de un empleado descontento o un terrorista?
Predecible vs Impredecible	¿La interrupción se debe a un aumento anticipado en la actividad de la llamarada solar o a la activación repentina de un dispositivo de interferencia?
Ambiental vs Hecho por el hombre	¿La interrupción se debe a una mayor actividad del clima solar o a un transmisor de radio configurado incorrectamente que opera en una banda de frecuencia adyacente?
Habitual vs Sofisticado	¿La interrupción es causada por un interferente de GPS de 50 dólares que se compra en línea, o por un hacker que manipula con precisión una señal de GPS para engañar a los envíos o al tráfico de las autopistas?
Local vs Generalizado	¿La interrupción es un ataque de suplantación selectiva contra una sola terminal de carga o cubre un área geográfica grande (por ejemplo, debido a un fenómeno meteorológico solar significativo)?

Obtenida de Volpe Center, *GPS Dependencies in the Transportation Sector: An Inventory of Global Positioning System Dependencies in the Transportation Sector, Best Practices for Improved Robustness of GPS Devices, and Potential Alternative Solutions for Positioning, Navigation, and Timing,* [en línea], August 2016, p.6. Dirección URL: https://ntl.bts.gov/lib/60000/60400/60433/DOT_VNTSC_NOAA_16_01.pdf. Traducción propia.

Hoy en día el Sistema de Posicionamiento Global es la columna vertebral de la infraestructura crítica terrestre. Los satélites son controlados por computadoras en

centros de datos como cualquier otra aplicación informática, por lo tanto, son vulnerables y están sujetos a los ataques cibernéticos más comunes así como a ataques más específicos del sector. En abril de 2017, Jeanette Hanna-Ruiz la jefa de información y seguridad de la NASA afirmó en una entrevista que era cuestión de tiempo antes de que alguien *hackeara* algo en el espacio, “somos un objetivo muy atractivo" declaró.

"Tenemos mucha gente que se enfoca en llevar satélites u otros activos al espacio y puede que no estén necesariamente pensando en la seguridad. La verdad es que no sé si quiero que piensen en seguridad. Quiero que estén entusiasmados y apasionados por ir al espacio" dijo Hanna-Ruiz[206]. En la misma entrevista manifestó que construir cohetes, satélites y otros instrumentos seguros antes de su lanzamiento era la clave para la resiliencia ante ataques cibernéticos por lo que los equipos de ciberseguridad intervienen para buscar vulnerabilidades en la codificación, el *firmware* y otras áreas.

Es por todo lo anterior que Estados Unidos se ve en la necesidad de desarrollar estrategias de mitigación y resiliencia para enfrentar las vulnerabilidades del Sistema de Posicionamiento Global ante ataques cibernéticos para a su vez, asegurar su capacidad basada en el espacio y proteger su seguridad nacional.

3.3. Situación actual y futura del Sistema de Posicionamiento Global.

El *Informe de la Comisión para Evaluar la Gestión y Organización de la Seguridad Nacional del Espacio de Estados Unidos* y la *Evaluación de Vulnerabilidad de la Infraestructura de Transporte basándose en el Sistema de Posicionamiento Global* fueron dos documentos que marcaron un hito en la evolución del GPS al ser los primeros en confirmar y declarar acerca de las vulnerabilidades que éste presentaba.

El gobierno de Estados Unidos comenzó a trabajar para mejorar el servicio proporcionado por el Sistema de Posicionamiento Global y el primer paso considerado como parte de su modernización tuvo lugar en mayo de 2000, cuando el presidente Bill Clinton ordenó al Departamento de Defensa que desactivara la función de Disponibilidad Selectiva del GPS implementada a nivel mundial, de esta manera se multiplicó la precisión del GPS civil por diez.

[206] Bloomberg Politics, *Outer-Space Hacking a Top Concern for NASA’s Cybersecurity Chief,* [en línea], abril de 2017. Traducción propia. Dirección URL: https://www.bloomberg.com/news/articles/2017-04-12/outer-space-hacking-a-top-concern-for-nasa-s-cybersecurity-chief. [Fecha de consulta: 23 de octubre de 2017].

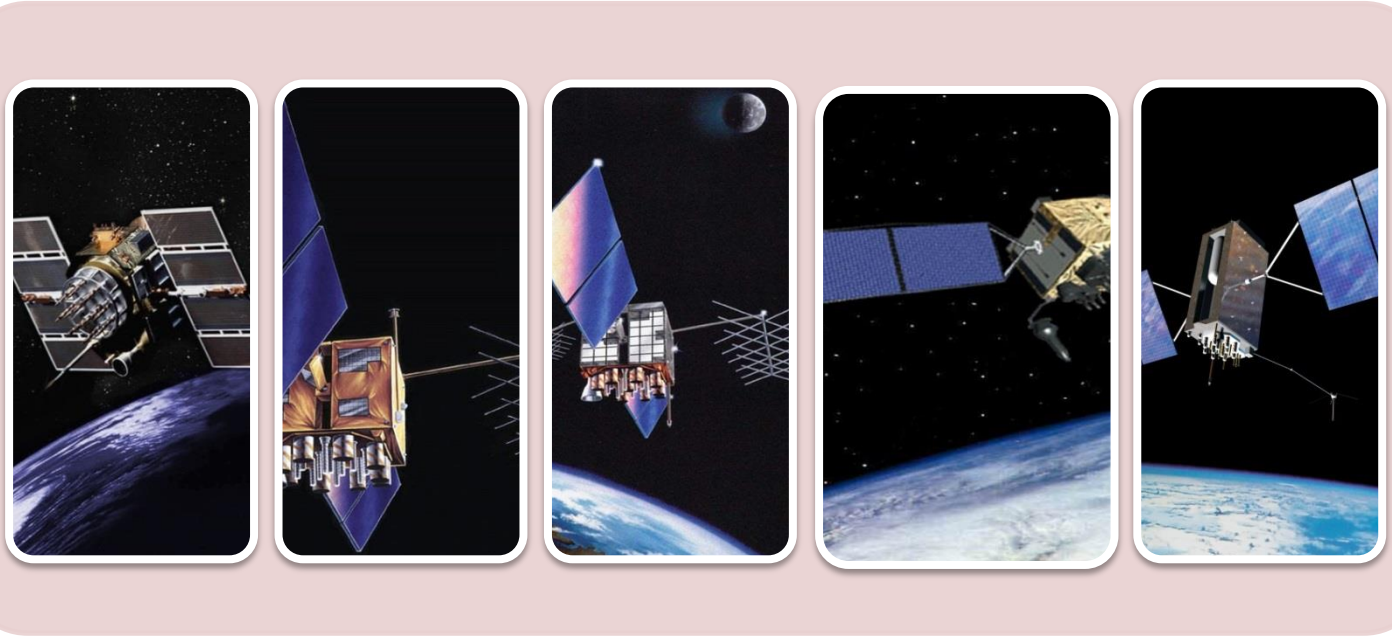
La modernización del Sistema de Posicionamiento Global implica el reemplazo completo de los satélites y sistemas terrestres GPS heredados por otros más nuevos y más capaces, este proceso requiere recursos del Departamento de Defensa y del Departamento de Transporte. En 1989, el contrato fue otorgado a *Lockheed Martin* para el desarrollo y la producción de 21 vehículos espaciales clasificados como *GPS IIR*. En agosto de 2000, la Fuerza Aérea de los Estados Unidos otorgó a la misma empresa un contrato para modernizar ocho satélites *GPS IIR* existentes y fue el 17 de agosto de 2009 que se lanzó el último satélite *GPS IIR-M* (modernizado) desde la Estación de la Fuerza Aérea de Cabo Cañaveral, Florida.

Una vez que se realizó esta modernización se reafirmó la continuidad del proceso a través de la *Política Espacial Nacional* de Estados Unidos en la que uno de los objetivos es "mantener su liderazgo en el servicio, suministro y uso de los Sistemas Mundiales de Navegación por Satélite para lo cual es indispensable invertir en capacidades nacionales y apoyar actividades internacionales para detectar, mitigar y aumentar la resiliencia a la interferencia perjudicial al GPS, e identificar e implementar, según sea necesario y apropiado, sistemas o enfoques redundantes y de respaldo para infraestructura crítica, recursos clave y funciones esenciales"[207].

El desarrollar, adquirir y operar sistemas espaciales y el mejorar la capacidad de detectar, advertir, caracterizar y atribuir rápidamente las perturbaciones naturales y provocadas por el hombre a los mismos, es de vital interés para la seguridad nacional de Estados Unidos. En el siguiente esquema se muestran los diferentes tipos de satélites que han conformado y forman hoy en día al Sistema de Posicionamiento Global así como sus respectivas características.

[207] NASA, *National Space Policy of the United States of America, Op. Cit.*

Esquema 3.2. Características de las generaciones actuales y futuras de satélites GPS.



Bloque IIA	Bloque IIR	Bloque IIR-M	Bloque IIF	GPS III
0 operacionales	12 operacionales	7 operacionales	12 operacionales	En producción
Código de Adquisición Coarse (C/A) en la frecuencia L1 para usuarios civiles.	C/A código en L1.	Todas las señales heredadas.	Todas las señales del bloque IIR-M.	Todas las señales del bloque IIF.
Señal P (Y) militar cifrada precisa en frecuencias L1 y L2 para usuarios militares.	Código P (Y) militar cifrado en L1 y L2.	Segunda señal civil en L2 (L2C).	3ª señal civil en frecuencia L5 (L5).	4ª señal civil en L1 (L1C).
Vida útil de diseño de 7.5 años.	Monitoreo del reloj a bordo.	Nuevas señales de código M militares para mejorar la resistencia a la interferencia.	Relojes atómicos avanzados.	Fiabilidad, precisión e integridad mejoradas de la señal.
Lanzado en 1990-1997.	Vida útil de diseño de 7.5 años.	Niveles de potencia flexibles para señales militares.	Mejora en la precisión, potencia de la señal y calidad.	Sin disponibilidad selectiva.
Último desmantelado en 2016.	Lanzado en 1997-2004.	Vida útil de diseño de 7.5 años.	Vida útil de diseño de 12 años.	Satélites 11+: reflectores láser; búsqueda y rescate de carga útil.
		Lanzado en 2005-2009.	Lanzado en 2010-2016.	Vida útil de diseño de 15 años.
				Primer lanzamiento no antes de 2018.

Obtenido de GPS, *Space Segment*, [en línea]. Dirección URL: https://www.gps.gov/systems/gps/space/#generations.

Traducción propia.

En mayo de 2008, se otorgó el primer contrato a la empresa *Lockheed Martin* para el desarrollo de satélites *GPS III* mismos que como se observa en la tabla se encuentran en producción y su lanzamiento está programado para el año 2018. Los vehículos espaciales *GPS III* presentarán nuevas capacidades para satisfacer las mayores demandas de usuarios militares y civiles. Brinda la capacidad completa para usar *M-Code*, una señal GPS militar modernizada, y amplía la cooperación internacional al permitir que la señal *L1C* sea compatible con el sistema europeo Galileo.

Los satélites *GPS III* también son necesarios para completar el despliegue de las capacidades de señales *L2C* y *L5* que comenzaron con los satélites modernizados *GPS IIR-M* y *GPS IIF*, cuentan con una mejora en su capacidad anti-interferencia, mejora la precisión, transmitirán múltiples señales civiles y militares y además tendrán un aumento de la potencia de cobertura de tierra sin disminuir la potencia de otras señales militares.

Otro de los enfoques principales del programa de modernización del GPS es la adición de nuevas señales de navegación a la constelación de satélites. La señal civil heredada es decir, la primera señal civil disponible es llamada *L1 C/A* o *C/A en L1* y se pretende que siga transmitiendo para un total de cuatro señales de GPS civiles. Las nuevas señales civiles se están introduciendo progresivamente a medida que la Fuerza Aérea lanza nuevos satélites GPS para reemplazar a los más antiguos. La mayoría de las nuevas señales serán de uso limitado hasta que se transmitan mediante 18 a 24 satélites.

La segunda señal civil (*L2C*) fue diseñada específicamente para satisfacer las necesidades comerciales. Su nombre se refiere a la frecuencia de radio utilizada por la señal (*1227 MHz* o *L2*) y al hecho de que es para uso civil. También hay dos señales militares en la frecuencia *L2*. Cuando se combina con *L1 C/A* en un receptor de doble frecuencia, *L2C* permite la corrección ionosférica, una técnica que aumenta la precisión y permite que los civiles con receptores GPS de doble frecuencia disfruten de la misma precisión que los militares.

Para usuarios profesionales con operaciones existentes de doble frecuencia, *L2C* permite una adquisición de señal más rápida, una confiabilidad mejorada y un mayor rango de operación. *L2C* transmite a una potencia efectiva más alta que la señal *L1 C/A* heredada, por lo que es más fácil de recibir debajo de los árboles e incluso en interiores.

El primer satélite GPS con *L2C* se lanzó en 2005 y todos los satélites GPS enviados desde entonces incluyen un transmisor con este tipo de señal.

L5 es la tercera señal de GPS civil, diseñada para cumplir con los requisitos del sector transporte, su nombre se refiere a la designación de los Estados Unidos para la frecuencia de radio utilizada por la señal (1176 MHz). *L5* se transmite en una banda de radio reservada exclusivamente para servicios de seguridad aérea y tiene una mayor potencia por lo que disponer de esa señal aumenta las posibilidades de las aproximaciones por instrumentos en todo el mundo, disminuyendo a su vez los errores que ocurren en las señales debido a perturbaciones en la ionosfera y proporcionando mayor precisión con poca o ninguna inversión en infraestructura de tierra.

Además de mejorar la seguridad, el uso de *L5* aumentará la capacidad y la eficiencia del combustible dentro del espacio aéreo, los ferrocarriles, las vías navegables y las autopistas de Estados Unidos. Más allá del transporte, *L5* en combinación con *L1 C/A* y *L2C* brindará a los usuarios de todo el mundo la señal de GPS civil más avanzada. En 2009, la Fuerza Aérea transmitió con éxito una señal experimental *L5* en el satélite *GPS IIR-20 (M)*. El primer satélite *GPS IIF* con un transmisor L5 completo se lanzó en mayo de 2010 y cuatro años más tarde la Fuerza Aérea comenzó a transmitir mensajes de navegación civil en la señal *L5*, sin embargo, ésta sigue siendo preoperativa.

La cuarta señal civil es llamada *L1C* y está diseñada para permitir la interoperabilidad entre el GPS y los Sistemas Internacionales de Navegación por Satélite. Su nombre se refiere a la frecuencia de radio utilizada por la señal (1575 MHz o *L1*). Hay dos señales militares en *L1*, así como la señal *C/A* heredada, su diseño mejorará la recepción de GPS móvil en ciudades y otros entornos.

L1C presenta un esquema de modulación de operador que permite la cooperación internacional al tiempo que protege los intereses de seguridad nacional de Estados Unidos. El gobierno estadounidense en cooperación con Europa desarrollaron originalmente *L1C* como una señal civil común para GPS y Galileo no obstante, el sistema satelital *Quasi-Zenith* de Japón y el sistema BeiDou de China también están adoptando señales similares a *L1C*. Estados Unidos planea lanzar su primera señal *L1C* con los satélites *GPS III*, misma que se transmitirá a la misma frecuencia que la señal *L1 C/A* original, que se conservará para compatibilidad con versiones anteriores.

Todo el proceso de modernización hasta ahora descrito forma parte de los segmentos espacial y civil, sin embargo hay que recordar que el Sistema de Posicionamiento Global está compuesto por tres segmentos, por lo que la modernización de alguno trae consigo la modernización de los dos restantes. El segmento de control también ha sufrido constantes cambios, el primero de ellos fue la llamada *Iniciativa de mejora de la precisión heredada* que amplió el número de estaciones de monitoreo de seis a 16 y finalizó en 2008.

Este aumento de estaciones de monitoreo triplicó la cantidad de datos recopilados en las órbitas de los satélites GPS permitiendo una mejora del 10% al 15%[208] en la precisión de la información transmitida desde la constelación GPS. El esfuerzo de *L-AII* como también es conocida dicha iniciativa agregó 10 estaciones de monitoreo de GPS operacionales que pertenecen y son operadas por la Agencia Nacional de Inteligencia Geoespacial (NGA, por sus siglas en inglés).

En 2007 la Fuerza Aérea desplegó las Operaciones de lanzamiento/órbita temprana, resolución de anomalías y eliminación para gestionar satélites GPS no operativos (Bloque IIA/IIR/IIR-M, IIF). Esta operación incluyó satélites recién lanzados en proceso de pago, satélites fuera de servicio para la resolución de anomalías, satélites residuales almacenados en órbita y satélites que requieren eliminación por encontrarse en el final de su vida útil. El sistema LADO (por sus siglas en inglés) cumple con funciones como es rastreo, control y la planificación y ejecución de movimientos de satélites.

El sistema LADO es parte del segmento de control operacional del GPS, pero está separado del *Plan de Evolución de la Arquitectura* (AEP, por sus siglas en inglés) que controla la constelación de satélites GPS operacional. Este Plan fue implementado en 2007, es comandado por la Fuerza Aérea estadounidense y permite administrar todos los satélites GPS actuales.

Bajo este plan la Fuerza Aérea reemplazó su estación maestra original de control de GPS con una totalmente nueva basada en tecnologías que permitieron mejorar la flexibilidad y capacidad de respuesta de las operaciones y las estaciones de monitoreo GPS y antenas de tierra. Además, el *Plan de Evolución de la Arquitectura* presentó una

[208] GPS, *Legacy Accuracy Improvement Initiative (L -AII),* [en línea]. Dirección URL: https://www.gps.gov/systems/gps/control/L-AII/. [Fecha de consulta: 25 de octubre de 2017].

estación de control maestro alternativa que sirve como una copia de seguridad totalmente operativa para la estación de control principal.

En 2014, el AEP se actualizó para admitir capacidades modernizadas de navegación civil permitiendo que los satélites GPS de los bloques IIR-M y IIF transmitan mensajes de navegación preoperativos en las señales *L2C* y *L5*. En 2016, las líneas de base de *hardware* y *software* del Plan se actualizaron con seguridad cibernética mejorada y compatibilidad mejorada, para respaldar las operaciones en el año 2020. En 2020 el *Plan de Evolución de la Arquitectura* se actualizará para proporcionar capacidades básicas de la señal de GPS militar modernizada, conocida como *M-Code*, a la comunidad militar de usuarios de GPS en virtud del programa *M-Code Early Use* (MCEU, por sus siglas en inglés) que se explicará más adelante.

El Sistema de Control Operacional de Próxima Generación (OCX), desarrollado por el gobierno estadounidense en conjunto con la empresa *Raytheon*[209]*,* es la versión futura del segmento de control GPS. OCX controlará todos los satélites GPS modernizados y heredados, administrará todas las señales de navegación civil y militar, y proporcionará seguridad cibernética mejorada y resistencia para la próxima generación de operaciones de GPS. Este sistema estará conformado por una estación de control principal y una estación de control maestro alternativa, estaciones de monitoreo, antenas de tierra, un simulador de sistema GPS y un entrenador espacial estandarizado[210]. El desarrollo de OCX sigue un enfoque incremental:

El Bloque 0 es el Sistema de Lanzamiento y Control (LCS) destinado a controlar las operaciones de Lanzamiento y Órbita Temprana (LEO) y el pago en órbita de todos los satélites *GPS III*. OCX Block 0 es un subconjunto de OCX Block 1 que proporciona el *hardware*, el *software* y la base de ciberseguridad para el Bloque 1. El 2 de noviembre de 2017 el Centro de Sistemas Espaciales y de Misiles[211] anunció que la Fuerza Aérea de

[209] Raytheon es una empresa estadounidense líder de tecnología e innovación especializada en los mercados de defensa, gobierno civil, comunicaciones e inteligencia y seguridad cibernética en todo el mundo. Durante la Segunda Guerra Mundial suministraron el 80% de los tubos de magnetrón utilizados en los Estados Unidos y los radares británicos y desarrollaron piezas para el fusible de proximidad crucial en los proyectiles antiaéreos, entre otros equipos.

[210] GPS, *Next Generation Operational Control System (OCX),* [en línea]. Dirección URL: https://www.gps.gov/systems/gps/control/OCX/. [Fecha de consulta: 31 de octubre de 2017].

[211] El Centro de Sistemas Espaciales y de Misiles del Comando Espacial de la Fuerza Aérea, ubicado en la Base de la Fuerza Aérea de Los Ángeles es el centro de adquisición de excelencia de la Fuerza Aérea de Estados Unidos para adquirir y desarrollar sistemas espaciales militares. Su cartera incluye el Sistema de Posicionamiento Global, las comunicaciones militares por satélite, los satélites meteorológicos de defensa, los sistemas espaciales de lanzamiento y alcance, las redes de control de satélites, los sistemas infrarrojos basados en el espacio y las capacidades de conciencia de la situación espacial.

Estados Unidos aceptó la entrega del Sistema de Posicionamiento Global del Sistema de Control Operacional de Siguiente Generación (GPS OCX) del Sistema de Lanzamiento y Verificación (LCS) pues está funcionando como se esperaba durante los ensayos lo que le da confianza para respaldar las operaciones de lanzamiento de los satélites *GPS III* programada para 2018[212].

El Bloque 1 incluye la capacidad operativa para controlar todos los satélites heredados y señales civiles (*L1 C/A*), señales militares (*L1P (Y), L2P (Y)*) así como los satélites *GPS III* y la señal civil modernizada (*L2C*) y la señal de seguridad de vuelo de la aviación (*L5*). Además, este bloque desplegará la capacidad operativa básica para controlar las señales militares modernizadas (*L1M* y *L2M* (código M)) y la señal compatible globalmente (*L1C*). También cumple completamente con los requisitos de defensa cibernética. El Bloque 2 coloca la capacidad operacional avanzada para controlar las características avanzadas de las señales militares modernizadas (*L1M* y *L2M* (código M)) y se entregará al mismo tiempo que el bloque 1.

El nuevo sistema GPS OCX está programado para ofrecer enormes mejoras, lo que aumenta drásticamente el rendimiento y la eficacia de todo el Sistema de Posicionamiento Global. Cambiará el límite a 64 satélites permitiendo una mejor geometría en áreas difíciles de alcanzar y será 10 veces más preciso. También se pretenden implementar altos estándares de ciberseguridad que brindan controles de seguridad de defensa en profundidad multinivel para proteger la misión del GPS de un espectro amplio de amenazas como el *spoofing* y la interferencia.

Sin embargo todo este proceso se ha visto eclipsado debido a un exceso de costos y retrasos en la entrega por fallas de algunos componentes, es por esto que el programa *GPS III* incluye dos esfuerzos como mitigación de riesgos para la entrega tardía de OCX: Operaciones de Contingencia (COps, por sus siglas en inglés) y Uso Previo de M-Code (MCEU, por sus siglas en inglés). Las primeras volarán vehículos espaciales *GPS III* para ser llevados a la constelación operacional, manteniendo los niveles actuales de rendimiento y evitando la degradación.

[212] Los Angeles Air Force Base, *Air Force accepts delivery of GPS Next Generation Operational Control System,* [en línea]. Dirección URL: http://www.losangeles.af.mil/News/Article-Display/Article/1361778/air-force-accepts-delivery-of-gps-next-generation-operational-control-system/. [Fecha de consulta: 5 de noviembre de 2017].

El programa de adquisición actual del Bloque OCX 1 pone en peligro el mantenimiento de la constelación de GPS ya que el segmento de control actual no puede operar satélites *GPS III. GPS III COps* es una modificación del segmento de control de corriente para operar los satélites GPS III de posicionamiento, navegación y temporización y mantener la capacidad limitada de *M-Code* de prueba hasta que se entregue el OCX Bloque 1.

Mientras que el uso temprano de *M-Code* es necesario para proporcionar capacidades básicas de la señal de GPS militar modernizada, conocida como *M-Code*, a la comunidad militar de usuarios de GPS. Sin *M-Code*, los usuarios militares de GPS seguirán estando amenazados por *jamming* y el *spoofing*. Por lo tanto al proporcionar la señal *M-Code* se tendrá mayor nivel de protección contra esas amenazas antes de la entrega del OCX Bloque 1.

Es así, como la imperiosa necesidad de modernizar el Sistema de Posicionamiento Global se ve reflejada en tres aspectos: el nuevo Sistema de Control Operacional de Próxima Generación (OCX), los satélites *GPS III* y el desarrollo de la señal militar *M-Code* fortalecida. Con las amenazas cibernéticas a la infraestructura militar, civil, corporativa y financiera de Estados Unidos que crece exponencialmente y se vuelve mucho más sofisticada, es fundamental que el sistema GPS sea completamente seguro y esté protegido contra *hackeos*, interrupciones o problemas de señal y/o suplantación de información.

La seguridad no se provee simplemente a través de agencias del gobierno y operadores, sino que también se logra a través de la coordinación con fabricantes, empresas, desarrolladores de *software*, otros países e incluso Organizaciones No Gubernamentales, haciendo ver a la cooperación como un factor fundamental en este proceso. Conforme pasa el tiempo los avances tecnológicos y con ellos el perfeccionamiento de técnicas como la interferencia, el *spoofing*, el robo de información o cualquier otro tipo de ciberataque por parte de posibles adversarios harán que el Sistema de Posicionamiento Global actual sea cada vez más vulnerable.

Las amenazas cibernéticas son reales, crecen y han sido una sorpresa estratégica para el gobierno de Estados Unidos al poner en riesgo no sólo sus capacidades militares de ataque y de defensa, sino también las actividades básicas incluidas en el llamado *american way of life*. Donald Trump ha dicho que una de sus

prioridades de defensa es la seguridad cibernética por lo tanto, la modernización del Sistema de Posicionamiento Global con mejoras en la ciberseguridad del mismo, ayudará a asegurar miles de millones en inversiones en su Infraestructura Nacional Crítica y por consiguiente a la conservación de la seguridad nacional.

Lo cierto es que la velocidad a la que avanza la tecnología no permite el aseguramiento por completo del ciberespacio, el constante desarrollo y aplicación de tecnologías y capacidades avanzadas que respondan en la medida de lo posible a los cambios en el entorno es la única forma de combatir los actuales y futuros riesgos y amenazas con el propósito de permitir una protección, disuasión y defensa efectivas. La capacidad de controlar el espacio contribuye a lograr la superioridad de la información y el dominio del espacio de batalla, algo que siempre ha sido de vital interés para los Estados Unidos.

Conclusiones

El ciberespacio ha permitido que dentro de él se desarrolle una gran infraestructura de comunicación global abierta que cualquier persona puede utilizar para compartir, intercambiar o descargar información desde cualquier lugar. Internet por ejemplo, se ha convertido en parte de la vida cotidiana de todos permitiendo además de comunicarse, obtener bienes y servicios, acceder a un cantidad inimaginable de información, crear aplicaciones, obtener indicaciones para llegar a algún lugar, entretenimiento y muchas otras cosas más.

Para 2050, una estimación sugiere que el 66 por ciento de la población mundial, 6.3 miles de millones de personas, vivirá en ciudades. El desarrollo de ciudades inteligentes o *smart cities* ha sido una tendencia mundial importante. Se espera que el mercado global de las mismas alcance los US$1,6 trillones en 2020. Desde la perspectiva de una ciudad inteligente, una tendencia obvia y alarmante es que los ciberataques sigan siendo capaces de causar daños físicos a las plantas y equipos[213].

Los avances tecnológicos en las industrias de oficinas, hogar, transporte y servicios son los cimientos de una ciudad inteligente. Si bien es cierto que Europa y Asia están por encima de los Estados Unidos en la implementación de iniciativas de ciudades inteligentes, varias ciudades estadounidenses han estado haciendo esfuerzos para ofrecer infraestructuras de servicios más inteligentes y eficientes, como por ejemplo Boston, Nueva York, San José, San Francisco y Seattle.

Los expertos dicen que ha faltado un enfoque claro sobre ciberseguridad en las iniciativas de ciudades inteligentes, lo que significa que dichas ciudades se convertirán en objetivos aún más grandes y atractivos para aquellos actores que realizan actividades maliciosas en la red. En 2014, un investigador de ciberseguridad mostró que alrededor de 200,000 sensores de control de tráfico en los principales centros como Washington, DC; Nueva York; New Jersey; San Francisco; Seattle; Lyon; Francia; y Melbourne, Australia no estaban cifrados y, por lo tanto, eran vulnerables a ataques cibernéticos. Los investigadores demostraron que era posible interceptar información proveniente de estos sensores desde 1,500 pies de distancia o por un dron[214].

[213] Tarek, Saadawi; John, Colwell, (editores); *Cyber Infrastructure Protection*, Volume III, Strategic Studies Institute, p.117.
[214] *Ibídem,* p. 105.

La importancia y capacidad de la tecnología ha crecido, por lo que la cantidad de las operaciones llevadas a cabo en la red llevó implícito un apresurado aumento de las actividades ilícitas cometidas en ella poniendo en riesgo datos, sistemas e infraestructuras que desempeñan papeles críticos en el funcionamiento de una ciudad o un país. Dicho lo anterior, la ciberseguridad y la ciberdefensa se han convertido en áreas prioritarias dentro de las agendas de seguridad con el fin de salvaguardar la seguridad de los ciudadanos y por consiguiente, la seguridad nacional.

En la década de 1990 y a principios del siglo XXI los análisis sobre ciberseguridad estaban dominados por ingenieros y programadores de computadoras al considerar que el tema era fundamentalmente técnico, por lo que los problemas se solucionaban con el desarrollo de sistemas de protección de software. Por supuesto hoy en día varias cosas han cambiado desde entonces; la primera y más notable es que la tecnología en redes se ha desarrollado de una manera exponencial y por lo tanto, se ha vuelto más compleja.

En segundo lugar, los ciberataques han diversificados sus motivaciones, yendo desde asuntos políticos, económicos, hasta sociales y militares. A medida que la sociedad exigía sistemas cibernéticos más interactivos y con una mayor capacidad, el estar expuesto a ataques a través de estos sistemas también crecía. Cada vez hay más pruebas de que tanto gobiernos como grupos insurgentes o individuos utilizan las plataformas cibernéticas como una forma de perpetrar ataques.

Por último, pero no menos importante, las innovaciones en la tecnología cibernética que se producen cada segundo hacen que las armas cibernéticas se vuelvan cada vez más sofisticadas y que el mismo mercado creado por la red, permita que éstas puedan llegar a manos de cualquier persona haciendo que los ciberataques sean cada vez más asequibles. Las tendencias en el desarrollo de la tecnología han permitido comprobar que los esfuerzos para defenderse de los ciberataques siempre serán más caros que los esfuerzos para desarrollar nuevas formas de ataque.

Estando conscientes de lo anterior entonces, ¿qué se puede hacer para combatir los ciberataques? Algunos actores ya sea gobiernos o Estados, organizaciones, empresas o individuos, han encontrado la respuesta en el aumento de la sofisticación tecnológica, desarrollando formas más rápidas de contrarrestar las ciberamenazas e

incrementando la ciber resiliencia de sus infraestructuras en caso de ser atacadas, entrando así en una especie de guerra tecnológica.

Otros más, al tener en cuenta que las ciberamenazas se difunden a través de redes cada vez más conectadas, han optado por contar con sistemas que no estén integrados de una manera total con la infraestructura cibernética más grande, es decir, cuentan con una especie de sistemas aislados que permiten que en caso de un ciberataque éstos se puedan rescatar o resultar menos dañados.

Actores como son los gobiernos de los países u organizaciones internacionales, han puesto sobre la mesa la necesidad de un organismo internacional independiente que tenga la facultad de supervisar, abordar y tomar las acciones legales pertinentes en caso de ciberdelitos internacionales, ciberataques, ciberespionaje, guerras cibernéticas y todas aquellas actividades ilícitas en el ciberespacio. El *Manual de Tallín* por ejemplo, surgió justo de esta necesidad de abordar de forma legal las acciones llevadas a cabo en una guerra cibernética[215].

Algunos más, combinan todas las posibilidades antes descritas. Lo cierto es que la evolución de la ciberseguridad requiere una comprensión nueva y más profunda de las dinámicas sociales, económicas y políticas que han ocasionado que surjan todo tipo de ciberamenazas y que el tema no se puede tratar de la misma manera que la seguridad convencional ha sido tratada porque el entorno es totalmente diferente.

A pesar de que la tecnología especializada es necesaria para contrarrestar los ataques cibernéticos y para garantizar la seguridad, muchos países, organizaciones o empresas aún no cuentan con una estrategia de ciberseguridad ni asignan los recursos necesarios para hacer frente a estos problemas. Se trata de un fracaso significativo dada

[215] El Centro de Excelencia para la Ciberdefensa Cooperativa de OTAN (CCD COE) publicó en el año 2013 una primera versión del "Manual de Tallín" (*Tallinn Manual on the International Law Applicable to Cyber Warfare*), documento que examina cómo poder aplicar las normas existentes de derecho internacional a la nueva Ciberguerra. El CCD COE es un Centro de Excelencia que recoge la capacidad de Ciberdefensa de la OTAN, creado en el año 2008, en Tallín (Estonia), y que pretende aunar los esfuerzos de los países que patrocinan el centro: Estonia, Letonia, Lituania, Alemania, Hungría, Italia, Polonia, Eslovenia, España, Holanda y Estados Unidos.
El Manual de Tallín no es un documento oficial por tanto no refleja la doctrina de la OTAN, ni la postura de las Organizaciones o Estados representados, ni la del propio centro. El manual es un documento que recoge las opiniones de un grupo de expertos independientes. En este manual se identifica por un lado el derecho internacional que puede aplicarse a la ciberguerra y, por otro, se establecen 95 normas que deberían regir este tipo de conflictos. Aborda temas como la soberanía, la responsabilidad de los Estados, el "jus ad bellum", el "jus in bello", el derecho humanitario internacional y la ley de neutralidad, entre otros. Cada norma definida tiene asociada una explicación que establece la regla de base en tratados y describe cómo el grupo de expertos interpretaría las normas aplicables en el contexto cibernético. También recoge los desacuerdos del grupo en cuanto a la aplicación de cada regla.

la sustancial y creciente dependencia de la sociedad de las redes para desarrollar sus actividades cotidianas.

Cada organización debe identificar, priorizar e implementar las políticas requeridas para defender su información más sensible e infraestructura de red, así como desarrollar un plan de resiliencia que le permita llevar a cabo su misión con eficacia, si es atacado. Debido a que gran parte de la actividad humana depende ahora de activos e infraestructura basados en el espacio, la infraestructura crítica de la mayoría de los países es potencialmente vulnerable a los ataques cibernéticos en ese dominio como es el caso que se presentó en esta investigación.

Como se expuso en este trabajo, Estados Unidos comenzó a adentrarse en temas de seguridad informática con la creación de ARPANET y la aparición en 1988 del Gusano Morris, teniendo como consecuencia la formación del Equipo de Respuesta ante Emergencias Informáticas (CERT) para atender futuros ataques informáticos. No obstante, es hasta el año 2010 con la Revisión Cuadrienal de la Seguridad Nacional que se mencionó de manera formal el concepto de ciberseguridad y se identificó el objetivo de salvaguardar y asegurar el ciberespacio como una de las cinco misiones prioritarias para la seguridad nacional de Estados Unidos.

Asimismo, en ese año también se creó el Cibercomando de Estados Unidos (USCYBERCOM) bajo el mando del Comando Estratégico. Para el año 2011, el presidente Barack Obama lanzó la *Estrategia Internacional para el Ciberespacio: Prosperidad, Seguridad y Apertura en un Mundo en Red* considerada como una hoja de ruta que permitió a los departamentos y agencias del gobierno definir y coordinar mejor su papel en la política internacional del ciberespacio.

En esa estrategia se reconoce que el rápido crecimiento de las redes trajo consigo nuevos desafíos para la seguridad nacional y económica y la de la sociedad internacional. Estos fueron los primeros pasos del gobierno estadounidense en cuestiones de ciberseguridad. Por otro lado, fue en la *Estrategia de Seguridad Nacional para un Nuevo Siglo de 1998* donde se incluyó por primera vez la protección a las infraestructuras críticas. En ese mismo año el entonces presidente Bill Clinton firmó la Directiva Presidencial de Decisión 63 en la que expresa que el gobierno tomará las medidas necesarias para eliminar cualquier vulnerabilidad significativa a ataques físicos o de información sobre las infraestructuras críticas estadounidenses.

Además, en este documento se reconoce la alta dependencia del poder militar y económico de Estados Unidos de ciertas infraestructuras críticas y de sistemas de información basados en el ciberespacio. En el año 2013 se publicó el *Plan Nacional de Protección de la Infraestructur*a con el fin de fortalecer la seguridad y la resistencia de la infraestructura crítica de la nación. Aquí, se acepta que el entorno de riesgo que afecta a la infraestructura crítica es complejo e incierto pues las amenazas, vulnerabilidades y consecuencias han evolucionado en los últimos 10 años.

La infraestructura crítica, que durante mucho tiempo estuvo sujeta a riesgos asociados con amenazas físicas y desastres naturales, ahora está cada vez más expuesta a ciberataques derivados de la creciente integración de las tecnologías de la información y las comunicaciones con las operaciones de infraestructura crítica. Hay que recordar que la infraestructura crítica de Estados Unidos está compuesta por instituciones privadas y públicas en diferentes sectores y que el ciberespacio es el sistema de control de todos esos servicios, por lo tanto, el óptimo funcionamiento del mismo es esencial para la economía y la seguridad nacional del país.

El Sistema de Posicionamiento Global forma parte esencial de la infraestructura crítica estadounidense dentro del sector de telecomunicaciones y como se comprueba en esta investigación, la infraestructura espacial es uno de los sectores que hoy en día se consideran más vulnerables. Un ataque al GPS, desde el interior o el exterior, establece una prioridad para Estados Unidos porque se pone en juego la estabilidad y seguridad de la nación.

Los satélites y la infraestructura espacial que también incluye vehículos espaciales y estaciones terrestres, son potencialmente vulnerables a una amplia gama de ciberataques, desde los más comunes como el robo de datos e información, así como a ataques más específicos del sector como la interferencia o el bloqueo de señal satelital. Hoy, el Sistema de Posicionamiento Global es la columna vertebral de la gran mayoría de la infraestructura virtual y física por lo que es algo que vale la pena conocer y por supuesto, proteger.

El GPS no es sólo para uso de navegación de los militares o una herramienta personal para encontrar un sitio, también es la referencia de sincronización de sistemas globales que forman parte de la vida diaria y que permiten el funcionamiento de múltiples actividades, desde sistemas bancarios y transacciones financieras, hasta de redes

eléctricas y telefónicas. En otras palabras, si internet fuera la autopista, el GPS sería el semáforo que permite un flujo seguro y eficiente[216].

Es por todo lo anterior que si el Sistema de Posicionamiento Global sufriera algún tipo de ciberataque, la vida de miles de millones de personas se vería afectada y en consecuencia, sería visto como un ataque a la seguridad nacional de Estados Unidos por ser éste quien controle dicho sistema. Hasta la fecha no ha habido un ataque estratégico contra el GPS, sin embargo, eso no quiere decir que esté a salvo de uno y que sea considerado como un talón de Aquiles y un objetivo con mucho potencial por la importancia que representa.

Las amenazas cibernéticas son reales, crecen y han sido una sorpresa estratégica para el gobierno de Estados Unidos que teme el sufrir ciberataques por parte de gobiernos extranjeros hostiles o actores no estatales. En la actualidad no es descabellado pensar que Rusia y China por ejemplo, que han estado desarrollando y evolucionando sus capacidades de intrusión cibernética, o grupos como el Estado Islámico, utilicen el ciberespacio como una arma de ataque muy eficiente.

El enemigo puede estar en cualquier parte del mundo, y las consecuencias para la seguridad nacional serán graves a menos que se le dé un seguimiento al compromiso de actualizar y proteger la infraestructura crítica como lo es el Sistema de Posicionamiento Global. Con ese fin por ejemplo, se ha lanzado el Sistema de Control Operacional de Próxima Generación, también conocido como proyecto OCX que plantea una evolución continua de sus satélites y una mejora significativa del segmento terrestre del GPS.

Empero, la vigilancia continua viene con un alto precio y este programa de actualización ha sido criticado en constantes ocasiones por creer que es excesivamente costoso y por los numerosos retrasos en la entrega del mismo. Los satélites *GPS III* y el desarrollo de la señal militar *M-Code* son los otros dos esfuerzos que Estados Unidos en conjunto con empresas privadas ha estado desarrollando con el fin de que el GPS sea completamente seguro y esté protegido.

El Sistema de Posicionamiento Global fue diseñado como un sistema de doble uso (militar y civil) con el objetivo principal de mejorar la efectividad de las fuerzas

[216] The Hill, *Cyber protection a priority for GPS*, [en línea]. Dirección URL:http://thehill.com/blogs/congress-blog/technology/261982-cyber-protection-a-priority-for-gps. [Fecha de consulta: 10 de diciembre de 2017].

militares estadounidenses y aliadas. Al proporcionar una ventaja militar sustancial se está integrando en prácticamente todas las facetas de las operaciones militares estadounidenses por lo que las amenazas directas y omnipresentes contra estas capacidades y el *American way of life* no tienen precedentes.

La creciente demanda de usuarios militares, civiles, comerciales y científicos ha generado que el GPS se convierta de manera rápida en un componente integral de la infraestructura de información global con aplicaciones que van desde el mapeo y la topografía hasta el funcionamiento de redes celulares y la gestión del tráfico aéreo internacional. Estados Unidos al ser el inventor y el proveedor de servicios del GPS tiene en sus manos una gran responsabilidad y un enorme poder cibernético que también debe proteger[217].

Es por todo lo desarrollado en esta investigación que la necesidad de una protección adecuada de las infraestructuras críticas es imperiosa. Un entorno inseguro en el espacio obstaculizará el desarrollo económico y aumentará los riesgos para las sociedades en sectores cruciales como comunicaciones, transporte (aéreo, marítimo y terrestre), transacciones financieras, energía (convencional, renovable y nuclear), agricultura, alimentos y otros recursos, medio ambiental y por supuesto, defensa. Por lo tanto, es necesario abordar las lagunas y deficiencias de ciberseguridad relacionadas con el espacio con carácter de urgencia.

Aunque la ciberseguridad es un problema técnico, la tecnología por sí sola no puede resolver los obstáculos que se presenten y hacerlo excluiría a muchas partes interesadas que podrían contribuir de forma útil para encontrar así, en conjunto, las respuestas a la variedad de amenazas propagadas a través de la red. Por lo tanto, un régimen eficaz para combatir los desafíos de la ciberseguridad requiere ver el problema desde un enfoque multidisciplinario que permita la participación integral de un círculo de actores desde los estatales, hasta empresas y organizaciones que coadyuven a ampliar el conocimiento y la comprensión del mismo.

Muchos expertos consideran que “un régimen internacional de ciberseguridad espacial en el que participen múltiples partes interesadas, basado en una comunidad internacional de las evaluaciones de riesgo y respuestas de amenaza compartidas y

[217] El poder cibernético se define como la capacidad de utilizar el ciberespacio para crear ventajas e influir en los eventos en otros entornos operativos y en todos los instrumentos de poder.

dispuestas, podría brindar la mejor oportunidad para desarrollar una respuesta sectorial que coincida con la gama de amenazas"[218].

Asimismo, creen que "el producir un conjunto de opciones para mitigar los riesgos traería beneficios previsibles y tangibles para la infraestructura espacial al aumentar la resiliencia de la infraestructura económica mundial a las amenazas cibernéticas y aumentar la confianza en los bienes y servicios espaciales, incluidos los asociados con los nuevos mercados mundiales en ciberseguridad espacial"[219].

La verdadera cuestión en ese caso sería ¿cuáles actores estarían dispuestos y cuáles no, a colaborar para que eso suceda?, ¿en qué medida? y ¿qué tanta es su necesidad por protegerse de las ciberamenazas como para compartir sus estrategias de seguridad con los demás actores? Las empresas privadas que desarrollan *software* por ejemplo, perderían millones en ganancias si decidieran compartir todos sus conocimientos en cuestiones de ciberseguridad. Además, si se piensa que éstas en mayor medida son quienes también crean los virus informáticos, las pérdidas son mayores que las ganancias.

Los Estados por otra parte, podrían verlo como un riesgo para su seguridad nacional ya que los demás sabrían con qué tipo de estrategias de ciberseguridad cuentan y eso facilitaría la forma en la se puede perpetrar un ataque. Lo cierto es que ningún actor de la sociedad internacional se encuentra a salvo de las amenazas procedentes del ciberespacio, y si no se toman acciones, aunque éstas a su vez conlleven riesgos, el problema será más difícil de resolver. Estos puntos seguirán siendo de gran controversia al poner la opción sobre la mesa de debate y sin duda alguna, originarán diversos obstáculos en dicho proceso.

[218] David, Livingstone; Patricia, Lewis, *Op. Cit*, p. 37.
[219] *Ídem.*

Glosario

1. Arma cibernética: Software, firmware o hardware diseñado o aplicado para causar daños a través del dominio cibernético[220].
2. ARPANET: (Advanced Research Projects Agency NETwork) Red Avanzada de Agencias para Proyectos de Investigación. Red de conmutación de paquetes desarrollada a principios de la década de los setenta por ARPA, se considera el origen de la actual red Internet.
3. Backbone: Es el enlace principal de una red, es el cableado que comunica todos los cuartos de telecomunicaciones con el cuarto de equipos. Mecanismo de conectividad primario en un sistema distribuido. Todos los sistemas que tengan conexión al backbone (columna vertebral) pueden interconectarse entre sí, aunque también puedan hacerlo directamente o mediante redes alternativas[221].
4. Botnets: Es una red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques de denegación de servicio distribuido (DDoS) sin el conocimiento o el consentimiento de los propietarios reales de los equipos. Estas redes de ordenadores zombis son gestionadas por los spammer que las utilizan para sacar miles de mensajes diariamente hacia direcciones de correo de todo el mundo[222].
5. Ciberamenaza: un peligro, ya sea comunicado o detectado, que puede ejercer una vulnerabilidad cibernética[223].
6. Cibercrimen: es el uso del ciberespacio para fines delictivos según lo define la legislación nacional o internacional. Dadas las leyes establecidas que definen la actividad delictiva, el término de cibercrimen está diseñado deliberadamente para hacer referencia inmediata a las estructuras legales existentes. Se entiende que las consideraciones jurisdiccionales tienen un rol integral en la aplicación de este término. Las complejidades surgen cuando las actividades son realizadas por un individuo en un país, utilizando recursos cibernéticos en otro (segundo) país, y afectando a alguien, organización u otra entidad en un tercer país[224].

   Cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo

[220] EastWest Institute, *Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity,* [en línea], 2014, p. 56. Dirección URL: https://www.eastwest.ngo/idea/critical-terminology-foundations-2. [Fecha de consulta: 24 de junio de 2017.]

[221] TechTarget, *Backbone,* [en línea]. Dirección URL: http://searchdatacenter.techtarget.com/es/definicion/Backbone. [Fecha de consulta: 30 de agosto de 2017].

[222] Avast, *Bonet,* [en línea]. Dirección URL: https://www.avast.com/es-es/c-botnet. [Fecha de consulta: 25 de junio de 2017].

[223] EastWest Institute, *Op. Cit.,* p. 38.

[224] EastWest Institute, *Op. Cit.,* p. 29.

informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito[225].

7. Ciberdelincuencia: un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos. Los actos comprendidos habitualmente en la categoría de ciberdelincuencia son aquellos en los que los datos o sistemas informáticos son el objeto contra el que se dirige el delito, así como los actos en que los sistemas informáticos o de información forman parte integrante del modus operandi del delito[226].

   Ciberguerra o guerra cibernética: es un estado escalado de conflicto cibernético entre Estados en el que los ciberataques son llevados a cabo por actores estatales contra la infraestructura cibernética como parte de una campaña militar. Si no hay actores políticos, entonces esto no es una guerra. La guerra cibernética puede ser más que estrictamente una actividad militar, especialmente al principio, es decir, una operación de inteligencia. La guerra cibernética puede ser conducida de diferentes maneras por diferentes grupos.

   Hay una tendencia de la guerra convencional a incluir la guerra cibernética.

   (i) Declarada: formalmente declarado por una autoridad de una de las partes.

   (ii) De facto: con la ausencia de una declaración[227].

8. Ciudad inteligente: implica el uso de la tecnología para reunir y analizar datos y tomar medidas para mejorar la eficiencia y mejorar la calidad de vida[228].
9. Conflicto cibernético: es una situación tensa entre y/o entre Estados-nación y/o grupos organizados donde los ciberataques no deseados resultan en represalias[229].

   El conflicto cibernético generalmente precede a la guerra cibernética.
10. Firmware: Es una mezcla o híbrido entre el hardware y el software, es decir tiene parte física y una parte de programación consistente en programas internos implementados en memorias no volátiles. Podría decirse que el firmware funciona como el nexo entre las instrucciones que llegan al dispositivo desde el exterior y sus diversas partes electrónicas[230].

---

[225] María Concepción, Rayón Ballesteros; José Antonio, Gómez Hernández, *Cibercrimen: particularidades en su investigación y enjuiciamiento,* p. 3. [en línea]. Dirección URL: https://dialnet.unirioja.es/descarga/articulo/4639646.pdf. [Fecha de consulta: 3 de noviembre de 2017].

[226] Organización de las Naciones Unidas, *El fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional,* 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 2015. Dirección URL: https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf. [Fecha de consulta: 20 de octubre de 2017].

[227] EastWest Institute, *Op. Cit.,* p. 32.

[228] Tarek, Saadawi; John D., Colwell (editors), *Cyber Infrastructure Protection*, Volume III, Strategic Studies Institute, 2017, p. 108.

[229] EastWest Institute, *Op. Cit.,* p. 31.

[230] Definición, *Firmware,* [en línea]. Dirección URL: https://definicion.de/firmware/. [Fecha de consulta: 25 de junio de 2017].

Un conjunto de instrucciones que forman parte de un dispositivo electrónico y le permiten comunicarse con una computadora o con otros dispositivos electrónicos[231].

11. Gusano: Es un programa similar a un virus que se diferencia de éste en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos solamente realizan copias de ellos mismos.
12. Intranet: Una red de equipos que es interna a una organización y es compatible con aplicaciones de Internet, especialmente el WWW. La mayoría de las intranet están configuradas de forma que sus usuarios puedan tener acceso a Internet sin permitir que los usuarios de Internet tengan acceso a los equipos de la Intranet[232].
13. Malware: Acrónimo de Malicious Software, es un término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar los virus, troyanos, gusanos, botnets, ransomwares, spyware, entre otros[233].
14. Ransomware: Es un código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga[234].
15. Sociedad de la información: Un estadio de desarrollo social caracterizado por la capacidad de sus miembros (ciudadanos, empresas y administración pública) para obtener y compartir cualquier información, instantáneamente, desde cualquier lugar y en la forma en que se prefiera[235].
16. Spyware: También conocido como software espía, es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento. Este software envía información a sus servidores, en función a los hábitos de navegación del usuario. También, recogen datos acerca de las webs que se navegan y la información que se solicita en esos sitios, así como direcciones IP y URLs que se visitan[236].

---

[231] Cambridge Dictionary, *firmware,* [en línea]. Dirección URL: https://dictionary.cambridge.org/es/diccionario/ingles/firmware. [Fecha de consulta: 25 de junio de 2017].

[232] La Web del programador, *Intranet,* Diccionario informático, [en línea]. Dirección URL: http://www.lawebdelprogramador.com/diccionario/buscar.php?opc=1&charSearch=intranet. [Fecha de consulta: 30 de mayo de 2017].

[233] Avast, *Malware,* [en línea]. Dirección URL: https://www.avast.com/es-es/c-malware. [Fecha de consulta: 25 de junio de 2017].

[234] Panda Security, *Ransomware,* [en línea]. Dirección URL: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/. [Fecha de consulta: 20 de junio de 2017.]

[235] Universidad Nacional de San Juan, *Concepto de Sociedad de la Información,* [en línea]. Dirección URL: http://www.unsj.edu.ar/unsjVirtual/comunicacion/seminarionuevastecnologias/wp-content/uploads/2015/05/concepto.pdf. [Fecha de consulta: 20 de mayo de 2017.]

[236] Avast, *Spyware,* [en línea]. Dirección URL: https://www.avast.com/es-es/c-spyware. [Fecha de consulta: 25 de junio de 2017].

17. Tecnologías de la Información y la Comunicación: Conjunto de elementos compuesto por herramientas, prácticas y técnicas que son utilizados para el tratamiento, procesamiento, almacenamiento, y transmisión de datos con la finalidad de estructurarlos en información útil que derive en la solución de problemas y la generación de conocimiento[237].
18. Troyano: Es un programa malicioso que se oculta en el interior de un programa de apariencia inocente. Cuando este último es ejecutado, el troyano realiza la acción o se oculta en la máquina del incauto que lo ha ejecutado. Habitualmente se utiliza para espiar a personas, usando esta técnica para instalar un software de acceso remoto que nos permita monitorear lo que alguien está haciendo en cada momento o enviando capturas de pantalla del escritorio[238].
19. Virus informático: Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos[239].

[237] Dora Alicia, Reyes Echeagaray (coordinadora), *Tecnologías de la Información y Comunicación en las Organizaciones,* UNAM, México, 2016, p. 14.
[238] Avast, *Troyano,* [en línea]. Dirección URL: https://www.avast.com/es-es/c-trojan. [Fecha de consulta: 25 de junio de 2017].
[239] Avast, *Virus informático,* [en línea]. Dirección URL: https://www.avast.com/es-es/c-computer-virus. [Fecha de consulta: 25 de junio de 2017].

Índice de siglas y abreviaturas

AEE. Agencia Espacial Europea.

AFCYBER. Air Forces Cyber.

ARCYBER. Army Cyber Command.

ARPA. Advanced Research Projects Agency.

ARPANET. Advanced Research Projects Agency Network.

BDS. BeiDou Navigation Satellite System.

BID. Banco Interamericano de Desarrollo.

CERT. Equipo de Respuesta ante Emergencias Informáticas.

CGCYBER. Coast Guard Cyber.

CIA. Central Intelligence Agency.

CIIP. Protección de la Infraestructura de Información Crítica.

CIP. Protección de la Infraestructura Crítica.

CORS. Continuously Operating Reference Stations.

CSIRTs. Equipos de Respuesta a Incidentes de Seguridad Informática.

CSIS. Center for Strategic and International Studies.

DHS. Department of Homeland Security.

DoD. Department of Defense.

ENISA. European Union Agency for Network and Information Security.

FAA. Federal Aviation Administration.

FBI. Federal Boreau Institute.

FedCIRC. Centro Federal de Respuesta a Incidentes Informáticos.

FLTCYBER. Fleet Cyber Command.

GATT. General Agreement on Tariffs and Trade.

GEANC. Grupo de Expertos de Alto Nivel sobre Cibersegruidad.

GLONASS. Globalnaya Navigazionnaya Sputnikovaya Sistema.

GNSS. Global Navigation Satellite Systems.

GPS. Global Positioning System.

GPSOC. Centro de Operaciones GPS.

ICANN. Internet Corporation for Assigned Names and Numbers.

ICE. Infraestructuras Críticas de la Unión Europea.

ICG. International Committee on Global Navigation Satellite Systems.

ICN. Infraestructuras Críticas Nacionales.

ICS. Industrial Control Systems.

IGS. International GNSS Service.

IRNSS. Indian Regional Navigation Satellite System.

ISOC. Internet Society.

L1 C/A. Primera señal civil del GPS.

L1C. Cuarta señal civil del GPS.

L2C. Segunda señal civil del GPS.

L5. Tercera señal civil del GPS.

MARFORCYBER. Marine Corps Forces Cyberspace Command.

MCS. Master Control Station.

MIT. Massachusetts Institute of Technology.

NASA. National Aeronautics and Space Administration.

NAVCEN. U.S. Coast Guard Navigation Center.

NavIC. Navigation Indian Constellation.

NDGPS. Nationwide Differential Global Positioning System.

NGA. National Geospatial-Intelligence Agency.

NIPC. National Infrastructure Protection Center.

NIPP. National Infrastructure Protection Plan.

NMS-CO. National Military Strategy for Cyberspace Operations.

NSA. National Security Agency.

NSC. National Security Council.

OACI. Organización de Aviación Civil Internacional.

OCX. Next Generation Operational Control System.

OEA. Organización de Estados Americanos.

ONU. Organización de las Naciones Unidas.

OTAN. Organización del Tratado del Atlántico Norte.

PEPIC. Plan Europeo para la Protección de Infraestructuras Críticas.

PIC. Protección de Infraestructuras Críticas.

PNT. Positioning, Navigation and Timing.

QZSS. Quasi-Zenith Satellite System.

SCADA. Supervisory Control And Data Acquisition.

SO. Sistemas Operativos.

TIC. Tecnologías de la Información y Comunicación

UIT. Unión Internacional de Telecomunicaciones.

US-CERT. Equipo de Respuesta ante Emergencias Informáticas de Estados Unidos.

USCYBERCOM. United States Cyber Command.

USSTRATCOM. United States Strategic Command.

WAAS. Wide Area Augmentation System.

WWW. World Wide Web.

Índice de esquemas, figuras, gráficas, imágenes, mapas y tablas.

Fuentes de consulta

Bibliografía

- French-Davis, Ricardo, *Macroeconomía, Comercio y Finanzas para Reformar las Reformas en América Latina,* McGraw-Hill Interamericana, Santiago, Chile, 1999, 226 pp.
- Gibson, William, *Neuromante,* Minotauro, España, 1984, 169 pp.
- Gómez, Vieites Álvaro, *Enciclopedia de la seguridad informática.* Alfaomega, México, 2007, 825 pp.
- Hobbes Thomas, *Leviatán. O la materia, forma y poder de una República, Eclesiástica y Civil,* Fondo de Cultura Económica, Buenos Aires, Argentina, 1992, 306 pp.
- Libicki, Martin C., *Cyberdeterrence and Cyberwar,* RAND, USA, 2009, 214 pp.
- Mounier, Pierre; Los Dueños de la Red: Una historia política de Internet, Editorial Popular, España, 2002, 246 pp.
- OEA, Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, 2015, 60 pp.
- OEA; BID, *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?,* Informe Ciberseguridad 2016, 193 pp.
- Reyes, Echeagaray Dora Alicia (coordinadora), *Tecnologías de la Información y Comunicación en las Organizaciones*, UNAM, México, 2016, 302 pp.
- Saadawi, Tarek; Jordan, Louis H. (Coordinadores), *Cyber Infrastructure Protection*, Volume III, Strategic Studies Institute, 261 pp.
- Saadawi, Tarek; Jordan, Louis H.; Boudreau, Vincent, (Editores); *Cyber Infrastructure Protection*, Volume II, Strategic Studies Institute, 27855 pp.
- Sevilla, Rodríguez José Luis, ""Hablando correctamente de seguridad de la información"*, Ambientes óptimos. De la incertidumbre a la acción segura,* Revista Seguridad. Cultura de prevención para TI, No. 20, abril-mayo 2014, México, UNAM, 37 pp.
- Williams, Paul D. (ed.), *Security studies: an introduction,* Routledge, USA, 2008, 464 pp.

Tesis

- Escárcega, García Fredy A., *La estrategia de ciberseguridad de Barack Obama: El ataque (ciberguerra) al Programa Nuclear Iraní en 2010*, FCPyS, UNAM, 2017, 140 pp.

- Zavaleta, Hernández Sandra Kanety, *Más allá de la visión tradicional de la seguridad y del desarrollo. Hacia la consecución de la seguridad humana y el desarrollo humano en las relaciones internacionales contemporáneas,* Tesis doctoral, FCPyS-UNAM, México, 2012, 314 pp.

Cibergrafía

- Arriola, Jonathan; Bonilla, Saus Javier; Campo Macarena del, *Hugo Grocio: en los orígenes del pensamiento internacional moderno,* [en línea], Universidad ORT Uruguay, 2010. Dirección URL: https://dspace.ort.edu.uy/bitstream/handle/20.500.11968/2779/documentodeinvestigacion59.pdf. [Fecha de consulta: 5 de julio de 2017].
- Avast, *Bonet*, [en línea]. Dirección URL: https://www.avast.com/es-es/c-botnet. [Fecha de consulta: 25 de junio de 2017].
- Avast, *Malware*, [en línea]. Dirección URL: https://www.avast.com/es-es/c-malware. [Fecha de consulta: 25 de junio de 2017].
- Avast, *Spyware*, [en línea]. Dirección URL: https://www.avast.com/es-es/c-spyware. [Fecha de consulta: 25 de junio de 2017].
- Avast, *Troyano*, [en línea]. Dirección URL: https://www.avast.com/es-es/c-trojan. [Fecha de consulta: 25 de junio de 2017].
- Avast, *Virus informático*, [en línea]. Dirección URL: https://www.avast.com/es-es/c-computer-virus. [Fecha de consulta: 25 de junio de 2017].
- Bloomberg Politics, *Outer-Space Hacking a Top Concern for NASA's Cybersecurity Chief,* [en línea], abril de 2017. Traducción propia. Dirección URL: https://www.bloomberg.com/news/articles/2017-04-12/outer-space-hacking-a-top-concern-for-nasa-s-cybersecurity-chief. [Fecha de consulta: 23 de octubre de 2017].
- Buckland, Benjamin S.; Schreier, Fred; Winkler, Theodor H., *Democratic Governance Challenges of Cyber Security,* [en línea], 2015. Dirección URL: http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security. [Fecha de consulta: 16 de junio de 2017].
- Cambridge Dictionary, *Firmware*, [en línea]. Dirección URL: https://dictionary.cambridge.org/es/diccionario/ingles/firmware. [Fecha de consulta: 25 de junio de 2017].
- Carrasco, Luis de Salvador, *Ciber-resiliencia,* [en línea], Instituto Español de Estudios Estratégicos, Abril, 2015, 15 pp. Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf. [Fecha de consulta: 3 de julio de 2017].
- Coast Guard Navigation Center, *Vulnerability Assessment of the Transportation Infrastructure relying on the Global Positioning System,* [en línea], John A. Volpe National Transportation Systems Center, August 29, 2001, 113 pp. Dirección URL: https://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf. [Fecha de consulta 19 de octubre de 2017].
- CSIS, *From Awareness to Action. A Cybersecurity Agenda for the 45th President,* [en línea], 34 pp. Dirección URL: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf. [Fecha de consulta: 18 de julio de 2017].
- Defense Technical Information Center, *Report to the Commission to Assess United States National Security Space Management and Organization,* [en línea], 11 de enero de 2001, 161 pp. Dirección URL: http://www.dtic.mil/docs/citations/ADA404328. [Fecha de consulta: 20 de octubre de 2017].
- Definición, Firmware, [en línea]. Dirección URL: https://definicion.de/firmware/.

[Fecha de consulta: 25 de junio de 2017].

- Department of Defense, *Department of Defense Strategy for Operating in Cyberspace,* [en línea], 2011, 19 pp. Dirección URL: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. [Fecha de consulta: 16 de julio de 2017].
- Department of Defense, *The DoD Cyber Strategy,* [en línea], 2015, 42 pp. Dirección URL: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.
- Department of Homeland Security, *About DHS,* [en línea]. Dirección URL: https://www.dhs.gov/about-dhs. [Fecha de consulta: 15 de julio de 2017].
- Department of Homeland Security, *National Risks Estimate: Risks to US critical infrastructure from global positioning system disruptions,* [en línea], 222 pp. Dirección URL: https://rntfnd.org/wp-content/uploads/DHS-National-Risk-Estimate-GPS-Disruptions.pdf. [Fecha de consulta: 20 de octubre de 2017].
- Department of Homeland Security, *Quadrennial Homeland Security Review,* [en línea], 2010, 4 pp. Dirección URL: https://www.dhs.gov/sites/default/files/publications/2010-qhsr-executive-summary.pdf.
- Department of Homeland Security, *The 2014 Quadrennial Homeland Security Review,* [en línea], 104 pp. Traducción propia. Dirección URL: https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.
- Department of State, *National Security Act of 1947,* [en línea], Office of the Historian. Dirección URL: https://history.state.gov/milestones/1945-1952/national-security-act. [Fecha de consulta: 11 de julio de 2017].
- Department of State, *NSC-68, 1950,* [en línea], Office of the Historian. Dirección URL: https://history.state.gov/milestones/1945-1952/NSC68. [Fecha de consulta: 11 de julio de 2017].
- DHS, *Cybersecurity Overview*, [en línea]. Dirección URL: https://www.dhs.gov/cybersecurity-overview. [Fecha de consulta: 14 de agosto de 2016.]
- DHS, *Homeland Security Act of 2002,* [en línea], 187 pp. Dirección URL: https://www.dhs.gov/homeland-security-act-2002. [Fecha de consulta: 19 de julio de 2017].
- DHS, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience,* [en línea], 57 pp. Dirección URL: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience. [Fecha de consulta: 20 de julio de 2017].
- DHS, *National Infrastructure Protection Plan,* [en línea], 2009, 188 pp. Dirección URL: https://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. [Fecha de consulta: 19 de julio de 2017].
- DHS, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets,* [en línea], 2003, 96 pp. Dirección URL:https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf. [Fecha de consulta: 20 de julio de 2017].
- DHS, *Office of Infrastructure Protection Strategic Plan: 2012–2016,* [en línea], 20 pp. Dirección URL: https://www.dhs.gov/sites/default/files/publications/IP-Strategic-Plan-FINAL-508.pdf. [Fecha de consulta: 19 de julio de 2017].
- DHS, *Office of Infrastructure Protection,* [en línea]. Dirección URL: https://www.dhs.gov/office-infrastructure-protection. [Fecha de consulta: 19 de julio de 2017].

- Discursos para la historia, *El discurso inaugural de Bill Clinton,* [en línea]. Dirección URL: https://discursosparalahistoria.wordpress.com/2010/03/26/el-discurso-inaugural-de-bill-clinton/. [Fecha de consulta: 12 de julio de 2017].
- DoD, *Dictionary of Military and Associated Terms: cyberspace,* [en línea]. Dirección URL: http://www.dtic.mil/doctrine/dod_dictionary/?zoom_query=cyberspace&zoom_sort=0&zoom_per_page=10&zoom_and=1. [Fecha de consulta: 25 de noviembre de 2016].
- EastWest Institute, *Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity,* [en línea], 2014, 82 pp. Dirección URL: https://www.eastwest.ngo/idea/critical-terminology-foundations-2. [Fecha de consulta: 24 de noviembre de 2016].
- Encyclopedia Britannica, *Rockwell International Corporation,* [en línea]. Dirección URL: https://www.britannica.com/topic/Rockwell-International-Corporation. [Fecha de consulta: 28 de agosto de 2017].
- Escuela Superior de Ingenieros de Telecomunicaciones, *Seguridad nacional y ciberdefensa. Aproximación conceptual: ciberseguridad y ciberdefensa,* [en línea], Madrid, Enero de 2013, 11 pp. Dirección URL: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf. [Fecha de consulta: 25 de noviembre de 2016].
- ESET, *La seguridad como rehén. Tendencias 2017,* [en línea], 58 pp. Dirección URL: http://www.eset-la.com/centro-prensa/articulo/2016/eset-informe-tendencias-2017-la-seguridad-como-rehen/4429. [Fecha de consulta: 1 de julio de 2017].
- ESET, *Tendencias 2016: (In) Security Everywhere,* [en línea], 73 pp. Dirección URL: https://www.welivesecurity.com/la-es/2016/01/20/tendencias-2016-seguridad-parte-de-nuestras-vidas/. [Fecha de consulta: 30 de junio de 2017].
- EUR-Lex, *Programa Europeo para la Protección de Infraestructuras Críticas,* [en línea]. Dirección URL: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:l33260. [Fecha de consulta: 30 de mayo de 2017].
- Federal Aviation Administration, *Satellite Navigation - Wide Area Augmentation System (WAAS),* [en línea]. Dirección URL: https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/waas/. [Fecha de consulta: 14 de septiembre de 2017].
- Federation of American Scientists, *National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue,* [en línea], 2000, 199 pp. Dirección URL: https://fas.org/irp/offdocs/pdd/CIP-plan.pdf. [Fecha de consulta: 19 de julio de 2017].
- Federation of American Scientists, *Protecting America's Critical Infrastructures: PDD 63,* [en línea], 1998. Dirección URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm. [Fecha de consulta: 19 de julio de 2017].
- Filosofía, *Jorge Bush: Discurso en el Capitolio*, [en línea]. Dirección URL: http://www.filosofia.org/his/20010921.htm. [Fecha de consulta: 2 de diciembre de 2016].
- Forigua, Rojas Emersson, *El Consejo de Seguridad Nacional de Estados Unidos: evolución, organización y lecciones,* [en línea], Papel Político, vol. 17, núm. 1, enero-junio, 2012, 31 pp. Dirección URL: http://www.redalyc.org/articulo.oa?id=77724876009. [Fecha de consulta: 11 de julio de 2017].
- Fox News, *Military Wipes Out Iraqi GPS Jammers,* [en línea]. Dirección URL: http://www.foxnews.com/story/2003/03/25/military-wipes-out-iraqi-gps-

jammers.html. [Fecha de consulta: 18 de octubre de 2017].
- GFCE, *The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection,* [en línea], 64 pp. Dirección URL: https://www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf.
- Global Geodetic Observing System, *About,* [en línea]. Dirección URL: http://176.28.21.212/en/about/ggos-infos/. [Fecha de consulta: 8 de septiembre de 2017].
- Global Research, *World Conquest: The United States' Global Military Crusade (1945-)*, [en línea]. Dirección URL: http://www.globalresearch.ca/the-united-states-global-military-crusade-1945/4610. [Fecha de consulta: 19 de agosto de 2017].
- Gobierno de España, *Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas,* [en línea], Ministerio de la Presidencia y para las Administraciones Territoriales. Dirección URL: http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630. [Fecha de consulta: 30 de mayo de 2017].
- GPS, *¿Qué es el GPS?*, [en línea]. Dirección URL: http://www.gps.gov/spanish.php. [Fecha de consulta: 18 de agosto de 2017].
- GPS, *Agreement on the Promotion, Provision and Use of Galileo and GPS Satellite-Based Navigation Systems and Related Applications,* [en línea], p. 14. Dirección URL: http://www.gps.gov/policy/cooperation/europe/2004/gps-galileo-agreement.pdf. [Fecha de consulta: 18 de septiembre de 2017].
- GPS, *Agricultura,* [en línea]. Dirección URL: http://www.gps.gov/applications/agriculture/spanish.php. [Fecha de consulta: 22 de septiembre de 2017].
- GPS, *Augmentation Systems,* [en línea]. Dirección URL: http://www.gps.gov/systems/augmentations/. [Fecha de consulta: 13 de septiembre de 2017].
- GPS, *Aviación,* [en línea]. Dirección URL: http://www.gps.gov/applications/aviation/spanish.php. [Fecha de consulta: 22 de septiembre de 2017].
- GPS, *Civil Global Positioning System (GPS) Service Interface Committee Charter,* [en línea]. Dirección URL: http://www.gps.gov/cgsic/charter/. [Fecha de consulta: 8 de septiembre de 2017].
- GPS, *Control Segment,* [en línea]. Dirección URL: http://www.gps.gov/systems/gps/control/. [Fecha de consulta: 18 de agosto de 2017].
- GPS, *Cronometría,* [en línea]. Dirección URL: http://www.gps.gov/applications/timing/spanish.php. [Fecha de consulta: 23 de septiembre de 2017].
- GPS, *Espacio,* [en línea]. Dirección URL: http://www.gps.gov/applications/space/spanish.php. [Fecha de consulta: 23 de septiembre de 2017].
- GPS, *Fiscal Year 2017 Program Funding,* [en línea]. Dirección URL: http://www.gps.gov/policy/funding/2017/. [Fecha de consulta: 13 de septiembre de 2017].
- GPS, *GPS Service Outages & Status Reports,* [en línea]. Dirección URL: http://www.gps.gov/support/user/. [Fecha de consulta: 8 de septiembre de 2017].
- GPS, *Legacy Accuracy Improvement Initiative (L -AII),* [en línea]. Dirección URL: https://www.gps.gov/systems/gps/control/L-AII/. [Fecha de consulta: 25 de octubre

de 2017].
- GPS, *National Coordination Office for Space-Based Positioning, Navigation, and Timing,* [en línea]. Dirección URL: http://www.gps.gov/governance/excom/nco/. [Fecha de consulta: 9 de septiembre de 2017].
- GPS, *Navegación marítima,* [en línea]. Dirección URL: http://www.gps.gov/applications/agriculture/spanish.php. [Fecha de consulta: 22 de septiembre de 2017].
- GPS, *Next Generation Operational Control System (OCX),* [en línea]. Dirección URL: https://www.gps.gov/systems/gps/control/OCX/. [Fecha de consulta: 31 de octubre de 2017].
- GPS, *Organization,* [en línea]. Dirección URL: http://www.gps.gov/governance/excom/
- GPS, *Space Segment,* [en línea]. Dirección URL: http://www.gps.gov/systems/gps/space/. [Fecha de consulta: 18 de agosto de 2017].
- Griffiths, Spielman John, *Teoría de la Seguridad y Defensa en el continente Americano. Análisis de los casos de EE.UU. de América, Perú y Chile,* [en línea], RiL Editores, Chile, 2011, 276-290 pp. Dirección URL: https://books.google.com.mx/books?id=LnAMhN7NXcIC&pg=PA277&lpg=PA277&dq=Acta+Goldwater-Nichols&source=bl&ots=yqBh5insQy&sig=jgIdaMDEjK8MejXSEQAonuIizQ4&hl=es419&sa=X&ved=0ahUKEwjympzXpoTVAhWE7SYKHbsCDBwQ6AEIZjAJ#v=onepage&q=Acta%20Goldwater-Nichols&f=false. [Fecha de consulta: 11 de julio de 2017].
- Hamilton, Alexander; Madison, James; Jay, John, *El Federalista,* [en línea], 376 pp. Dirección URL: https://d3n8a8pro7vhmx.cloudfront.net/danielcassidyforld24/pages/1/attachments/original/1418716919/El-Federalista.pdf?1418716919. [Fecha de consulta: 5 de julio de 2017].
- History, *Lanzamiento del primer gusano informático,* [en línea]. Dirección URL: https://uy.tuhistory.com/hoy-en-la-historia/lanzamiento-del-primer-gusano-informatico. [Fecha de consulta: 17 de mayo de 2017].
- IGS, *About,* [en línea]. Dirección URL: http://www.igs.org/about. [Fecha de consulta: 17 de septiembre de 2017].
- Indian Space Research Organisation, *Indian Regional Navigation Satellite System (IRNSS):NavIC,* [en línea], Department of Space. Dirección URL: https://www.isro.gov.in/irnss-programme. [Fecha de consulta: 21 de septiembre de 2017].
- Information and Analysis Center for Positioning, Navigation and Timing, *GLONASS History,* [en línea]. Dirección URL: https://www.glonass-iac.ru/en/guide/index.php. [Fecha de consulta: 21 de septiembre de 2017].
- Infosec Institute, *Hacking Satellites … Look Up to the Sky,* [en línea]. Dirección URL: http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/#gref. [Fecha de consulta: 21 de septiembre de 2017].
- Instituto de Investigaciones Jurídicas UNAM, "Hugo Grocio, vida y obra", *Fundadores del Derecho Internacional*, [en línea], 41 pp. Dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/1/383/7.pdf. [Fecha de consulta: 5 de julio de 2017].

- Internet Society, *¿Quiénes somos?,* [en línea]. Dirección URL: https://www.internetsociety.org/es/%C2%BFqui%C3%A9nes-somos-0. [Fecha de consulta: 19 de mayo de 2017.]
- La Web del programador, *Intranet*, Diccionario informático, [en línea]. Dirección URL: http://www.lawebdelprogramador.com/diccionario/buscar.php?opc=1&charSearch=intranet. [Fecha de consulta: 30 de mayo de 2017].
- Lanza, Lucas; Fidel, Natalia, *Política 2.0 y la comunicación en tiempos modernos*, [en línea], Centro de Estudios en Diseño y Comunicación, 2011, 11 pp. Dirección URL: http://www.scielo.org.ar/pdf/ccedce/n35/n35a06.pdf. [Fecha de consulta: 4 de julio de 2017].
- Livingstone, David; Lewis, Patricia, *Space, the Final Frontier for Cybersecurity?,* [en línea], Chatham House, The Royal Institute of International Affairs, September 2016, 46 pp. Dirección URL: https://www.chathamhouse.org/publication/space-final-frontier-cybersecurity. [Fecha de consulta: 30 de septiembre de 2017].
- Los Angeles Air Force Base, *Air Force accepts delivery of GPS Next Generation Operational Control System,* [en línea]. Dirección URL: http://www.losangeles.af.mil/News/Article-Display/Article/1361778/air-force-accepts-delivery-of-gps-next-generation-operational-control-system/. [Fecha de consulta: 5 de noviembre de 2017].
- Meridian 2016, *El Proceso Meridian,* [en línea]. Dirección URL: https://www.meridian2016.mx/spanish/Paginas/inicio.aspx. [Fecha de consulta 2 de julio de 2017].
- NASA, *Explorer 1: Overview,* [en línea]. Dirección URL: https://www.nasa.gov/mission_pages/explorer/explorer-overview.html. [Fecha de consulta: 29 de agosto de 2017].
- NASA, *National Space Policy of the United States of America,* [en línea], 18 pp. Dirección URL: https://www.nasa.gov/sites/default/files/national_space_policy_6-28-10.pdf. [Fecha de consulta: 17 de septiembre 2017].
- NASA, *The Global Differential GPS System,* [en línea]. Dirección URL: http://www.gdgps.net/. [Fecha de consulta: 17 de septiembre de 2017].
- National Academy of Sciences, *The Global Positioning System,* [en línea], Beyond Discovery. The Path from Research to Human Benefit, 1997, 8 pp. Dirección URL: http://www.nasonline.org/publications/beyond-discovery/the-global-positioning-system.pdf. [Fecha de consulta: 13 de agosto de 2017].
- National Geodetic Survey, *Continuously Operating Reference Station (CORS),* [en línea]. Dirección URL: https://www.ngs.noaa.gov/CORS/. [Fecha de consulta: 14 de septiembre de 2017].
- National Security Strategy Archive, *A National Security Strategy of Engagement and Enlargement,* [en línea], 1994. Dirección URL: http://nssarchive.us/national-security-strategy-1994/. [Fecha de consulta: 12 de julio de 2017].
- National Security Strategy Archive, *A National Security Strategy for a New Century,* [en línea], 1998. Dirección URL: http://nssarchive.us/NSSR/1998.pdf. [Fecha de consulta: 13 de julio de 2017].
- National Security Strategy Archive, *National Security Strategy 2015,* [en línea]. Dirección URL: http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf. [Fecha de consulta: 18 de julio de 2017].
- National Security Strategy Archive, Reports, [en línea]. Dirección URL: http://nssarchive.us/. [Fecha de consulta: 11 de julio de 2017].

- National Security Strategy Archive, *The National Security Strategy of the United States,* [en línea], 2002. Dirección URL: http://nssarchive.us/national-security-strategy-2002/. [Fecha de consulta: 15 de julio de 2017].
- NATO Cooperative Cyber Defense Centre of Excellence, *Cyber Security Strategy Documents,* [en línea]. Dirección URL: https://ccdcoe.org/cyber-security-strategy-documents.html. [Fecha de consulta: 18 de julio de 2017].
- New York Times, *Flexing Muscle, China Destroys Satellite in Test*, [en línea], 19 de Enero de 2007. Dirección URL: http://www.nytimes.com/2007/01/19/world/asia/19china.html?ex=1326862800&en=74a017e997a72c53&ei=5088&partner=rssnyt&emc=rss. [Fecha de consulta: 10 de octubre de 2017].
- Norse, *Norse Attack Map,* [en línea]. Dirección URL: http://map.norsecorp.com/#/
- Norse, *Who we are,* [en línea]. Dirección URL: http://www.norse-corp.com/about-us/who-we-are/. [Fecha de consulta: 22 de mayo de 2017].
- NSA Archive, *National Military Strategy for Cyberspace Operations*, [en línea], 2006. Dirección URL: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf. [Fecha de consulta: 16 de julio de 2017].
- Office of the Director of National Intelligence, *Who We Are,* [en línea]. Dirección URL: https://www.dni.gov/index.php/who-we-are/history. [Fecha de consulta: 16 de julio de 2017].
- Office of the Federal Register, *Improving Critical Infrastructure Cybersecurity,* [en línea], Executive Order 13636. Dirección URL: https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity. [Fecha de consulta: 20 de julio de 2017].
- Organización de las Naciones Unidas, *El fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional*, 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 2015. Dirección URL: https://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf. [Fecha de consulta: 20 de octubre de 2017].
- Panda Security, *Ransomware*, [en línea]. Dirección URL: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/. [Fecha de consulta: 20 de junio de 2017.]
- Pilotnaval, *Navegación III,* [en línea]. Dirección URL: http://pilotnaval.blogspot.mx/2013/09/caracteristicas-de-los-radares-marinos.html. [Fecha de consulta: 30 de agosto de 2017].
- Política y otras cosas, *¿Cómo se engaña a un GPS?,* [en línea]. Dirección URL: https://mrjaen.com/2017/05/21/como-se-engana-a-un-gps/. [Fecha de consulta: 30 de agosto de 2017].
- PYME, *Cronología de Internet,* [en línea]. Dirección URL: http://pyme.net.uy/documentos/cronologia_internet.htm. [Fecha de consulta: 19 de mayo de 2017.]
- Rayón, Ballesteros María Concepción; Gómez, Hernández José Antonio, *Cibercrimen: particularidades en su investigación y enjuiciamiento*, 26 pp. [en línea]. Dirección URL: https://dialnet.unirioja.es/descarga/articulo/4639646.pdf.

[Fecha de consulta: 3 de noviembre de 2017].

- Reagan Library, *Statement by Deputy Press Secretary Speakes on the Soviet Attack on a Korean Civilian Airliner,* [en línea]. Dirección URL: https://reaganlibrary.archives.gov/archives/speeches/1983/91683c.htm. [Fecha de consulta: 8 de septiembre de 2017].
- Real Academia Española, *Ciberespacio,* [en línea]. Dirección URL: http://dle.rae.es/?id=98Wdd57. [Fecha de consulta: 28 de noviembre de 2016].
- Real Academia Española, *Diccionario: seguridad,* [en línea]. Dirección URL: http://dle.rae.es/?id=XTrIaQd. [Fecha de consulta: 28 de marzo de 2017].
- Real Academia Española, *Diccionario: seguro,* [en línea]. Dirección URL: http://dle.rae.es/?id=XTrgHXd. [Fecha de consulta: 28 de marzo de 2017].
- Resilient Navigation and Timing Foundation, *Cybersecurity,* [en línea]. Dirección URL: https://rntfnd.org/cybersecurity/. [Fecha de consulta: 1° de octubre de 2017].
- Reynaud, Mélodie, *Cyber Security for Satellite Systems,* [en línea], Observatoire-FIC. Dirección URL: https://www.observatoire-fic.com/cyber-security-for-satellite-systems-by-secgate/. [Fecha de consulta: 30 de agosto de 2017].
- Schmitt, Michael N. (General editor), *Tallin Manual on the International Law applicable to Cyber Warfare,* [en línea], Cambridge University Press, 2013, 282 pp. Dirección URL: http://www.cambridge.org/es/academic/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB&isbn=9781107177222#iosDIuJbXbJFyABP.97. [Fecha de consulta: 27 de enero de 2018].
- Schreier, Fred, *On Cyberwarfare,* [en línea], DCAF Horizon, 2015, 133 pp. Dirección URL: http://www.dcaf.ch/Publications/On-Cyberwarfare. [Fecha de consulta: 23 de mayo de 2017].
- Schriever Air Force Base, *50 SW completes GPS constellation expansion,* [en línea]. Dirección URL: http://www.schriever.af.mil/News/Article-Display/Article/277054/50-sw-completes-gps-constellation-expansion/. [Fecha de consulta: 6 de septiembre de 2017].
- Significados, *Telemetría,* [en línea]. Dirección URL: https://www.significados.com/telemetria/. [Fecha de consulta: 30 de agosto de 2017].
- Sistemas de Gestión de Seguridad de la Información, *¿Qué significa la Seguridad de la Información?,* [en línea]. Dirección URL: http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/. [Fecha de consulta: 17 de mayo de 2017].
- TechTarget, *Backbone*, [en línea]. Dirección URL: http://searchdatacenter.techtarget.com/es/definicion/Backbone. [Fecha de consulta: 30 de agosto de 2017].
- The Australian, *Tamil Tigers 'hijack' satellite,* [en línea]. Dirección URL: http://www.theaustralian.com.au/australian-it-old/tamil-tigers-hijack-satellite/news-story/9185f387b78dbcc208f9f085ecbf195a. [Fecha de consulta: 16 de septiembre de 2017].
- The Hill, *Cyber protection a priority for GPS*, [en línea]. Dirección URL:http://thehill.com/blogs/congress-blog/technology/261982-cyber-protection-a-

priority-for-gps. [Fecha de consulta: 10 de diciembre de 2017].
- The National Counterproliferation Center, *Who We Are,* [en línea]. Dirección URL: https://www.dni.gov/index.php/ncpc-who-we-are. [Fecha de consulta: 16 de julio de 2017].
- The National Counterterrorism Center, *History,* [en línea]. Dirección URL: https://www.dni.gov/index.php/nctc-who-we-are/history. [Fecha de consulta: 16 de julio de 2017].
- The White House, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* [en línea]. Dirección URL: https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal. [Fecha de consulta: 21 de julio de 2017].
- The White House, *Presidential Policy Directive--Critical Infrastructure Security and Resilience,* [en línea], 2013. Dirección URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. [Fecha de consulta 20 de julio de 2017].
- Truman Center, *GPS, A WEAK LINK IN CYBERSECURITY?* [en línea]. Dirección URL: http://trumancenter.org/doctrine-blog/gps-a-weak-link-in-cybersecurity/. [Fecha de consulta 20 de julio de 2017].
- U.S. Department of Transportation, *Nationwide Differential Global Positioning System Program Fact Sheet,* [en línea]. Dirección URL: https://www.fhwa.dot.gov/publications/research/operations/02072/index.cfm. [Fecha de consulta: 14 de septiembre de 2017].
- U.S. Strategic Command, *U.S. Cyber Command (USCYBERCOM),* [en línea]. Dirección URL: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/. [Fecha de consulta: 17 de julio de 2017].
- UIT, *Agenda sobre Ciberseguridad Global.* Dirección URL: http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html. [Fecha de consulta 20 de julio de 2017].
- UIT, *Ciberseguridad-Grupo de Expertos,* [en línea]. Dirección URL: http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=06&ipage=05&ext=html. [Fecha de consulta: 21 de mayo de 2017].
- UIT, *La Agenda sobre Ciberseguridad Global,* [en línea]. Dirección URL: http://www.itu.int/itunews/manager/display.asp?lang=es&year=2008&issue=09&ipage=18&ext=html. [Fecha de consulta: 17 de mayo de 2017].
- UIT, Rec. UIT-T X.1205. Sector de Normalización de las Telecomunicaciones de la UIT (04/2008). Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad*. Seguridad en el ciberespacio – Ciberseguridad. Aspectos generales de la ciberseguridad.* (04/2008) *[en línea]*. Dirección URL: http://www.itu.int/es/Pages/default.aspx. [Fecha de consulta: 14 de agosto de 2016].
- United Nations Office for Outer Space Affairs, *International Committee on Global Navigation Satellite Systems (ICG),* [en línea]. Dirección URL:

http://www.unoosa.org/oosa/en/ourwork/icg/icg.html. [Fecha de consulta: 18 de septiembre de 2017].

- Universidad de Granada, *Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario,* Grupo de Estudios en Seguridad Internacional, Marzo 2015, [en línea]. Dirección URL: http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario. [Fecha de consulta: 17 de mayo de 2017].
- Universidad Nacional de San Juan, *Concepto de Sociedad de la Información*, [en línea]. Dirección URL: http://www.unsj.edu.ar/unsjVirtual/comunicacion/seminarionuevastecnologias/wp-content/uploads/2015/05/concepto.pdf. [Fecha de consulta: 20 de mayo de 2017.]
- US-CERT, *About Us,* [en línea]. Dirección URL:https://www.us-cert.gov/about-us. [Fecha de consulta: 16 de julio de 2017].
- US-CERT, *The National Strategy to Secure Cyberspace,* [en línea], 2003. Dirección URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. [Fecha de consulta: 17 de julio de 2017].
- USCode, *10 USC 2281: Global Positioning System,* [en línea]. Dirección URL: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section2281&num=0&edition=prelim. [Fecha de consulta: 12 de septiembre de 2017].
- USCode, *49 USC 301: Leadership, consultation, and cooperation,* [en línea]. Dirección URL: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title49-section301&num=0&edition=prelim. [Fecha de consulta: 12 de septiembre de 2017].
- USCode, *51 USC 50112: Promotion of United States Global Positioning System standards,* [en línea]. Dirección URL: http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title51-section50112&num=0&edition=prelim. [Fecha de consulta: 12 de septiembre de 2017].
- Volpe Center, *GPS Dependencies in the Transportation Sector: An Inventory of Global Positioning System Dependencies in the Transportation Sector, Best Practices for Improved Robustness of GPS Devices, and Potential Alternative Solutions for Positioning, Navigation, and Timing,* [en línea], August 2016, p.6. Dirección URL: https://ntl.bts.gov/lib/60000/60400/60433/DOT_VNTSC_NOAA_16_01.pdf.
- W. Sturdevant, Rick; Anderson, Haithe, *Space Effects in Operation Iraqi Freedom,* [en línea]. Dirección URL: http://www.spacebusiness.com/sample2.pdf. [Fecha de consulta: 18 de octubre de 2017].
- White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World,* [en línea], 2011, 30 pp. Dirección URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. [Fecha de consulta: 18 de julio de 2017].

- White House, *U.S. GLOBAL POSITIONING SYSTEM POLICY,* [en línea]. Dirección URL: https://clintonwhitehouse3.archives.gov/WH/EOP/OSTP/NSTC/html/pdd6.html. [Fecha de consulta: 8 de septiembre de 2017].
- World Economic Forum, *The Global Risks Report 2017,* 12th Edition, [en línea]. Dirección URL: https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/The%20Global%20R isks%20Report%202017-01-2017.pdf. [Fecha de consulta: 22 de mayo de 2017].