UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

CENTRO DE RELACIONES INTERNACIONALES

LA CIBERGUERRA EN LA POLÍTICA DE SEGURIDAD Y DEFENSA DE ESTADOS UNIDOS DE AMÉRICA

T E S I S

PARA OBTENER EL TÍTULO DE LICENCIADO EN RELACIONES INTERNACIONALES

P R E S E N T A

STEPHANIE MÓNICA NÚÑEZ ZEPEDA

ASESOR

DR. JESÚS GALLEGOS OLVERA

CIUDAD UNIVERSITARIA, CDMX, 2016

Índice

Índice de gráficos

(tablas, mapas, gráficas e imágenes)

Pág.

INTRODUCCIÓN

La amplitud de riesgos y amenazas en el siglo XXI se ha convertido ya en una de las prioridades de los Estados-nación, dicha amplitud ha intensificado la protección de las fronteras físicas y virtuales, así como de la integridad de la población a través de la creación de nuevas estrategias para la defensa de la seguridad nacional.

Hoy en día, la capacidad de afectar a un Estado se ha incrementado con el uso de las nuevas Tecnologías de la Información y Comunicación, uno de ellos es la del ciberespacio cuyas amenazas suponen la vulnerabilidad informática de las sociedades civiles y sus infraestructuras de seguridad.

El ciberespacio es un medio de fácil acceso donde cualquier persona guardando su anonimato puede llegar a delinquir generando grandes daños: por ende, éste representa una esfera de alta vulnerabilidad debido a que el Estado deposita en su estructura cibernética información confidencial y un gran andamiaje de sus instituciones económicas, políticas, financieras, militares y sociales.

La digitalización de datos y de redes que conectan los modernos sistemas de información y comunicación (Big Data) se están convirtiendo en los principios rectores del funcionamiento de la sociedad actual.[1] Cada día millones de usuarios acceden de manera legítima a datos de cualquier parte del mundo por medio de redes internas o de servicios que ofrece el internet.[2] Sin embargo, también crece el número de accesos no autorizados que se sirven de canales de servicios de internet para infligir daños a los sistemas de información, dichos sujetos son nombrados "hackers" o intrusos informáticos.

A los ataques malintencionados perpetrados a través de cauces electrónicos contra las bases de datos, el funcionamiento (o el mal uso) de una red informática esencial

[1] Wegener Henning, "La guerra cibernética" [en línea], *Política Exterior*, Vol. 15, No. 80 (Mar. - Apr., 001), pp. 131-142, 145-149, Publicado por: Estudios de Política Exterior S. A, Dirección URL: http://bit.ly/1LMiOgi.
[2] Ese tipo de servicios pueden ser: Word wide web, e-mail, telnet, ftp, IRC, usenet NEWS

para así dañar la infraestructura crítica de un Estado, se les denomina "ciberguerra"[3], y puede ser originado por un Estado, individuo u organización anónima. Un ataque enmascarado por una o varias estaciones no sólo dificulta las medidas de defensa y la identificación del agresor, sino que, además puede hacer imposible la identificación geográfica del agresor.[4] Por lo tanto, las medidas de protección y defensa del sistema agredido podrían emplearse contra inocentes, además, de que no existe un marco jurídico que sancione los delitos en el ciberespacio.[5]

Dichas medidas se engloban en el término de ciberseguridad la cual es la protección de la infraestructura crítica a través de contrarrestar las amenazas y riesgos informáticos, el desarrollo de la tecnología avanzada, así como el desarrollo de leyes informáticas, la investigación de delitos cibernéticos, y la apertura y salvaguarda de Internet.[6]

El intruso informático puede acceder y emplear información privada referida a determinado grupo al que no pertenece, puede manipular archivos introduciendo datos propios o alterando los existentes, o bien, reprogramar sistemas de información que controlan importantes procesos mediante la introducción de comando falsos y destruir la integridad del sistema, o modificando servicios que proporciona la internet para que sistemas enteros dejen de funcionar.

Tal es el caso de la infiltración de información de hasta cuatro millones de empleados federales de Estados Unidos por parte de piratas informáticos chinos, en 2015, un ciberataque considerado como el mayor robo de información estatal.[7] Otro es el ataque a las redes sociales Facebook y Twitter de las compañías Newsweek y Delta, por parte del grupo de piratería informático yihadista

---

[3] Prabir Purkayastha, ¡Haz la ciberpaz y no la ciberguerra! [en línea], Alaii, Disponible en: http://bit.ly/1LMiOgi.

[4] Wegener Henning, *óp. cit.*, pp. 131-142, 145-149.

[5] Trejo Delarbre, Raul, Derecho, delitos y Libertades en internet [en línea], Disponible en: http://bit.ly/1X2W27n.

[6] Elaboración propia.

[7] "Un ataque saca a la luz los datos de 4 millones de funcionarios en EEUU" [en línea], El *Confidencial,* Disponible en: http://bit.ly/2c2XKV6.

autodenominado “El cibercalifato Estado Islámico”.[8] Así como los ataques que reciben más de la mitad de las bolsas de valores del mundo con el fin de sustraer dinero o datos de clientes y usuarios.[9]

Las redes existentes que comunican, organizan, califican y almacenan información secreta; las que controlan plantas nucleares, sistemas de agua y energía, etc., de países de todo el mundo se encuentran vulnerables ante los peligros cibernéticos. El desarrollo de las redes supone un traspaso de poder hacia agentes no estatales de diversa índole, capaces de organizarse en redes formadas por múltiples organizaciones con mayor rapidez que los actores estatales, tradicionales y jerárquicos.[10]

Los ataques a las infraestructuras críticas de seguridad nacionales e internacionales van desde la simple lectura (acceso a información estratégico-militar), a la introducción de datos erróneos en los sistemas del rival, la manipulación de sistemas de control de armamento, la inutilización de sistemas de radar y detección vía satélite, y el colapso de redes informáticos, especialmente las relacionadas con centros de mando.

Más de un centenar de gobiernos se están preparando para librar batallas en el dominio en línea. Por otra parte, los problemas pueden ser conceptualizados a través de los temas políticos difíciles que estas "cosas" ya ha producido: escándalos como WikiLeaks y NSA monitoreo, nuevas armas cibernéticas como Stuxnet, y el papel que las redes sociales desempeña en todo, desde las revoluciones de la Primavera Árabe a su propio las preocupaciones sobre la privacidad personal.[11]

Una vez que la ciberguerra empezó a tener auge, altos funcionarios políticos estadounidenses y europeos, tales como los secretarios de la seguridad y defensa nacional, también líderes de gobierno de la Organización del Atlántico Norte (OTAN)

---

[8] “Newaweek y Delta sufren ciberataques en las redes sociales” [en línea], Doctor Shoper, Disponible en: http://bit.ly/2bQnPYL.

[9] Hernández Enrique, “Sufren ciberataques más del 53% por ciento” [en línea], *Forbes,* junio de 2016, Disponible en: http://bit.ly/1O6sSmw.

[10] S/ autor, *Ciberdefensa-Ciberseguridad: Riesgos y Amenazas* [en línea], CARI, noviembre 2013, disponible en: http://bit.ly/1N3cj97.

[11] S/ autor, Cybersecurity and cyberwar [en línea], Disponible en: http://bit.ly/1LEbbpl.

y de la Unión Europea (UE), así como investigadores, ejército, y empresas de seguridad privadas principalmente, comenzaron a mostrarse interesados por el concepto, se percataron de que estas tendencias conflictivas aumentaban la importancia de la comunicación y la coordinación intergubernamental en todos los asuntos, desde el intercambio de información de los servicios de inteligencia hasta las operaciones tácticas las cuales refieren a la ciberdefensa.[12]

Las operaciones que se encargan de calibrar los aspectos de un posible ataque contra la información y las funciones informativas de un rival, además de garantizar su información son denominadas "ciberdefensa", la cual está adquiriendo relevante importancia en la política de seguridad de las naciones y de las organizaciones internacionales especializadas en la materia como la Organización del Tratado del Atlántico del Norte (OTAN) a través del "'Acuerdo Técnico de colaboración' para fomentar el intercambio de información y buenas prácticas sobre procedimientos técnicos."[13]

Hoy en día, toda nuestra forma de vida, desde la comunicación, el comercio, los conflictos, entre otros depende fundamentalmente de Internet. Por lo tanto, las cuestiones de ciberseguridad que resultan un desafío literalmente en todo el mundo: políticos que luchan con todo contra la ciberdelincuencia, en favor de la libertad en línea; los generales que protegen a la nación de nuevas formas de ataque, mientras que la planificación de nuevas ciberguerras se van creando; los ejecutivos de negocios que buscan defender sus firmas de amenazas inimaginables, y que buscan hacer dinero fuera de ellos; abogados y expertos en ética que construyen nuevos marcos para bien y el mal.

Por encima de todo, las cuestiones de seguridad cibernética nos afectan como individuos. Nos enfrentamos a nuevas preguntas en todo, desde nuestros derechos y responsabilidades como ciudadanos tanto del mundo en línea y real, simplemente cómo protegernos de un nuevo tipo de peligro. Sin embargo, aun cuando existen

---

[12] Arquilla, John; David Ronfeldt, *Redes y guerras en red: El futuro del terrorismo, el crimen organizado y el activismo político*, Alianza Editorial, 2003, p. 34.

[13] "La OTAN y la UE aumentan la cooperación en ciberseguridad" [en línea], *Departamento de Seguridad del Gobierno de España,* Disponible en: http://bit.ly/2c33nTn.

casos que han cobrado relevancia de manera importante y que afecta a tantos, permanecen tan poco conocidos.[14]

Es por eso que es pertinente cuestionar la fortaleza y vulnerabilidad de Estados Unidos de América (EUA) en la ciberguerra, es decir, ¿cómo implementa este país la ciberguerra en la política de seguridad y defensa?, el cual se encuentra inmerso en un contexto inestable no sólo en el aspecto ideológico sino en materia de militar, política y económica.

Las aportaciones de esta investigación permitirán identificar las principales naciones que junto a EUA encabezaran escenarios de guerra y conflicto, ya sea en la esfera tecnológica, la militar, la económica o la ciberespacial.

La hipótesis consiste en que los EUA constituye un eje fundamental en el estudio de las Relaciones Internacionales ya que a través de la teoría y la praxis ha liderado los grandes debates y la agenda de la comunidad internacional. En el caso del ciberespacio, no será la excepción debido a que su desarrollo tecnológico lo ha convertido en un actor de primer nivel en el escenario mundial. Esta condición le ofrece una oportunidad y una amenaza. Por lo tanto, la pertinencia del estudio de la ciberguerra en la política de seguridad y defensa de EUA, conduce al análisis y a la reflexión de la creación de nuevas estrategias de seguridad en el que se desarrollará una nueva era en materia de combate y guerra, así como del avance tecnológico y militar.

El dominio de los actores en el ciberespacio pone a prueba la fortaleza y estructura de los Estados más fuertes, en este caso de EUA. Los actores ciberespaciales lo vuelven cada vez más vulnerable dado el descontrol que posee en el ciberespacio aunado a los posibles ataques a su gobierno. Son los actores ciberespaciales, estatales, empresariales, tecnológicos e individuales los que dinamizan la evolución tecnológica para que EUA refuerce sus capacidades de defensa y seguridad.

Con esta investigación se incorporan nuevas tendencias y conceptos en el estudio de la disciplina de las relaciones internacionales para así enriquecer el

[14] Cybersecurity and cyberwar [en línea], Disponible en: http://bit.ly/1LEbbpl.

entendimiento del comportamiento actual de las relaciones entre los Estados. El surgimiento de la actividad ciberespacial, específicamente con la ciberguerra, complementa y diversifica el estudio de la seguridad nacional con una nueva área que permitirá reflexionar, discutir y analizar los nuevos retos de la comunidad internacional ya que muchos gobiernos son los que están preocupados por actualizar sus agendas de seguridad respecto al espacio virtual para protegerse de amenazas y ataques.

El objetivo de la presente investigación se centra principalmente en analizar la estrategia de defensa y seguridad de EUA ante los ataques de diversos actores en el ciberespacio; por ello, el presente trabajo de investigación ha sido organizado en 3 capítulos y sus conclusiones como se indica:

En el Capítulo 1, a partir del enfoque teórico del Neorrealismo se exponen las aproximaciones conceptuales a la ciberseguridad, se hace una descripción de la dinámica ciberespacial: estructura, funcionamiento y organización; la ciberguerra en el mundo virtual; se cita la diferencia de la operación entre ciberestrategia y ciberdefensa; y, se clasifica las principales amenazas informáticas y su campo de acción en el ciberespacio.

En el Capítulo 2, se analiza la agenda de seguridad nacional estadounidense y su definición de ciberguerra, identificando las principales fortalezas de seguridad nacional en el ámbito de la ciberguerra; así como de sus capacidades.

En el Capítulo 3, se enfoca en profundizar el estudio del comportamiento estadounidense en el ciberespacio en el contexto de ciberguerra; la planeación de su defensa ante la ciberguerra; y la ciberdefensa para establecer las principales acciones a favor de la protección y seguridad nacional; por último, se concluye este trabajo de investigación con los puntos más importantes que a juicio de la autora reflejan el contenido de la investigación.

Capítulo I Aproximaciones históricas y conceptuales a la ciberserguridad

La trascendencia del concepto de *seguridad* en el marco de las relaciones internaciones, va más allá de lo delimitado por un Estado respecto a sus fronteras.

Hoy en día, el concepto de seguridad se escucha por doquier debido al reconocimiento pleno de otras amenazas a las tradicionales como las guerras que pueden dañar al Estado a largo plazo, o bien, que pueden poner en riesgo su existencia. Ahora dichas amenazas abarcan temas como el cambio climático, la pobreza, la crisis energética, la crisis económica, y otros más novedosos como los peligros y amenazas en el espacio cibernético; éste último ha cobrado importancia debido a los avances tecnológicos y a las necesidades del mundo actual. A partir de lo anterior, en el presente capítulo se identificarán y estudiarán los conceptos de seguridad y amenaza; así como el ciberespacio, su dinámica, estructura y funcionamiento, para comprender la relación e importancia que existe entre esos tres conceptos.

1.1Seguridad: multidimensional, tradicional y humana

La seguridad en su acepción más general es el bien más preciado de los seres humanos.[15] En consecuencia, la libertad está implícita en la seguridad. El concepto de seguridad va desde lo individual hasta lo internacional pasando por cada uno de los niveles de organización gubernamental.

[15]Blin Arnaud y Gustavo Marín (Ed.), "Seguridad", *Diccionario del poder mundial,* Foro por una Nueva Gobernanza Mundial, París, Francia, 2013, p. 277.

Tradicionalmente, la seguridad se ha concebido a partir del enfoque político-militar centrado en la viabilidad y el resguardo (supervivencia) del Estado.[16] Dicho en otras palabras, desde esta visión la seguridad prevalece únicamente en el Estado y sus amenazas son de carácter militar las cuales son provenientes de otros Estados.

En contraste con Barry Buzan perteneciente a la corriente neorrelista, la seguridad consiste en la habilidad de los Estados y las sociedades de mantener su identidad independiente y su integridad funcional;[17] donde la seguridad tiene un impacto en la toma de decisiones, es decir, la invocación a la seguridad ha servido para legitimar el uso de la fuerza, el establecimiento de una condición de emergencia y de despliegue de todas las capacidades para hacer frente a dicha amenaza.[18]

Otra idea es la de Walter Lippmann quien partiendo de la dualidad Estado-nación dice que una nación es segura en la medida en que no está en peligro de tener que sacrificar los valores fundamentales si se quiere evitar la guerra, y es capaz, en caso de desafío, para mantenerlos por la victoria en caso de guerra.[19]

Mientras que Richard Ullman divide amenaza-seguridad, y parte de que una amenaza para la seguridad nacional es una acción o secuencia de eventos que atenta de manera drástica y durante un periodo relativamente breve de espacio y tiempo para degradar la calidad de vida de los habitantes de un Estado, o desafia de manera significativa a reducir la gama de opciones de política a disposición del

[16]Chanona Alejandro, "El debate teórico sobre la construcción de las comunidades de seguridad", en *La comunidad de seguridad en América del Norte, una perspectiva comparada con la Unión Europea,* México: Facultad de Ciencias Políticas y Sociales, UNAM, 2010, p. 12.

[17] Buzan Barry, "The national security problem in International Relations*",* p. 22, en *People States and Fear: An agenda for international security studies in the Post-Cold War Era,* London: Harvester, Wheatsheaf, 1991, pp 1-34.

[18]*Ibíd*. p. 12.

[19] Cited and Arnold Wolfers, *Discord and Collanoration,* Baltimore: John Hopkins University Press, 1962, p. 150, en Buzan Barry, *The national security problem in International Relations,* p. 20.

gobierno de un Estado o de entidades gubernamentales, no privadas dentro del Estado.[20]

De esta manera, Ullman parte de la amenaza para definir a la seguridad, es decir, cambia la concepción de seguridad y definición de amenaza de acuerdo al nivel de peligrosidad que afecta no sólo a la toma de decisiones de los dirigentes de un Estado sino también a sus habitantes, incluyendo el sector empresarial público y privado. Lo mismo que Buzan al incluir a la sociedad y al Estado en lucha por mantener su integridad.

Mientras que Lippmann hace mención del no sacrificio de los valores fundamentales o nacionales para mantener la seguridad, Buzan y Ullman refieren a la toma de decisiones, a saber, en los tres autores existe una variable dependiente: la capacidad del Estado junto con sus instituciones para defensa del mismo y su sociedad. Entonces, la seguridad es la condición generada después de la respuesta del Estado (toma de decisiones) frente a las amenazas y riegos que desafían la integridad y viabilidad del Estado-nación.

Por lo tanto, para llegar a obtenerla se tienen que buscar los medios adecuados que no irrumpan otras esferas de la seguridad. Es importante identificar y saber que ésta se diversifica para cubrir todas las áreas donde el ser humano se encuentra indefenso, por ejemplo, la económica, jurídica, política, social, o la seguridad humana, entre otras.

Con el fin de la Guerra Fría el Sistema Internacional comenzó a identificar nuevas amenazas debido a que las formas de conflictos habían cambiado. La carrera armamentista que emprendieron las naciones protagonistas -Estados Unidos y la Unión de Repúblicas Socialistas Soviéticas-, forjaron la innovación y consecuente creación de armas de guerra más eficientes y peligrosas como misiles balísticos, así como la destacada nave espacial Sputnik[21], con la cual el gobierno

[20]Richad H. Ullman 'Redefining security', *International Security,* 1983, note 32, p. 133 en Buzan Barry, *The national security problem in International Relations,* p. 20 en *People States and Fear: An agenda for international security studies in the Post-Cold War Era,* London: Harvester, Wheatsheaf, 1991, pp 1-34.

[21] "L'Agenzia A.R.P.A."[en línea], *Le origini di Internet,* Disponible en: http://bit.ly/1LOA7sz.

estadounidense se mostraba tecnológicamente obsoleto. En otras palabras, el desarrollo de tecnología de guerra incitó a que ambas naciones lucharan por liderar la supremacía mundial. En su defecto, con la herencia de Guerra Fría, y la entrada del siglo XXI y el inicio de la globalización aparecieron conflictos los de carácter étnico, civil, de competencia económica, migración, pobreza y hambruna, entre otros, que representaban nuevos desafíos.[22] Así, la visión militar de la seguridad comenzó a ampliarse dando paso a una nueva categorización que fue ganando importancia: la seguridad multidimensional.

De la misma manera, a inicios del siglo XXI la "Conferencia de Naciones Unidas sobre Desarme y Desarrollo", afirmó que la seguridad contiene aspectos no sólo militares, sino también económicos, sociales, medioambientales y de derechos humanos.[23]De tal forma que la seguridad se vuelve múltiple: seguridad alimentaria, para no tener hambre; seguridad ecológica, para no ser asfixiado por la contaminación del aire o inundado por los tsunamis o la crecida de los ríos y los maremotos; seguridad de la vida, del cuerpo y de la mente, para no estar enfermos, etc.[24]

Para efectos del objetivo de la seguridad multidimensional el 28 de octubre de 2003, los países asistentes de la Conferencia Especial sobre Seguridad firman la "Declaración sobre Seguridad en las Américas"[25], destacando junto con la Declaración Bridgetown:

---

[22] *Ibíd*. p. 14

Según el diccionario Espasa Calpe, (2005) entiéndase como *desafío,* un reto, cosa difícil a la hay que enfrentarse. El verbo *desafiar* implica "afrontar o enfrentarse a un peligro o dificultad". Aquel objetivo o empeño difícil de llevar a cabo, y que constituye un estímulo y un desafío para quien lo afronta, obtenido en Raimundi, Maria Julia; Molina, Maria Fernanda, et. al., ¿Qué es un desafío? Estudio cualitativo de su significado subjetivo en adolescentes de Buenos Aires. *Rev. latinoam. cienc. soc. niñez juv,* [en línea], 2014, vol.12, n.2, pp. 521-534, Disponible en: http://bit.ly/1ShUd5O.

[23]*Ibíd*. p. 15

[24]*Idem.*

[25] La DSA fue resultado de la Conferencia Especial sobre Seguridad celebrada en México en 2003, la cual marcó el proceso de culminación de un proceso de reflexión acerca del panorama de seguridad de la región y fue también el punto de partida de una nueva etapa caracterizada por el arribo de un nuevo paradigma de la seguridad en el hemisferio, de alcance multidimensional; obtenido en *Misión permanente de México ante la OEA* [en línea], Disponible en: http://bit.ly/1PEav3f. Al igual que la Declaración Bridgetown aprobada en 2002 sostiene un enfoque multidimensional en la seguridad hemisférica reconociendo las "nuevas amenazas" a las de la seguridad tradicional.

> "(…) nuestra nueva concepción de la seguridad en el Hemisferio es de alcance multidimensional, incluye las amenazas tradicionales y las nuevas amenazas, preocupaciones y otros desafíos a la seguridad de los Estados del Hemisferio, incorpora las prioridades de cada Estado, contribuye a la consolidación de la paz, al desarrollo integral y a la justicia social, y se basa en valores democráticos, el respeto, la promoción y defensa de los derechos humanos, la solidaridad, la cooperación y el respeto a la soberanía nacional".[26]

Así, se destaca que la característica de la seguridad multidimensional es la amplitud de amenazas que incluye e identifica de diversa naturaleza e índole, además de riesgos y desafíos a la seguridad de los Estados y sus sociedades. Cabe destacar que la sociedad cobra importancia respecto a su independencia, integridad y funcionalidad, por lo tanto, la implementación de nuevas estrategias de protección resultan indispensables para hacer frente a dichas amenazas.

En esta consideración, así como los Estados y sus gobiernos, las personas se muestran vulnerables a *amenazas de carácter intersectoriales*. Dichas amenazas presentan diferencias en los diferentes niveles, tanto nacional como internacional diversificándose a través del tiempo. Es decir, resulta necesario ampliar y puntualizar la seguridad de las personas ante las adversidades que hoy en día se presentan, dando lugar a la *seguridad humana*.

La seguridad humana es ahora un concepto esencial en la toma de decisiones de los gobiernos, quienes se han visto en la necesidad de implementarlo no sólo a nivel local o estatal sino también a nivel global, como en el Documento Final de la Cumbre Mundial 2005 de Naciones Unidas (A/RES/60/1), titulado
'Seguridad humana', donde Jefes de Estado y de Gobierno subrayaron "el derecho de las personas a vivir en libertad y con dignidad, libres de la pobreza y la desesperación" y reconocieron que "todas las personas, en particular las que son vulnerables, tienen derecho a vivir libres del temor y la miseria, a disponer de iguales oportunidades para disfrutar de todos sus derechos y a desarrollar plenamente su potencial humano".[27]

---

[26] Toro Ibacahe, Lenisset, *El enfoque multidimensional de la seguridad hemisférica,* Estudios Latinoamericanos, N° 22, Año 1, Segundo semestre 2009, pp. 67-75.

[27] *Seguridad humana para todos* [en línea], Fondo Fiduciario de las Naciones Unidas para la Seguridad Humana, Disponible en: http://bit.ly/1F712BR.

De manera que, de acuerdo con el párrafo anterior, el nuevo elemento que se incorporan a la seguridad, específicamente, a la humana, son los Derechos Humanos como valor supremo donde el Estado debe ser garante de los mismos. Es decir, la seguridad humana se preocupa por el pleno desarrollo del ser humano, en su nivel más esencial y natural.

Por su parte Naciones Unidas dice que "[l]a seguridad humana es un marco normativo dinámico y práctico para hacer frente a las amenazas de carácter intersectorial y generalizado con que se enfrentan los gobiernos y las personas.

Dado que las amenazas a la seguridad humana presentan grandes diferencias en el plano nacional e internacional y a lo largo del tiempo, la aplicación del concepto de seguridad humana requiere una evaluación de las inseguridades humanas que sea amplia, centrada en las personas, específica para cada contexto y orientada a la prevención, (…)"[28] para conseguir establecer paz y orden en cualquier rubro en el que se encuentre afectado.

Es decir, dicha seguridad podría considerarse dentro de la seguridad nacional, como una especie de círculos concéntricos, en cuyo centro u origen prevalece la seguridad de las personas. Lo anterior fundado en la protección de las necesidades humanas, sin excluir que del máximo círculo también se protege el espacio, sea natural o artificial, imprescindible de igual forma para el humano. Este planteamiento ayuda a centrar la atención en las amenazas existentes y emergentes para la seguridad y el bienestar de las personas y las comunidades.

La seguridad humana desprendida de la seguridad multidimensional marca mayor énfasis e importancia en la administración de cada gobierno para atender y enfrentar efectivamente a los riesgos y amenazas a los que se enfrenta su sociedad, y partir de ellos para crear estrategias integrales que cubran holísticamente, de la integridad estatal a la individual. Y en conjunto, lograr la paz y seguridad mundial humana.

Asimismo, Naciones Unidas la destaca como un marco normativo que requiere de evaluación para la aplicación de normas en su beneficio. Así, un factor

[28] *El concepto de seguridad humana* [en línea], United Nations Trust for Human Security, Disponible en: http://bit.ly/1KivEkv.

a considerar en la seguridad humana es la variabilidad de las amenazas que atentan contra el pleno desarrollo humano en cualquiera de sus cambios o modificaciones, a saber, las amenazas llegan a cambiar o modificarse, puede sufrir una especie de evolución, que las vuelve más peligrosas y dañinas, según sea su tipología. Con "tipología" se refiere a la diversidad que de ellas existen, es decir, así como la seguridad se multidimensiona, por ende, las amenazas lo hacen de la misma manera. Hoy en día las amenazas se diferencian según la clasificación de los sectores a los que afectan, por ejemplo: el económico, el social, el medioambiental, el humano, entre otros; e incluso el daño puede ser intersectorial, como anteriormente se mencionó.

La libertad del ser humano se vuelve una prioridad de los gobiernos, y una obligación, garantizar los medios necesarios para que no sea privativo de la misma. En tanto, los gobiernos deben salvaguardar su bienestar y defenderlo de todo aquello que provoque una perturbación a su vida y desarrollo, ya sea en materia de salud, de medio ambiente, personal (libertad), de la comunidad (identidad), política (derechos humanos), alimentaria, económica, etc. Es por eso que la definición y securitización de las nuevas amenazas en una sociedad es un factor clave para la creación de medidas que ayuden a enfrentarlas y prevenirlas, es decir, advertir y proporcionar información a la sociedad de las mismas. Este proceso conlleva la modificación de los entornos en todos los niveles, según sea el tipo y grado de amenaza para rescatar y rehabilitar el daño ocasionado y/o persistente.

Para ello es importante que los Estados identifiquen cuáles son las principales amenazas para su sociedad y los entornos en el que se desenvuelven. Las nuevas megatendencias del riesgo del siglo XXI han marcado un gran parteaguas para la focalización de las mismas, a saber: Difusión del poder; Empoderamiento individual; Patrones demográficos; y Comida, agua y recursos energéticos.[29] De los cuales, para fines de este trabajo se destaca la difusión de poder con el surgimiento de actores de nuevas tecnologías.

[29] *Global Trends: 2030: Alternative Worlds* [en línea], National Intelligence Council, Estados Unidos de América, diciembre 2012, Disponible en: http://bit.ly/1CSdG5K.

El cada vez más influyente uso de las Tecnologías de la Información y de Comunicación a través de Internet ha despertado interés y llamado la atención de muchos países, empresas e industrias por conocer e identificar acerca de sus riegos y amenazas a los que están expuestos, es por ello que se han reunido expertos para homologar una percepción de riesgos y encontrar posibles soluciones.

Un ejemplo de ello, es el anual Informe Global de Riegos 2016[30], (Informe Global Risks) celebrado en Davos, Suiza, por el Foro Económico Mundial, con el tema central de "La Cuarta Revolución Industrial", en colaboración con los 750 miembros de la comunidad del FEM ponen en la mira al menos 29 riesgos globales separados para ambos impacto y probabilidad en un horizonte temporal de 10 años.

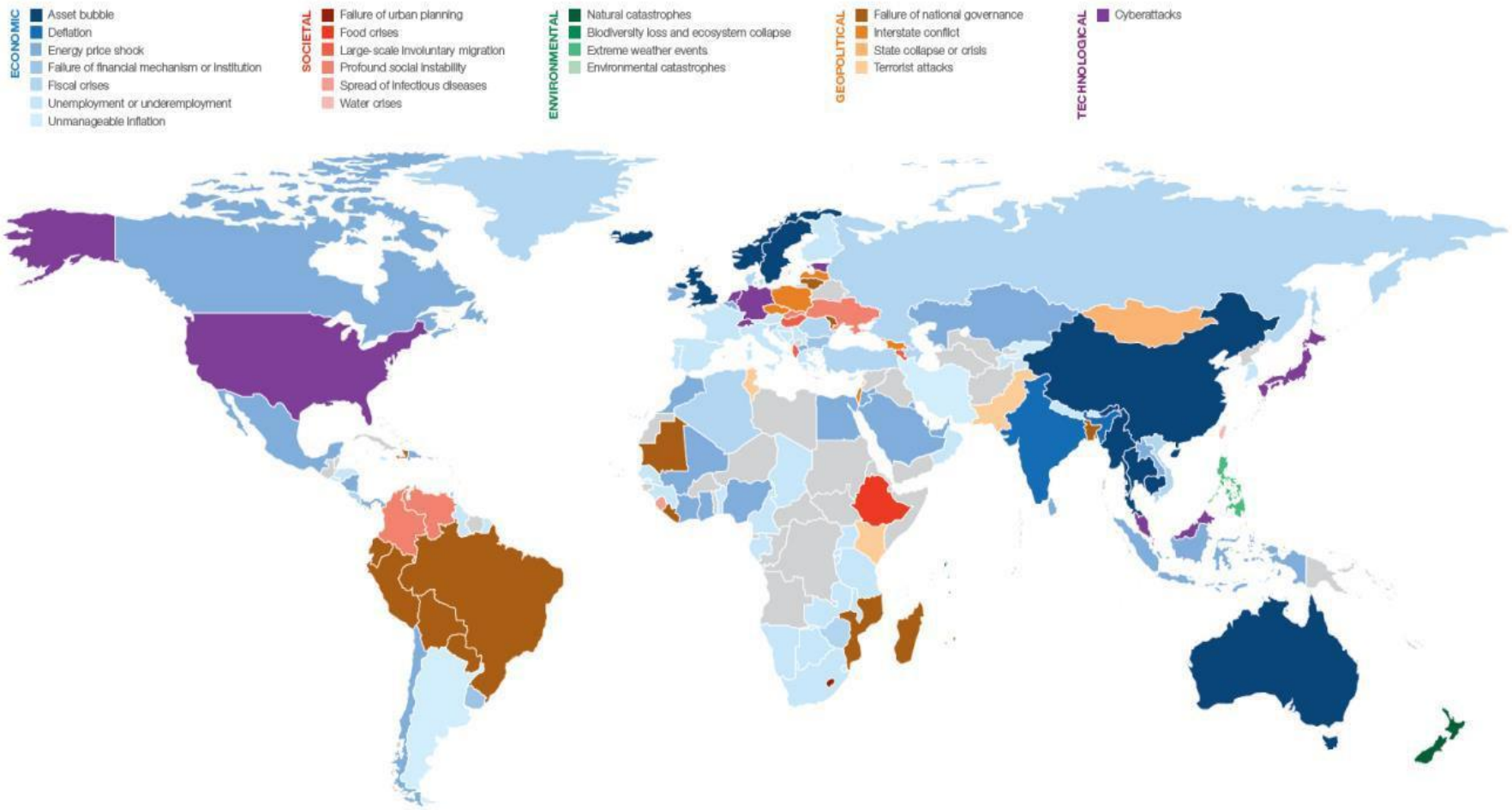
Entre los cuales durante los últimos tres años, el informe ha clasificado a los ataques cibernéticos entre sus principales riesgos tanto desde la perspectiva de probabilidad e impacto.[31] Asimismo, hace énfasis a los países más sobresalientes en materia tecnológica, principalmente para los Estados Unidos de América, quienes otorgan el primer lugar a dicha amenaza antes que los fenómenos meteorológicos extremos. El cual se puede ver en el siguiente mapa 1.1.

Éste es un problema que no sólo afecta a unos cuántos, debido a que el ataque puede llegar a cualquier parte del mundo sin importar el estatus económico, político o social del país, llegando a ocasionar graves perturbaciones. De acuerdo con el Informe los delitos en el ciberespacio cuesta a la economía mundial un estimado de 445 millones de dólares, superior a los ingresos de las economías.[32] Con lo que es importante reflexionar acerca de la escala y alcance potencial de futuros conflictos cibernéticos.

[30] *¿Cuáles son los principales riegos globales para 2016?* [en línea], World Economic Forum, Disponible en: http://bit.ly/1ZIW4RD.
[31] *Ibídem.*
[32] *Global Risks Repot 2016* [en línea], World Economic Forum, Disponible en: http://bit.ly/1RvWKZK.

Los riesgos globales de mayor preocupación para hacer negocios, por país, 2016

Mapa 1.1 Donde se muestra en color morado los países que se ven mamenazados por los riesgos tecnológicos.
Fuente: Foro Económico Mundial, Global Risks 2016, Disponible en: http://bit.ly/1RvWKZK.



Paisaje de la evolución de riesgos 2007-2016

Cuadro 1.2 Cuadro que muestra el paisaje de la evolución de riesgos de 2007 a 2016

Fuente: Foro Económico Mundial, Global Risks 2016, Disponible en: http://bit.ly/1RvWKZK.

De acuerdo con *Global Risks Report 2016,*

> "(l)os riesgos globales pueden no ser estrictamente comparables entre años, así como las definiciones y el conjunto de los riesgos globales que han evolucionado con las nuevas cuestiones emergentes en el horizonte de 10 años. Por ejemplo, los ataques cibernéticos, la disparidad de ingresos y el desempleo entraron en el conjunto de los riesgos globales en 2012. Algunos fueron reclasificadas riesgos globales: las crisis del agua y el aumento."

Empero, la ascendencia de los ataques cibernéticos se debe a la constante evolución tecnológica que ha tenido lugar, y junto con ello, la complejidad de riesgos.

Ante las amenazas y riesgos es necesario una evaluación por parte de cada gobierno afectado respecto a sus vulnerabilidades en la infraestructura crítica, además, podría tratarse de un nuevo desarrollo respecto a las doctrinas estratégicas para la gestión de conflictos, que van desde innovaciones en materia de seguridad y defensa.

Asimismo es fundamental establecer una definición de amenaza y diferenciarla de riesgo, a saber: la amenaza es una manifestación que formula un actor o actores, con el propósito de transmitir a otro u otros, la capacidad de producirle daños a sus bienes o intereses.[33]

Otra definición de amenaza es:

> "el impacto de aquellas tendencias y factores que podrían incidir negativamente sobre los intereses y objetivos nacionales de (…) [un país] y sobre las condiciones para el desarrollo social y económico de su población. Asimismo, (…) aquellos riesgos globales derivados de la transformación del panorama tecnológico, energético, demográfico y ambiental. Del mismo modo, (…) [aquellas] vulnerabilidades que pueden comprometer la estabilidad y el desarrollo de la nación."[34]

En consecuenica, la amenaza puede corresponder a un fenómeno de origen natural, socio-natural, tecnológico o antrópico en general, definido por su

[33]Parafraseando a Armending Gisela, *Una mirada hacia la Declaración de las Américas,* Centro Argentino de Estudios Internacionales, Programa Defensa y Seguridad, Disponible en: http://bit.ly/1PXNETW.

[34]*Programa de Seguridad Nacional 2014-2018* [en línea], SEGOB, Disponible en: http://bit.ly/1iDi3BK.

naturaleza, ubicación, recurrencia, probabilidad de ocurrencia, magnitud e intensidad (capacidad destructora).[35] Esto sin olvidar que existen otro tipo de amenazas que de la misma manera ponen en riesgo la seguridad de una nación.

Para efectos de seguridad nacional, es importante destacar que la amenaza está representada por aquellos elementos que en un contexto de incertidumbre atentan contra la estabilidad, viabilidad, desarrollo y existencia de un Estado en cualquiera de sus esferas de seguridad. Por lo tanto, la variabilidad de las amenazas definirá la implementación de políticas que prevengan y reduzcan riesgos.

Entonces, es importante que el Estado identifique y defina las principales amenazas que atenten contra su seguridad para implementar medidas que prevengan o reduzcan posibles daños. Y una vez expuestas las diferentes categorizaciones de definen a la seguridad ahora es posible que los Estados tengan un espectro más grande para su defensa.

Por su parte "el riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad." [36]

Mientras que las amenazas por sí solas, no representan un peligro, al juntarse con la vulnerabilidad, se convierten en un riesgo, el cual sí representa un peligro con probabilidad e impacto. [37] Es decir, la amenaza constituye un riesgo o perjuicio, peligro o daño, siempre y cuando hay vulnerabilidad sobre de algo o alguien. En el caso del ciberespacio, su vulnerabilidad se encuentra en su misma ingeniería, que a continuación se conocerá y detallará.

---

[35] Chardon, Anne-Catherine y Juan Leonardo González, "Amenaza, vulnerabilidad, riesgo, desastre, mitigación, prevención…", *Programa de información e indicadores de gestión de riesgos,* Banco Interamericano de Desarrollo, CEPAL, Universidad Nacional de Colombia, IDEA, Dic. 2012, p. 3.

[36] *Definición de Riesgo* [en línea], Centro Internacional para la Investigación del Fenómeno de El Niño, Disponible en: http://bit.ly/2awi7wG.

[37] *Idem.*

1.2 Ciberespacio e internet: estructura, funcionamiento, organización y gobernanza de las redes ciberespaciales.

Para dar lugar y entendimiento al espacio cibernético o ciberespacio es necesario conocer la creación de su infraestructura la cual hoy conocemos como *Internet.* Un primer acercamiento a Internet es establecer una definición, la cual consiste en un "conjunto de redes interconectadas a escala mundial con la particularidad de que cada una de ellas es independiente y autónoma."[38] Sin embargo, "es importante destacar que Internet no es una gigantesca red que interconecta ordenadores de todo el mundo. Debe considerarse Internet como una red mundial que interconecta redes locales, de manera que permite que éstas sean independientes y automáticas."[39]

A mediados del siglo XX la conformación de una red interconectada se vio casi ilusoria y obsoleta, empero, con la eventualidad de los conflictos entre Estados en el marco de la Guerra Fría, liderada por Estados Unidos, se hizo necesario la creación de nuevas tecnologías que permitieran avanzar y tomar ventaja frente al enemigo.

Así, la tecnología de redes para los años sesenta ya era posible. No obstante, la conexión que lograban las computadoras era únicamente bilateral. Lo ideal era la creación de un sistema que permitiera la conexión multilateral. Entonces, se puso en marcha dicho proyecto donde científicos se basaron en dos principios: la conmutación de paquetes y la utilización de un mismo protocolo.[40]

Éstos permitían, que la información no se enviara dentro de la red en forma continua, sino en pequeños paquetes de datos que al llegar a su destino se unieran

---

[38] Rodríguez Ávila Abel, *Iniciación a la red Internet, Concepto, funcionamiento, servicios y aplicaciones de Internet,* Ed. Ideas propias, España, 2007, p. 2, citado en Herrera Capetillo, Héctor Ernesto, *"*Historia y desarrollo de Internet", *Evolución del pensamiento geopolítico en la estudio del ciberespacio,* México, 2014, FCPyS, UNAM, p. 131.

[39] *La estructura de internet* [en línea], Disponible en: http://bit.ly/1Oc96nv. [40] Ibíd. p. 132.

Entiéndase por protocolo de red o de comunicación al conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las unidades que forman parte de una red. Obtenido de: *Protocolos de redes* [en línea], EcuRed, Disponible en: http://bit.ly/2eXhTvs.

acelerando el proceso de envío[41]. Para 1967 la innovación de intercambio de paquetes fue retomada por el científico Lawrence G. Roberts[42] junto con los principios que venían realizando Leonardo Kleinrock[43] (MTT), Paul Baran[44] (RAND Corporation) y Donald Davies[45] (National Physical Laboratory) para introducirlo a ARPA (Advanced Research Projects Agency).

ARPA fue creada dentro del Departamento de Defensa con la finalidad de establecer un claro liderazgo en el área de la ciencia y la tecnología aplicada en las Fuerzas Armadas a través de la construcción de una red de telecomunicaciones incluso en caso de guerra.[46] Con la utilización de un mismo protocolo buscó crear un lenguaje común para todos los ordenadores, de tal forma que pudiera establecerse una comunicación entre ellos.

Amén de cumplir el objetivo, en 1969 nació la Agencia de Proyectos de Investigación Avanzada (ARPANET) compuesta por cuatro nodos de investigación repartidos en Estados Unidos: la Universidad de California, Los Ángeles, el Instituto de Investigaciones de Stanford, la Universidad de California, Santa Bárbara y la Universidad de Utha.[47]

---

41 Barry M. Leiner (et. al) "A brief history of the Internet" [en línea], en Internet Society, Disponible en: http://www.internetsociety.org/es/breve-historia-de-internet.

42 L. G. Robets diseñó y gestionó la primera red de paquetes, ARPANET (el precursor de Internet). En 1967 se convirtió en jefe científico de ARPA para sumir la tarea de diseñar la financiación, la gestión y el concepto radicalmente nuevo a la red de comunicaciones de conmutación de paquetes. Obtenido de *Internet Hall of Fame* [en línea], Disponible en: http://bit.ly/21t3CIz.

[43] L. Kleinrock desarrolló la teoría matemática de redes de paquetes, la tecnología que sustenta Internet. El nacimiento de Internet se produjo en su laboratorio de la Universidad de California en Los Ángeles, EUA, cuando su equipo anfitrión se convirtió en el primer nodo de Internet en 1969. Obtenido de *The University of California, ULCA,* [en línea], Disponible en: http://bit.ly/1PAfiTM.

[44] Investigador de RAND en 1959, diseñó la red de comunicaciones más robusta, utilizando "redundancia" y la tecnología digital, convirtiéndose en la base para la Word Wide Web. Desarrolló la conmutación centralizada, nodos de comunicaciones distribuidas y adoptó el nombre de "conmutación de paquetes" junto con Donald Davies. Obtenido de *Rand Corporation* [en línea], Disponible en: http://bit.ly/1tvpkRa.

[45] D. Davies fue uno de los inventores de las redes de computadoras de conmutación de paquetes, acuñó el término de "paquete". ARPA y ARPANET recibió su diseño y se convirtieron en las primeras dos redes de paquetes de ordenadores en el mundo mediante la técnica. Obtenido de *Internet Hall of Fame* [en línea], Disponible en: http://bit.ly/24Yu7qk.

46 "L'Agenzia A.R.P.A."[en línea], *Le origini di Internet,* Disponible en: http://bit.ly/1LOA7sz.

[47] Castells Manuel, *The Internet Galaxy. Reflections on the Internet, business and society,* Ed. Oxford University Press, Estados Unidos, 2011, citado en Herrera Capetillo, Héctor Ernesto, "Historia y desarrollo de Internet", *Evolución del pensamiento geopolítico en la estudio del ciberespacio,* México, 2014, FCPyS, UNAM, p. 133.

> "El Grupo de Trabajo de Redes (Netwrok Working Group, NWG) creó el Protocolo de Control de Redes (Network Control Protocol, NCP) que se utilizó como lenguaje en común para vincular las redes, vigente de 1970 hasta 1983 cuando se sustituyó por el Protocolo de Control de Transmisión /Protocolo de Internet (Transmission Control Protocol/ Internet Protocol, TCP/IP) funcionando hasta la actualidad."[48]

Así, el Consejo Federal de Redes (FNC, por sus siglas en inglés, Federal Networking Council) con previa consulta a las comunidades de Internet adoptó una resolución que definía a Internet como:

> "(…) el sistema de información global que está enlazado lógicamente a un espacio global de direcciones únicas basadas en el Protocolo de Internet (IP), o sus subsecuentes extensiones; y que puede soportar la comunicación usando el conjunto de Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) o sus subsecuentes añadidos para proveer o dar acceso , ya sea de manera pública o privada, a servicios de alto nivel superpuestos en las comunicaciones y las infraestructuras relacionadas."[49]

Como el embrión de Internet fue desarrollado por la comunidad científica desde los centros de investigación universitarios en Estados Unidos, Reino Unido fue la primera conexión fuera del país. En respuesta, Francia apoyó un proyecto llamado Cyclades que contaba con un sistema menos complejo para el intercambio de paquetes con Estados Unidos, el cual complementaría a ARPANET. Ésta más tarde con el trabajo de Vinton Cerf y Robert Kahn, materializa la creación del TCP/IP, protocolo que permite la transmisión de datos entre los ordenadores.

Un hecho importante para la creación de la infraestructura de Internet se dio cuando el gobierno estadounidense bajo la presidencia de William Clinton, y el vicepresidente Al Gore lanzaron el proyecto "Superautopista de la información" (World Wide Web) el cual construiría la infraestructura necesaria para la comunicación y la instalación de redes de fibra óptica, esto para alcanzar una mayor

---

[48] Félix Badia, *Internet: situación actual y perspectivas.* Ed. La Caixa, Barcelona España, 2002, p. 17, citado en Herrera Capetillo, Héctor Ernesto, *"*Historia y desarrollo de Internet", *Evolución del pensamiento geopolítico en la estudio del ciberespacio,* México, 2014, FCPyS, UNAM, p. 133.

[49] *Ibíd*. p. 131.

velocidad. Mientras que el Helsinki Institut of Technology creó *Erwise*, el primer navegador.[50]

Además, cabe destacar que el lanzamiento de la World Wide Web (www) o también llamada "telaraña mundial" o simplemente "la Red", permitió que el uso de Internet se simplificara haciendo más fácil su uso, la cual no sólo enviaba texto sino también imágenes, sonidos y videos.[51]

El desarrollo de Internet fue de tal manera, que no sólo instituciones sino también personas podían acceder a la red habiendo una amplia apertura, en adición se crearon parámetros técnicos comunes para su desarrollo. Hoy en día su acceso es fácil debido a las diversas máquinas portátiles que lo hacen posible, aún más con al gran avance tecnológico que las impulsa, sin importar el lugar en donde nos encontremos, sea en el hogar, la calle o en el automóvil. Un medio que nos permite una mayor conexión es el cable de fibra óptica que permite el tráfico de información a banda ancha haciendo ultraveloz su envío y recepción.

La creación y avance de Internet es gracias a las instituciones gubernamentales y académicas, así como de la industria privada que en conjunto lograron un alto desarrollo y avance tecnológico. Sin embargo, su regulación y control no compete a ninguna de ellas. El problema de la gobernanza de Internet radica en que no hay un órgano que la lidere en los principios, normas, reglas y procedimientos que configuren el uso de Internet.

La razón quizá sea sencilla, el que lidere el espacio cibernético tendrá el control total del mundo, respecto de su gestión y progreso tecnológico, incluyendo normas jurídicas y teniendo repercusiones en el ámbito político, simplemente por la necesidad que resulta hoy en día Internet. Además de que éste es un medio útil a la sociedad para su organización, por lo que al considerar que un Estado u

[50] *Ibíd.* p. 139.

[51] *Ibíd.* p. 136.

Es importante hacer una diferenciación entre la World Wide Web e Internet, mientras la primera hace referencia a un sistema o conjunto de protocolos para consultar documentos de hipertexto, Internet es el medio a través del cual es posible la transmisión de dichos documentos.

organización encabece su gobernanza, limitaría y restringiría la acción social y organizacional con fines contraestatales.

Por su parte, los principales sectores que en Internet requieren de supervisión y regulación son: 1) los nombres de los dominios, 2) los números de Protocolos de Internet, 3) los servidores de raíz y 4) las normas técnicas para la interoperabilidad de la red: la forma en que los enrutadores envían el tráfico.[52]Todo esto llamado "gobierno de Internet" puede tener un fuerte impacto en asuntos políticos. Por lo tanto, el carácter global de Internet impide que autoridades nacionales o regionales regulen holísticamente su delimitación ciberespacial, así como la delimitación política. El conflicto surge principalmente con la soberanía nacional y el conflicto de intereses que de ella se derivan.[53] El tráfico de datos e información en el caso de entre personas no conoce fronteras, en caso de la existiera una regulación
"internacional" se entraría en conflicto con leyes particulares de cada Estado, con ello en Derecho Internacional tendría que existir un tratado cuyos principios armonicen las leyes del ciberespacio y así evitar conflictos de intereses, sin embargo, esta idea es casi inalcanzable.

Así, otro elemento a considerar es el choque de sistemas jurídicos[54] entre Estados, en caso de regular la red con un uso jurídico, no se puede homologar un protocolo para sancionar los delitos en el ciberespacio en todos los países, además de que el uso de internet también tiene sus variantes entre los Estados ya que ya existen normas internas que prohíben y sancionan ciertos nombres de dominios para sus ciudadanos, tal es caso de China.

---

[52]*Ibíd.* p. 142.

[53]Con soberanía refiero no sólo a la delimitación de las fronteras territoriales, marítimas, aéreas y quizá del espacio exterior, sino en la capacidad de actuar autónoma y responsablemente. Es decir, la soberanía como uso del poder de mando o control político, le concede a los gobiernos la capacidad de actuar a su ventaja y beneficio, sin embargo, dichas acciones se sustentan en una racionalización jurídica, por lo que cualquier decisión queda fundamentado en ella. El problema radica en que dicha autonomía puede llegar a afectar o transgredir la de otros Estados a través de las decisiones "libres y responsables" que se llevan a cabo, en la búsqueda del cumplimiento de sus intereses.

[54] Por choque de sistemas jurídicos refiero a la discrepancia que existe entre los diferentes conjuntos normativos, actitudes, creencias y costumbres jurídicas por los cuales se rige un Estado. Por lo que al intentar homologar medidas a favor del uso del ciberespacio con fines de sanción y procuración de justicia, pueden existir diferencias y grandes confrontaciones entre un sistema jurídico y otro.

Para entender mejor lo anterior:

> "El sistema de nombres de dominio o DNS es un sistema diseñado para que Internet sea accesible para las personas. La principal forma en que los equipos informáticos que conforman Internet se encuentren entre sí es mediante una serie de número (denominada 'dirección IP'), que es específica de cada dispositivo. Los nombres de dominio se componen de dos partes de dos partes separadas por 'el punto'. En la parte derecha del punto se encuentra el dominio de primer nivel o TLD y corresponde con las terminaciones 'com', 'net', u 'org', entre otras. En cada caso hay una compañía (denominada registro) a cargo de todos los dominios que terminan con ese TLD concreto y que tiene acceso a una lista completa con los dominios que tienen ese nombre, así como las direcciones IP con las que estas asociadas los nombres."[55]

Y para ello existen tres organizaciones internacionales que se encargan del control de aspectos técnicos, y de la regulación de Internet hasta donde la red *per se* es posible, a saber:

El Grupo de Trabajo de Ingeniería de Internet

(IETF) La Sociedad de Internet (ISOC)

La Cooperación de Internet para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés) quien se encarga de la coordinación de los identificadores únicos en todo el mundo.

La tarea principal de la Cooperación de Internet para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés) es hacer la red sea segura, operable e interoperativa a través de la coordinación de los identificadores (dirección electrónica, ya sea un nombre o un número), sin ella sería imposible tener internet a nivel mundial. Esto no quiere decir que controle el contenido en Internet. Su funcionalidad radica en la importancia y evolución que le da a Internet gracias a la coordinación del sistema de nombres de Internet.[56]

Mientras que el Grupo de Trabajo de Ingeniería de Internet (IETF) se encarga de los estándares tecnológicos. "Los estándares son solo reglas que definen como

[55] *¿Qué hace ICANN?* [en línea], en ICANN, Disponible en: http://bit.ly/1Qe0E5B.
[56] *Ibídem.*

deben funcionar las cosas, permitiendo una uniformidad que es necesaria para que no haya problemas de compatibilidad. Éste está formado por gente que viene de proveedores de servicio, fabricantes de equipamiento, investigadores, profesores, estudiantes y otros."[57]

Por su parte, la Sociedad de Internet (ISOC) se implica en un amplio espectro de problemas relacionados con Internet, entre los que se incluyen las políticas, la gobernanza, la tecnología y el desarrollo. Establece y promueve:

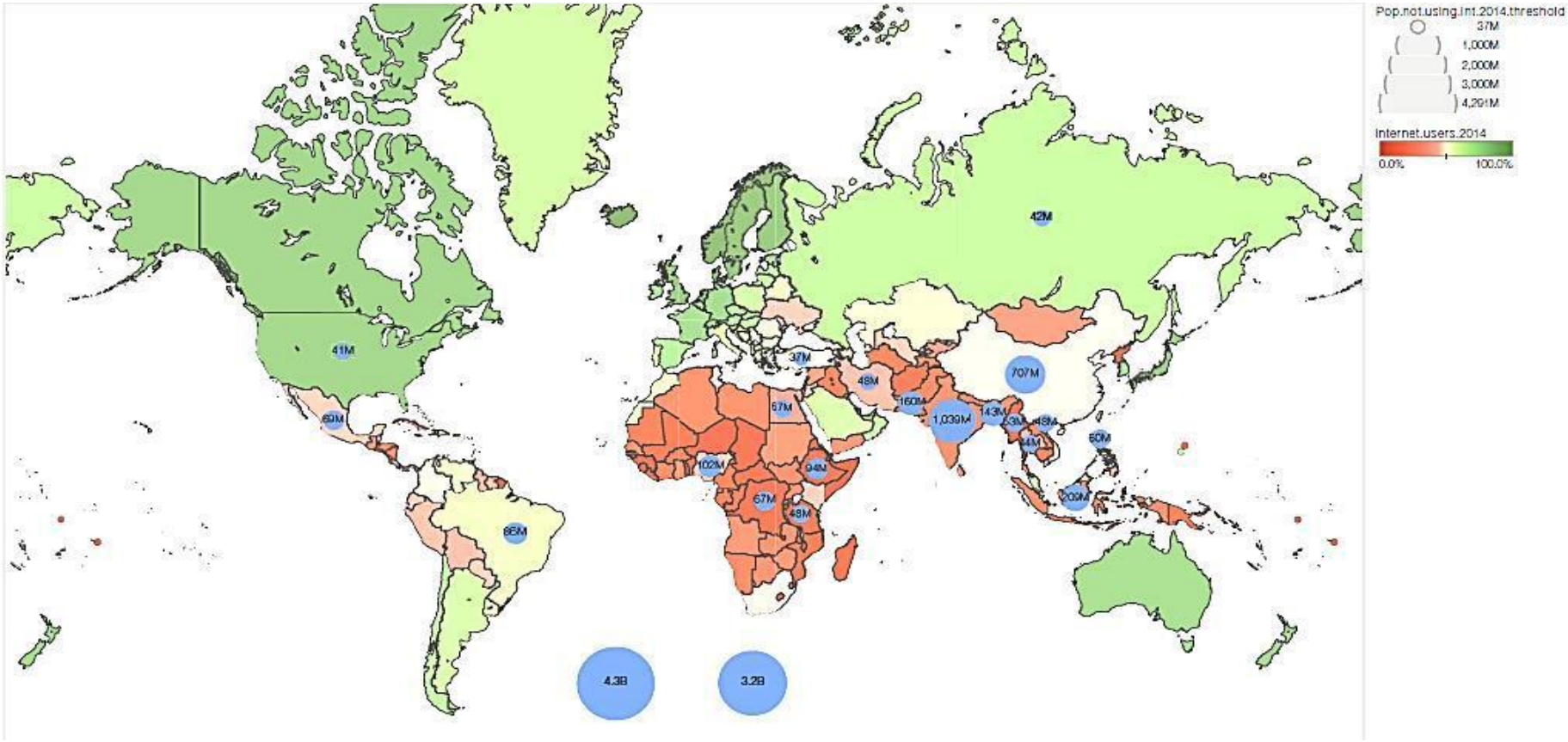
> "(…) principios que tienen como finalidad persuadir a los gobiernos para que tomen decisiones que resulten adecuadas para sus ciudadanos y para el futuro de todos los países. Toda aquella actividad en la que se embarca tiene como objetivo asegurar que Internet esté disponible para todo el mundo, tanto para los que hoy lo habitan como para los próximos mil millones de usuarios."[58]

La necesidad de hacer operable y accesible a Internet forja a estas instituciones a cumplir con su tarea para que todas las personas del mundo puedan utilizarla fácilmente sin problemas ni fallas. Para llevar cabo esto, se necesita de las políticas públicas eficaces, de calidad y con buena orientación política, para que la población no padezca de necesidades, y pueda enfrentar exitosamente las vulnerabilidades en el ciberespacio, lo que se traduce en una sociedad mejor informada y preparada.

De acuerdo con el documento "Internet para todos. Un marco de referencia por acelerar el proceso de acceso y adopción de Internet", más de 4 mil millones de personas no tienen acceso a Internet, equivalente a más de 55% de la población mundial.[59] Ilustrado de mejor manera en el mapa 1.2

[57] *¿Qué es el IETF en español claro?* [en línea], en Internet Society, Disponible en: http://bit.ly/1N9Oasy.
[58] *¿Qué hacemos en Internet Society?* [en línea], Disponible en: http://bit.ly/1XKdih5.
[59] "Internet for all. A framework for accelerating Internet access and adoption" [en línea], *World Economic Forum,* abril 16, Disponible en: http://bit.ly/20Z44hD.

Veinte países son el hogar de tres cuartas partes de 4,3 mil millones de los no usuarios de Internet mundialmente.
Mapa 1.3 Donde se muestran los veinte países con falta de acceso a Internet, en color rojo. Fuente: “Internet for all. A framework for accelerating Internet access and adoption” [en línea], *World Economic Forum,* abril 16, Disponible en: http://bit.ly/20Z44hD.



Cabe destacar la importancia que Internet ha tenido durante las últimas décadas desde su nacimiento, gracias a ésta ha evolucionado y crecido la economía mundial, asimismo ha impulsado a las sociedades, se han creado nuevas formas de comunicación y hasta de pensamiento, sin olvidar que hasta en la política ha tenido beneficios en los tiempos de crisis.

Así, puede identificarse cuáles son las áreas en que a consecuencia de diferentes factores, se ven privado de la conexión a Internet, entre los que destacan, la falta de recursos económicos, tecnológicos, e inclusive culturales.

> "La disponibilidad, la calidad, la fiabilidad y la asequibilidad de internet el acceso se ven afectados por la infraestructura (…). Muchas barreras impiden la construcción de infraestructura y la instalación, incluyendo la falta de electricidad, la cobertura de la red móvil limitada, redes centrales subdesarrolladas y la disponibilidad de alta capacidad backhaul. Estos desafíos son especialmente frecuentes en zonas remotas debido a las largas distancias, las dificultades del terreno, grandes gastos de capital, altos costos operativos y de baja los ingresos medios por usuario. Muchas áreas urbanas presentan su desafíos de infraestructura propios, a pesar de que casi 60% de la población mundial está proyectado, vivirá en ciudades para 2030."[60]

Una vez bien estructurada y coordinada la infraestructura de Internet, ya se puede hablar de ciberespacio, el cual refiere a "un ámbito caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura física asociada. El ciberespacio se puede considerar como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física."[61]

---

[60] United Nations, 2014a, *World Urbanization Prospects: The 2014 Revision, Highlights*, *óp. cit.*

[61] Definición extraída del glosario de términos informáticos, Whatis, Disponible en http://whatis.techtarget.com/, citado en Caro Bejarano María José, *Alcance y ámbito de la seguridad nacional en el ciberespacio* [en línea], Disponible en http://bit.ly/1MCU3Eh.

Dicho en otras palabras, el ciberespacio es el resultado de la construcción de los sistemas interconectados, o sea, de las redes informáticas, permitiendo así la generación de un campo exclusivo para el tráfico de información y datos.

Por su parte "El Departamento de Defensa de EEUU considera el ciberespacio como un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de TI, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y procesadores embebidos y controladores."[62]

En esta definición se aprecia un espectro amplio de todo lo que tiene que ver con las redes, las tecnologías de la información y su infraestructura. De manera tal que los Estados Unidos identifican claramente cuál es el blanco en el que se ha de trabajar para lograr su seguridad, así como los medios a través de los cuales se tiene que ocupar para la consecución de la misma.

1.3 Ciberseguridad: ciberguerra, ciberdefensa y ciberestrategia

El ciberespacio se ha vuelto uno de los entornos más peligrosos debido al desarrollo que ha mostrado Internet, así como la dependencia que éste genera con las personas brindándole comodidad y rapidez al realizar sus actividades diarias. A consecuencia de ello, se han cometido delitos de los cuales, dada la naturaleza del ciberespacio, cualquiera puede cometerlos y/o ser víctima, obteniendo así, daños y perjuicios irreparables.

Del mismo modo, el ciberespacio desde una visión más amplia "proporciona las herramientas necesarias para que los más pequeños puedan enfrentarse,

[62] Joint Publication 1-02. Department of Defense. *Dictionary of Military and Associated Terms*, 2009, [en línea], Disponible en: http://www.dtic.mil, *óp. cit.*

incluso vencer y mostrarse superiores a los más grandes, con unos riesgos mínimos para ellos"[63]

Así ha surgido la necesidad de brindar seguridad en el ciberespacio. La Unión Internacional de Telecomunicaciones en su Resolución 181 la define así:

> "La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger (…) usuarios en el ciberentorno."[64]

Así, acciones como supervisión de las redes y medios de la infraestructura crítica, mejorar la capacidad de alerta y prevención, contar con el equipo necesario para detectar, responder y recuperarse de ataques cibernéticos. Además de una estrategia de defensa, son algunos de los elementos que debe contar la seguridad en el ciberespacio, o bien, la ciberseguridad.

Cabe destacar que como tal, no existe una definición oficial global de ciberseguridad que sea reconocida por los Estados, sin embargo, se pueden enlistar y englobar una lista de acciones, medidas y recursos necesarios amén de lograr la seguridad cibernética con las cuales, algunos Estados han establecido una definición propia . Asimismo, los militares, cuyo enfoque es la guerra, del mismo modo, son los encargados de hacer frente a las amenazas cibernéticas, por lo que su preparación debe incluir en campo informático.

Si bien, los países se han ocupado de la creación de informes en materia de ciberseguridad[65], han hecho el esfuerzo por plasmar una delimitación de ésta, y esbozar los medios con los que harían frente a las amenazas cibernéticas, traducido

---

[63] Sánchez Medero, Gema. "Ciberguerra y ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica". Amérigo Cuervo-Arango, Fernando; Peñaranda Algar, Julio. *Dos décadas de Posguerra Fría*. Instituto Universitario General Gutiérrez Mellado, 2009. Tomo I, p. 215-241, *óp. cit.*

[64] *Ciberseguridad* [en línea], en Actualidades de la UIT, Disponible en: http://bit.ly/1QPmqNo.

[65] Es importante señalar la diferenciación entre los conceptos: "ciberseguridad" y "seguridad cibernética". Básicamente y términos ontológicos significan lo mismo, el primer término es un anglicismo, y el segundo es término desagregado. Mientras que el primero se utiliza en el campo de Defensa, el segundo término expone un matiz jurídico-político

en planes, estrategias y medios de acción para la salvaguarda y protección del espacio cibernético y su infraestructura.

Por lo tanto, el tema de la ciberseguridad es necesario y pertinente debido a que hoy en día todos los movimientos en cualquier nivel de gobierno e individual giran en torno al internet, es por eso que una manera de provocar daños es a través de sus estructuras informáticas y ciberespaciales. La ciberguerra no es algo nuevo, desde hace bastante tiempo se han creado herramientas dañinas que pueden llegar a alterar el bienestar de los gobiernos paralizándolos, afectando sus instituciones gubernamentales o a su misma sociedad.

Joseph Nye expone que el término "ciberguerra" es utilizado vagamente para cubrir un amplio rango de comportamientos que refieren a la guerra, es decir, es un simple y llano término que hace referencia a la existencia de conflictos en el ciberespacio. Empero, argumenta que algunos expertos lo utilizan para definir una "guerra sin derramamientos de sangre" entre Estados que consiste exclusivamente en un conflicto electrónico en el ciberespacio.[66] Es importante reflexionar la idea de Nye, la guerra a través del tiempo se ha modernizado, sin embargo, no deja de ser un enfrentamiento de dos o más bandos o enemigos bien identificados, inicialmente entre Estados, cuyo objetivo es generar violencia en cualquiera de sus modalidades, es decir, física, psicológica, moral, entre otras, sea por tierra, mar, aire o espacio exterior.

El caso del enfrentamiento en el ciberespacio implica una interacción en la cual se desconoce el enemigo a enfrentar, los medios de ataque se vuelven no sólo más sofisticados, sino que su alcance es mayor a una arma convencional, a excepción de las bombas químicas de alto impacto, por lo tanto, su asimilación con la guerra convencional difiere en gran medida.

Como tal, la "guerra" cibernética hace referencia a los ataques y su capacidad de daño en el espacio cibernético a través de Internet, empero, la modernidad del término "guerra" ha hecho referencia no sólo al enfrentamiento entre Estados, sino

[66] Nye Joseph*, Cyberwar and peace* […], *óp. cit.*

también a Individuo vs Estado, donde el individuo cobra fuerza a través de los medios de mayor alcance, como las tecnologías de la información, tal es el caso de los hackers, entre otros.

Asimismo, es importante reflexionar en la "guerra a través de los individuos", una semejanza puede ser el terrorismo, el cual actúa a través de la sociedad para generar un daño o cambio, de la misma manera, el espacio cibernético se presta para accionar a través de los individuos, como la afectación de sistemas bancarios, de comunicación social, de infraestructuras burocrática, etc., es decir, al dañarse algún tipo de capacidad (económica, política, social, electoral, etc.), se daña en consecuente una organización o institución a la que pertenezca, o en el caso de que se afecte a "cierto sector" de la población se afecta y debilita a sí mismo, fracturando el tejido social trastocando al Estado.

Otro elemento a considerar es la posible utilización del término "ciberguerra" como último eslabón dentro de una clasificación de daños en el ciberespacio, es decir, este término refiere al daño "máximo" que va directamente en contra del Estado a través de la infiltración a sus bases de datos y/o del ciberespionaje para obtener información acerca de su infraestructura bélica, sea tecnológica, humana y financiera, de modo tal que dicha información pueda ser utilizada por otro Estado o como amenaza por algún individuo u organización generalmente radical.

Es por esto que los Estados se han encargado de crear los mecanismos y herramientas necesarias para proteger y defender sus estructuras cibernéticas contra las amenazas que afecten a su seguridad. Tales acciones se ejemplifican en "(…) la protección de sus redes, el monitoreo y análisis del tráfico de datos, la detección de ataques digitales y su respuesta a ellos."[67] Expuesto lo anterior se puede hablar de *ciberdefensa*, la cual corre a cargo de las instituciones especializadas del gobierno del Estado, cuyo objetivo debe responder a la protección de sus redes y sistemas.

[67] *The defence cyberstrategy* [en línea], en Netherlands Ministry of Defence, 2012, Disponible en: https://ocdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf.

Cade destacar que de acuerdo con la operatividad del Estado en el ciberespacio y sus capacidades, serán los medios de defensa, en los cuales se incluyen "(…) ordenadores infiltrantes, redes de computadoras, sistemas de armas y sensores y software con el fin de recopilar información e inteligencia y para afectar los sistemas."[68]

Otro elemento son las Fuerzas Armadas, de acuerdo con la Estrategia de Ciberseguridad de Holanda:

> "Las operaciones militares implicarán cada vez más el uso de las capacidades cibernéticas operacionales, principalmente en apoyo de las operaciones regulares de las fuerzas armadas, sino también como un arma en su propio derecho. Las capacidades cibernéticas operacionales deben convertirse en una parte integral de la capacidad militar general de las fuerzas armadas (…). Por ello, la organización de Defensa debe invertir sustancialmente en el fortalecimiento de sus capacidades cibernéticas."[69]

En tanto que las autoridades correspondientes se preparan para la defensa, es preciso previamente formar una estrategia que responda a los intereses del Estado respecto a su seguridad. De acuerdo con el Spanish Cyber Institute de Imss Forum, las ciberestrategias tienen "Como principal objetivo, (…) la ciberseguridad como materia prioritaria en la agenda de los respectivos gobiernos. Y promulgan, con más o menos éxito, establecer un liderazgo único para coordinar las acciones y los actores involucrados en la lucha contra los riesgos derivados del ciberespacio"[70], los cuales que más adelante se mencionan.

Asimismo, ponen de manifiesto la gravedad y complejidad de las ciberamenazas, así como el grado de organización alcanzado por los grupos delincuentes o terroristas que pueden, en dado caso, estar detrás de ellas. Y

---

[68] *Idem.*

[69] *Idem.*

[70] Solé Pascual, Carles y Adolfo Hernández, *Estrategias nacionales de seguridad en el mundo* [en línea], Home Red Seguridad. Revista Especializada en Seguridad TIC, 23 de septiembre de 2014, Disponible en: http://bit.ly/2brTmOw.

enfatizan la dimensión social del problema, esto sin olvidar que el contacto con los individuos es de primera mano, cuya intervención en Internet los vuelve vulnerables a recibir cualquier daño, como anteriormente se había mencionado, hoy en día casi cualquier delito no físico es afecto a realizarse por la red. Es por eso que trasciende en la pérdida económica o en el daño individual que puedan causar.

También identifican la necesidad de coordinación entre los estamentos públicos dedicados a la ciberseguridad y la de éstos con los actores privados, una de las principales barreras a la hora de luchar contra el cibercrimen, debido a que son las que tienen en sus manos la gran medida la capacidad de libertar o limitar a través de sus productos, sean redes sociales, aparatos y/o software informático, entre otros, la interacción entre los individuos y protegerlos o no de los ataques cibernéticos. Destacan, por supuesto, la necesidad de cooperación internacional, otra gran asignatura pendiente en la batalla contra un riesgo que, por naturaleza, es global."[71]

Así con esto, la seguridad del ciberespacio para los Estados requiere de la creación de una serie de planes, programas y estrategias, así como de medios, para lograr una efectiva defensa frente a cualquier amenaza, riesgo o peligro. Cuyo objetivo es crear una protección integral a las redes y sistemas cibernéticos se necesita de la cooperación y participación de instituciones, agencias y otros organismos públicos y privados especializados.

1.4 Amenazas y vulnerabilidades en el ciberespacio

El contenido real de la ciberguerra se traduce en acciones, es decir, en los ataques en el espacio cibernético o ciberataques. De acuerdo con la Organización del Atlántico Norte (OTAN) los ciberataques se consideraban un riesgo real pero de ámbito y consecuencias limitadas, y que requería de respuestas técnicas acompañadas de unos pocos esfuerzos de información pública. Sin embargo, hoy

[71] *Idem.*

día esto ha cambiado convirtiéndose en una prioridad para la mayoría de los gobiernos quienes han identificado el ciberespacio como una "zona clave" para el resguardo de su seguridad.

Las características de los ataques cibernéticos se clasifican en:

> "físicas (capilaridad y ubicuidad, anonimato y seguridad para el atacante, por cuanto es difícil ser detectado), por ejemplo, fraudes bancarios, usurpación de identidad, etc.;
> económicas (eficiencia, rendimiento, mantenibilidad, por ejemplo, un ordenador con conexión a Internet puede ser suficiente para concretar un ciberataque y la información que contiene puede ser duplicada fácilmente en caso de recibir un ataque de respuesta);
> propagandísticas (difusión, divulgación e impacto de la información con la que se desea sensibilizar y conseguir apoyo), tal es el caso del ciberterrorismo; y,
> operativas del entorno (velocidad, alcance fácil acceso y coordinación, disuasión, factor miedo que se produce cuando se es objeto de ataque, difícil atribución, potencia, criticidad de objetivo al atacar o afectar sistemas de información de personas, grupos o instituciones).[72]

Una vez expuestas las características de los ciberataques se pueden considerar otros como el ciberterrorismo, el ciberespionaje, la ciberusurpación, el ciberdelito y los que de éste se deriven, así como la infiltración de la información y datos confidenciales.

Asimismo, dichas características son los elementos de los cuales se sirve un individuo para atacar, de los cuales se generan la dificultad para implementar planes de seguridad y defensa, así como el diseño de programas informáticos con los mismos fines.

Amén de cumplir el objetivo de cada ciberataque, ciberdelito y otros, se utilizan diferentes medios como:

---

[72] Sancho Hirane Carolina, *Ciberespacio: delitos, amenazas a la seguridad y ¿guerras?* [en línea], en Academia Nacional de Estudios Políticos y Estratégicos (ANEPE), Disponible en: http://bit.ly/1OcTy36.

> "la distribución de virus o gusanos, descargas ilegales de información a través del phishing (intento de adquirir información (y, en ocasiones, también de dinero, aunque sea de forma indirecta), como nombres de usuarios, contraseñas y datos de tarjetas de crédito haciéndose pasar por una entidad de confianza en una comunicación electrónica);la pharming (forma de ataque cuyo objetivo es redireccionar el tráfico de un sitio web hacia una página fraudulenta);el malware (término general que se utiliza para referirse a distintas formas de software hostil, intrusivo o molesto);el spyware (tipo de malware (software malintencionado) que se instala en las computadoras para obtener información sobre los usuarios sin que éstos lo sepan) y el spam (uso de sistemas de mensajes electrónicos para enviar de forma indiscriminada un gran número de mensajes no solicitados)."[73]

Así, los Estados a través de la identificación de sus principales amenazas y sus medios de ataque buscarán las tácticas de prevención y defensa que le permitan mantener su estructura cibernética a salvo, junto con la información confidencial que tenga bajo reserva del gobierno. Es importante que cada Estado securitice sus amenazas pero también sus principales enemigos, con los cuales mantenga un margen de actuación y, en caso, de ser atacado por éstos previo tener un plan de ataque y/o defensa.

En cada caso los tomadores de decisiones se encuentran influenciados por la percepción del riego que representa una amenaza, de acuerdo con Gross Stein, el impacto de la aversión a las pérdidas en la percepción de la amenaza es considerable, por lo tanto los líderes, en este caso, quienes tienen a su cargo la protección y defensa de su país, se encuentran más sensibles a lo que tienen porque tienden a darle más valor a dichas riquezas.[74]

De manera tal, los desafíos que representa la amenaza son una pantalla útil para el tomador de decisiones e idear los mecanismos de defensa necesarios. Es

---

73 *¿Qué son el malware, el spyware, el spam, el phishing, el pharming, etc.?* [en línea], en Totalbank, Disponible en: http://bit.ly/1Tbkwbb.

74 Gross Stein Janice, *The Oxford Handbook of Political Psichology,* 2ª Ediciónpoy Leonie Huddy, David O. Sears, y Jack S. Levy. Oxford University Press, 2013, p.p. 23-25.

por eso que los líderes tienen que vigilar sus amenazas evaluando posibles pérdidas, que bajo dichas circunstancias es probable que se sobrestimen las amenazas.

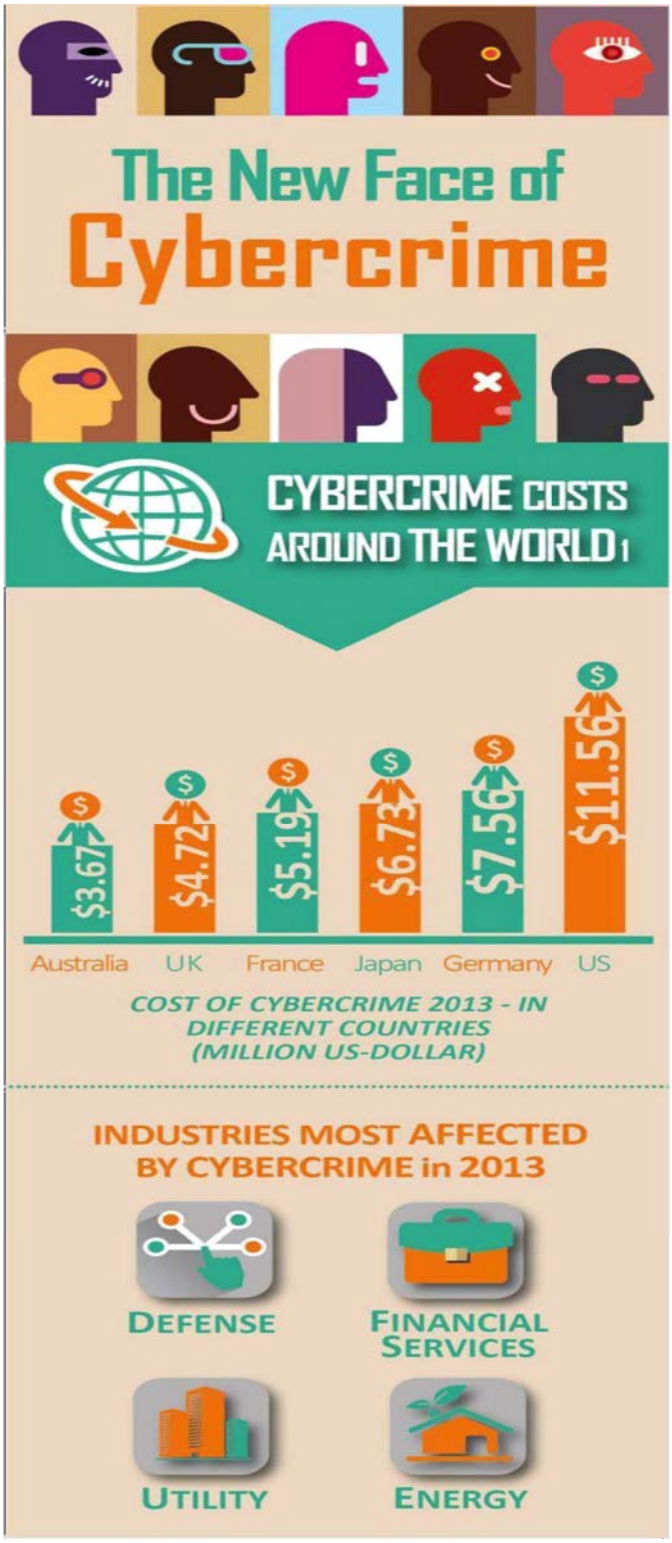
Asimismo podrá medirse su vulnerabilidad a través de las características y circunstancias de una comunidad, sistema o todo aquel o aquello que sea susceptibles a los efectos dañinos de las amenazas cibernéticas.[75] Sin olvidar, el grado de desventaja que se tiene ante el riesgo expuesto, asimismo el grado de fragilidad para enfrentar dicha amenaza y recibir el impacto, así como la capacidad de resiliencia, la cual refiere a la capacidad de un sistema, comunidad o sociedad expuestos a una amenaza para resistir, absorber, adaptarse y recuperarse de sus efectos de una manera oportuna y eficaz, lo que incluye la preservación y la restauración de sus estructuras y funciones básicas.[76]

La diversidad de amenazas a la seguridad nacional hace necesario la prevención de éstas. Específicamente, el ciberespacio es hoy día uno de los más importantes y estratégicos medios para la guerra y el uso de la información ajena. Las principales potencias mundiales como Estados Unidos, China, Rusia, Inglaterra, Alemania, entre otros, son quienes de manera notoria se han visto inmersos en problemas con su ciberespacio.

Es por eso que el surgimiento de nuevos actores a la escena internacional, hoy en día presentes con el afán de causar daños principalmente a Estados u otros entes no gubernamentales, no estatales e incluso individuales, genera cambios en los gobiernos, por ejemplo, en la siguiente En la imagen 1.4 titulada *The New Face of Cybercrime*, “La nueva cara del cibercrimen” [77], se pueden apreciar los grandes alcances que ha tenido el problema alrededor del mundo, no sólo en materia meramente de seguridad, sino que genera estragos en otros sectores de gubernamentales.

[75] *Definición del Riesgo* [en línea], CIIFEN, Disponible en: http://bit.ly/1hRPdCP.
[76] *Idem.*
[77] La imagen se dividió en tres partes, para mayor claridad en la misma y su contenido.

Imagen 1.4 *The New Face of Cybercrime*, "La nueva cara del cibercrimen" Fuente: http://www.hobsoft.com/.



Dicha imagen ubica un top de 6 países de costos generados por el cibercrimen durante el 2013,a saber, en primer lugar se ubica Estados Unidos con un costo total de 11.56 millones de dólares, seguido de Alemania con 7.56 millones de dólares, en tercer lugar se encuentra Japón con un gasto de 6.73 millones de dólares, en el cuarto Francia con 5.19 millones de dólares, el quinto lugar lo ocupa Reino Unido con un costo de 4.72 millones de dólares y el sexto lugar es de Australia con un costo de 3.72 millones de dólares.

De acuerdo con los datos anteriores, se puede clasificar los países no sólo más afectados, así como el nivel de daño, sino también los más preocupados por reparar el daño causado y con mayor capacidad económica.

Asimismo, expone que las industrias más afectadas por el cibercrimen son la de defensa, el sistema financiero, la industria energética y la de servicios públicos. Mismas que componen la infraestructura crítica de un país, a saber, los más importantes, sin dejar de lado algunos otros que pueden ser fuertemente afectados como el de salud, sistema aéreo, de transportes, hasta el comercial, que en su conjunto llevan el control y funcionamiento de las actividades fundamentales de un país y su administración.

De acuerdo a la información mostrada en la imagen de la derecha subtitulado *World wide security threats, "Las amenazas a la seguridad de todo el mundo":*

El robo de datos causa el 43% de los costos externos totales. En 2013 incrementó un 2%.

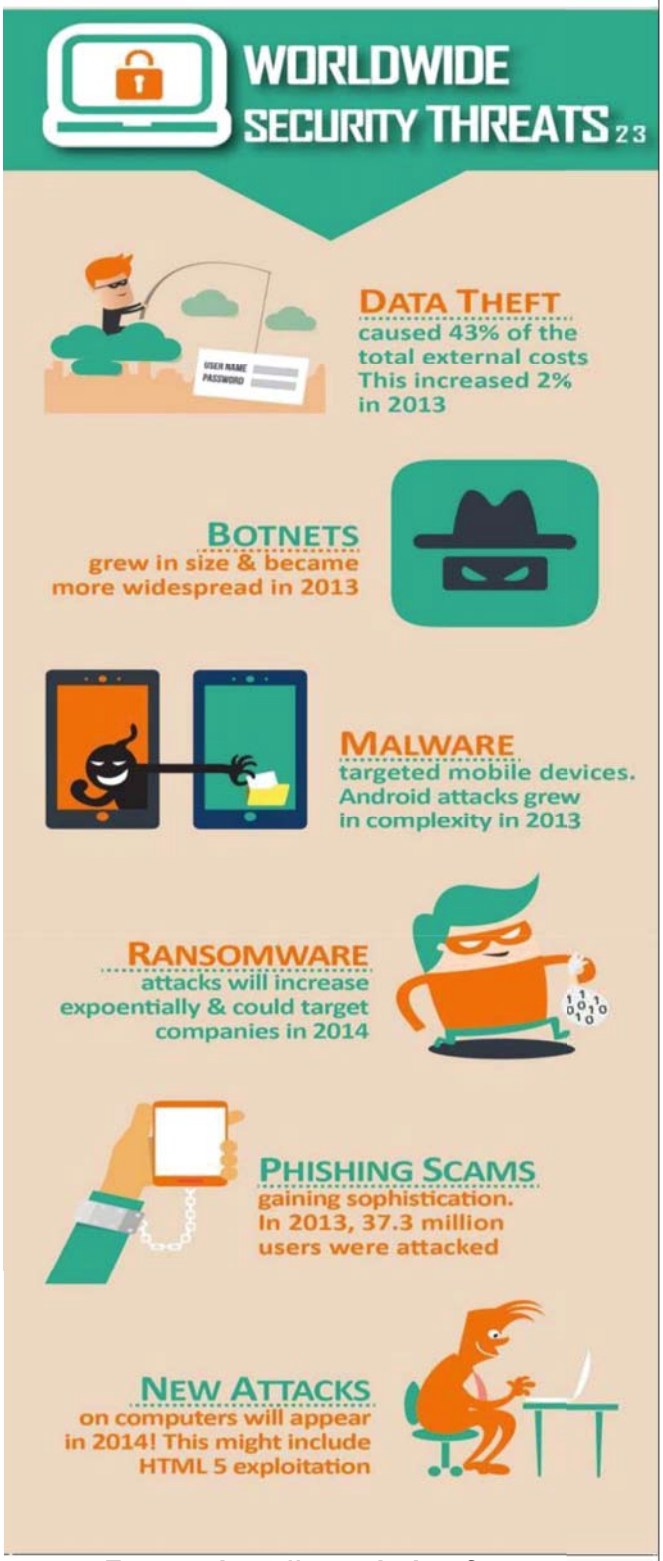
Los robots informáticos los cuales crecieron en tamaño y comienzan a extenderse en 2013.

El malware o software para dañar o deshabilitar computadoras o sistemas, que va dirigida a dispositivos móviles. Se destaca que los ataques al sistema operativo Android crecieron en 2013 en su complejidad.

El Ransomware o software malicioso diseñado a bloquear el acceso a un sistema computacional hasta que una suma de dinero es pagada, bajo el cual los ataques incrementaron exponencialmente y que pudieron haberse dirigido a compañías en 2014.

La estafa o suplantación de identidad, los cuales ganaron sofisticación. En 2013 37.3 millones de usuarios fueron víctimas de este delito.

1.4.1 World wide security threats, "Las amenazas a la seguridad de todo el mundo"



Fuente: http://www.hobsoft.com

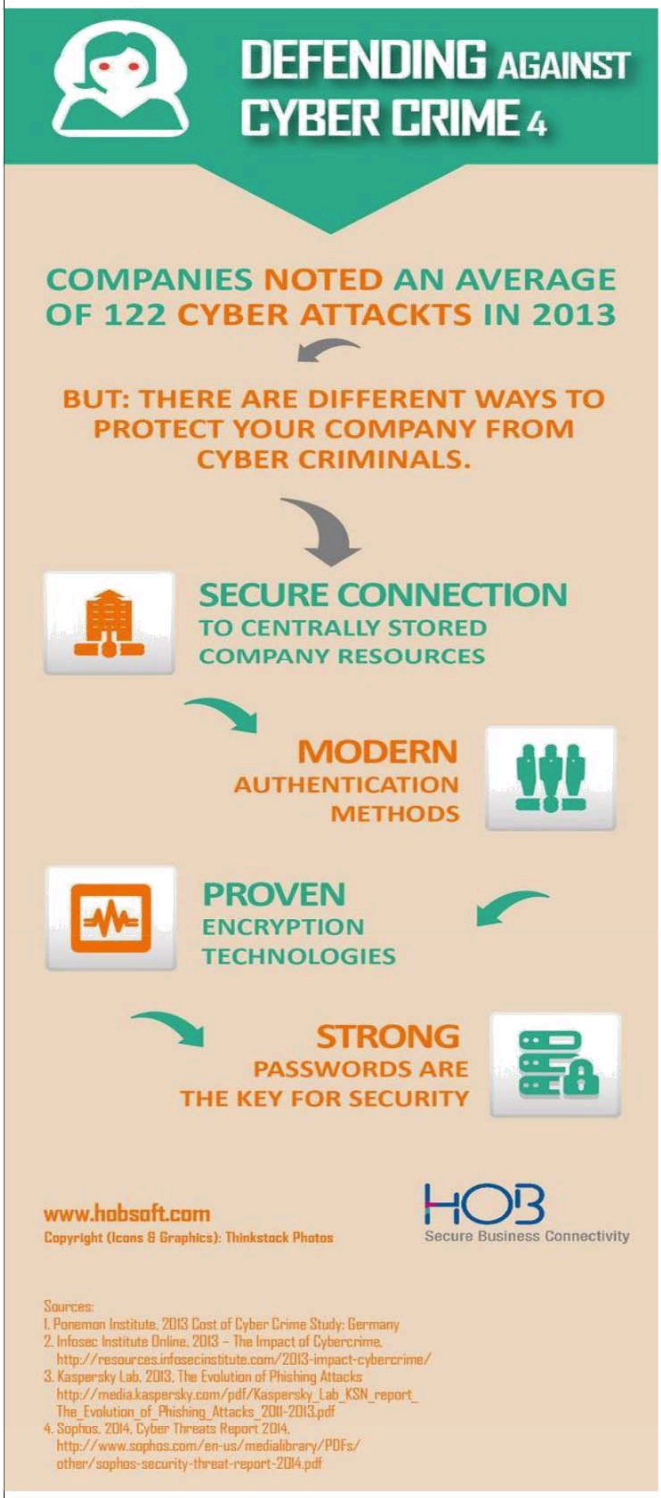
Es importante destacar que 2013 fue el año de la Gran Violación a la Seguridad Cibernética sobre todo con fines financieros, hackeando empresas y gobiernos. Entre los que destacan, usurpación de identidad y robo de datos, como fechas de nacimiento, información de tarjetas de crédito, número de documentos de identidad, domicilios particulares, historias clínicas, números de teléfono, información financiera, direcciones de correo electrónico, claves de acceso, contraseñas y otra clase de información personal, cuyo número alcanzó hasta los 10 millones de identidades afectadas.[78]

Entre los más conocidos ejemplos están: el ciberataque a la empresa Sony Pictures en 2014 por Corea del Norte, el ataque al gobierno estadounidense en 2015 donde se dejó al descubierto la información de 21.5 millones de ciudadanos. Otro es el hackeo de un coche Chysler con el control de la electrónica del vehículo en movimiento, que en consecuencia generó numerosas pérdidas a la mencionada empresa.

Dichas amenazas son algunos de los muchos que pueden efectuarse a través de ciberespacio indirectamente en perjuicio del Estado, sin mencionar otros de los ataques dirigidos directamente a las instituciones gubernamentales.

[78] *Tendencias de seguridad cibernética en América Latina y el Caribe,* Organización de los Estados Americanos, junio de 2014, p. 10, Disponible en: http://bit.ly/2a3Kr3t.

1.4.2 Defending against cybercrime, "Defensa contra el cibercrimen" Fuente: www.hobsoft.com



La imagen a la izquierda subtitulada *Defending against cybercrime,* "Defensa contra el cibercrimen" expone que en 2013 Compañías anunciaron un promedio de 122 ciberataques, por lo que presenta diferentes formas de proteger a una compañía (pública o privada):

- Lo primero es establecer una conexión segura para almacenar de forma centralizada los recursos de la compañía,
- Utilizar métodos modernos de autenticación,
- Implementar tecnologías de encriptación probadas,
- Así como establecer fuertes contraseñas ya que son la llave para la seguridad.

Como se menciona estos son las amenazas y cifras que se manejan para 2013, sin embargo, no debe olvidarse que el espacio cibernético obedece a una constante evolución y complejidad, por lo que para la actualidad y en un futuro se podrá hablar de amenazas y daños de mayor alcance y complejidad. De la misma manera sucede con los costos totales generados para cada país ya que ante los desafíos que representan dichos ciberataques, serán mayores las inversiones por parte del Estado para su defensa.

Una nueva alternativa a contrarrestar los efectos o daños de los ciberataques es la que presenta el Foro Económico Mundial a través del *Informe Global Risks 2016,* como resultado de la búsqueda de soluciones a los riesgos "en foco", uno de ellos a destacar, es el de la dinámica compleja de las sociedades en la era digitalizada, dicha alternativa es la *resiliencia imperativa,* "una necesidad urgente de encontrar nuevas vías y más oportunidades para mitigar y aumentar la resiliencia frente a los riesgos y amenazas a través de los diferentes grupos de interés."[79]

Según los riesgos "en foco", la clave para aumentar la resiliencia es la estabilidad de las sociedades, por lo que dicha estrategia va encaminada a los social, donde se explora el camino a la inestabilidad social, si los gobiernos y las empresas tomas acciones represivas o no, como respuesta a la incertidumbre de cómo hacer frente a una ciudadanía más informada, conectada y exigente, lo que podría generar mayor desconfianza y una respuesta más dura de cada lado.

Es decir, se trata de dar solución a los problemas y tensiones creadas por la creciente conectividad cibernética entre las personas quienes al ser ciudadanos se ven marginados por los procesos de toma de decisiones por los gobernantes. A saber, con el propósito de brindar medidas de seguridad cibernética a los ciudadanos, muchos de éstos no la reciben o simplemente son apartados.

Así, se puede apreciar que la seguridad cibernética no sólo es un problema que aqueje a los gobiernos e instituciones privadas, etc., sino también a las personas. Directa o indirectamente son quienes reciben los efectos de los daños generados por los ataques cibernéticos. Ya sean ataques entre individuos-Estado o Estado-Estado, las consecuencias negativas se enfocan no sólo en la infraestructura crítica sino en un segundo plano en los individuos (ciudadanos) quienes al ser usuarios de dichos servicios reciben los efectos de los ciberataques a través de las diferentes formas de ataques como la Denegación de Servicio, usurpación de indentidad, robos o estafas bancarias, robo de información, etc.

[79] *Global Risks Repot 2016* [en línea], World Economic Forum, Disponible en: http://bit.ly/1RvWKZK.

Es por ello que, es tarea fundamental de los tomadores de decisiones, la industria privada, los espacios de investigación, los organismos, entre otras agencias especializadas, por encontrar y ejecutar las mejores medidas y medios a favor de la seguridad cibernética que beneficien a la gran mayoría, amén de salvaguardar la protección de los mismos, y así lograr que cualquier persona sea capaz de reaccionar y enfrentar dichos ataques, así como también estén mejor preparados ante las amenazas y riesgos cibernéticos.

Es importante rescatar y enfatizar la preparación del individuo en contra de los ciberataques y en favor de su ciberseguridad. No sólo con tecnologías y paquetes de seguridad informática sino también a través de leyes que les sirvan como mecanismo de defensa contra el hacker o atacante donde el Estado mismo por medio de empresas o instituciones brinde el apoyo y seguridad cibernética del individuo con una ciberestrategia previa.

Asimismo, con la existencia de leyes con respecto a los daños generados el Estado establece algunas leyes[80]:

- Ley Uniforme de operaciones electrónicas

- Firma Electrónica en Global y la Ley Nacional de Comercio

- Ley de Seguridad Nacional - Ley de Desarrollo de Seguridad Cibernética Investigación y

- La protección de los niños en la Ley de siglo 21

- Ley de Protección de Niños en Internet

- Adam Walsh de Protección del Niño y la Ley de Seguridad

- Mantener el Desprovisto de Internet Sexual - Ley de Depredadores

- Libertad de Información - Ley de Privacidad

[80] *Global Cybersecurity Index & Cyberwellness Profiles Report* [en línea], ITU, april 2015, Disponible en: http://bit.ly/1oERpmG.

Capítulo 2. La política exterior de Estados Unidos de América en materia de seguridad: el ciberespacio

La política exterior de los Estados Unidos de América durante la administración de Barack Obama enfrentó constantes altibajos. La lucha fue constante por reposicionar el poderío estadounidense, especialmente respecto a su seguridad nacional frente aquellas amenazas o peligros que ponen en riesgo los valores o convicciones morales que forman parte esencial del pueblo estadounidense. Frente a las crisis geopolíticas, como en el caso de la guerra cibernética, Estados Unidos se ha preparado en forma y fondo con los recursos necesarios para hacerle frente. A continuación, se presentarán las bases en su política de seguridad y en la estrategia de seguridad nacional en materia de ciberguerra.

2.1 La Política de Seguridad de Estados Unidos de América

De acuerdo con el Firepower Index 2016[81], Estados Unidos de América lidera hoy en día como la nación más poderosa, entre los factores a consideran en dicho índice se destacan: la salud económica, los factores geográficos y recursos, la capacidad militar, así como otros factores que le permite hacerle frente a nuevos retos y oportunidades del siglo XXI. Sin embargo, desde principios del siglo, Estados Unidos ha sufrido importantes daños que afectan a la nación, un ejemplo clave es el atentado a la Torres Gemelas el 11 de septiembre de 2001, el cual significó un parteaguas en la doctrina estadunidense en materia de seguridad nacional desatando una guerra contra el terrorismo; tal es caso de la invasión a Afganistán y

[81] *United States of America Military Strength* [en línea], Disponible en: http://bit.ly/1K3i4z4.

la Guerra de Irak, hasta el derrocamiento de Sadam Husein, su captura en 2003 y ejecución en 2006.

De la misma forma la *Gran Recesión de 2008* marcó una pauta importante para el gobierno que puso en duda la fortaleza y confianza de su economía y su mercado, además de que dichas consecuencias afectaron a otros países. A saber, la región Asía-Pacífico representaba, e incluso actualmente representa, un contrapeso y fuerte rival económica, especialmente con China. De manera que la creación de nuevos polos y bloques de poder han contrarrestado el poderío estadounidense.

Con la entrada de la administración de Obama en 2009,

> "hay un reconocimiento implícito del fin de la primacía de EEUU y de la Unipolaridad (cuya existencia era, por otra parte, virtual), aunque se siga manteniendo la supremacía militar estadounidense y una búsqueda de mejora del poder normativo norteamericano. Se ha dado prioridad a iniciativas como la creación del "Smart Power" y la desmilitarización de la política exterior de EEUU, dando un mayor protagonismo al Departamento de Estado y reduciendo el peso del Departamento de Defensa, política además llevada a cabo con entusiasmo por su secretario Robert Gates."[82]

Por su parte, en la *Estrategia de Seguridad Nacional 2010,*[83] el gobierno estadounidense reconoce que la fuerza e influenza en el extranjero empieza "en

[82] García David, *La "Doctrina Obama", la teoría de la Guerra Limitada y la nueva política exterior de EEUU: ¿Hacia una política neo-nixoniana?* [en línea], UNISCI, Universidad Complutense de Madrid, No. 18, Enero 2012, Disponible en: http://bit.ly/23pwZhT.

[83] Como fundamento es importante recordar "La Ley Goldwater-Nichols de 1986 (…) [la cual requería] que cada gobierno presente un informe anual al Congreso, estableciendo los objetivos estratégicos de seguridad integral de la nación. La tradición comenzó con el presidente Harry S. Truman en 1950 con la NSC-68, un informe preparado por Paul Nitze, que se concentraba en Estados Unidos y la entonces Unión Soviética y establecía la doctrina de contención que dominó la subsiguiente guerra fría. Desde entonces cada presidente presenta un documento similar al Congreso en diversas formas y diferentes grados de especificidad" Es así como cada Estrategia de Seguridad Nacional mantiene los mismo objetivos de preservación del bienestar y estabilidad de la nación pero con diferentes contextos frente los cuales Estados Unidos se mantiene al tanto de las amenazas y riesgos. Ejemplo de ello es la ESN de G. Bush en 2002 presentada después del 11S; así como la evolución de visión en las Estrategias de B. Obama frente los nuevos retos del siglo XXI y la condición estadounidense frente al mundo después de la guerra. Obtenido de: "Agenda de Política Exterior de los

casa", y que ésta tiene que ser extendida a más países. Expuesto de igual forma en *La renovación del liderazgo estadounidense* de Barack Obama[84] en 2009, donde habla de una "seguridad común y una humanidad común", como resultado de brindar seguridad y bienestar tanto para los estadounidenses como para los que viven más allá de las fronteras, así con ello, el bien de los demás generará el de los estadounidenses.

Asimismo la ESN conviene en que debe construir e integrar las capacidades que puedan aventajar sus intereses, y dichos intereses con otros países y personas, lo que se traduce en la extensión de su influencia a más países .Por lo que Obama, aclama la reconstrucción de alianzas, asociaciones e instituciones necesarias para enfrentar amenazas comunes y reforzar la seguridad común.[85]

> "Al final de 2014, los Estados Unidos (…) [habrían] puesto punto final a más de diez años de operaciones militares en Irak y Afganistán en los que el país ha contemplado una profunda crisis económica y financiera que ha sacudido los fundamentos del modo de vida americano mientras otros, aprovechando en parte esa situación, han experimentado espectaculares crecimientos económicos sostenidos y comienzan a perfilarse como competidores en el tablero internacional, en el que reclaman una participación más activa y favorable a sus intereses."[86]

Lo que pone en desafío a toda costa, la capacidad, eficiencia, efectividad, responsabilidad, liderazgo y poder de Estados Unidos. Asimismo porque hoy en día,

---

Estados Unidos de América", *Periódico electrónico del Departamento de Estado de Estados Unidos,* Vol. 7, Núm. 4, p. 2, Disponible en: http://bit.ly/2bCiuR8.

[84] *Óp. cit.*

[85] Dichas alianzas representan para Estados Unidos poder desarrollarse en un medio seguro y de oportunidades para todos sus connacionales. Al estar al tanto de lo que sucede en el globo, es posible ayudar y prepararse ante las eventualidades del medio internacional, sean conflictos, guerras, el surgimiento de nuevas amenazas a la paz y seguridad mundial. Frente los cuales, el Estado se ve vulnerable a través de sus aliados porque podría tener efectos de gran alcance. Asimismo, remarca la necesidad de potenciar a sus aliados para que en conjunto venzan efectivamente Obtenido de: "Discurso de Barack Obama en la Academia Militar de West Point" [en línea], *Red Voltaire,* 28 de mayo de 2014, Disponible en: http://bit.ly/2bAVaWV.

[86] Sánches Tapia Salvador, *Política exterior y de seguridad de los Estados Unidos: la "Pax americana" después de Afganistán* [en línea], Instituto Español de Estudios Estratégicos, 43/2014, Disponible: http://bit.ly/1JD6IWU.

las amenazas se han vuelto tan peligrosas y complejas que las que han enfrentado en el pasado, y por ende, forjan la necesidad de nueva visión de liderazgo para el siglo XXI. Es importante destacar que Estados Unidos prevé a éste a través de hechos y ejemplo.

Otro punto a destacar es el poder bélico, donde el gobierno de Barack Obama plasma los "límites que tiene el poder militar" para resolver los múltiples desafíos que enfrenta Estados Unidos en los problemas de paz y seguridad mundiales, dicha afirmación responde a la cuestión de que nuevas amenazas no convencionales ponen a prueba la capacidad bélica y su pronta respuesta a ellos, cuyos resultados no son los más satisfactorios.

Para ello, en la *Estrategia* se resalta a las Fuerzas Armadas como piedra angular de la seguridad nacional, sin embargo, admite que deben ser complementadas, lo que quiere decir que requieren de actualización y mayor capacitación junto con nuevas tecnologías.

De acuerdo con Obama, se necesita revitalizar el aparato militar, hacerlo más fuerte para mantener la paz, con la capacidad de derrotar rápidamente cualquier amenaza convencional o enemigos que pelean en campañas asimétricas, y defender sus intereses vitales.[87]

Lo mismo sucede en el ámbito económico, donde Estados Unidos reconoce que se tiene que abordar eficazmente para así resguardar sus propias capacidades. En consecuencia, el liderazgo y la fortaleza de Estados Unidos dependerán de sus capacidades y debilidades, así como de los riesgos a los que se enfrenta; por lo tanto, en su ámbito interno reorganiza y ordena para poder después repuntar ante los nuevos actores del medio internacional que lo desafían. Un ejemplo claro, es el de las amenazas del ciberespacio, frente las cuales los Estados Unidos deben consolidarse de igual forma como líderes, llevando a cabo una serie de estrategias para lograr su fortificación interna y externamente. Así como la creación de recursos

[87] *La Renovación del liderazgo estadounidense* [en línea], Nuevo Orden Mundial, 9 de febrero de 2009, Disponible en: http://bit.ly/23iTcwP.

tecnológicos, humanos capacitados, alianzas para la cooperación y desarrollo a favor de la seguridad cinbernética.

2.1.1 La definición estadounidense de la ciberguerra en la seguridad nacional

The 2014 Quadrennial Homeland Security Review (QHSR 2014)[88] o La Revisión 2014 de Seguridad Nacional es el documento que refleja el enfoque y colaboración del gobierno de EUA entre sus Departamentos de Seguridad y Defensa a través de sus capacidades de planeación, estrategia y análisis. Dicho documento prioriza los riesgos que amenazan la seguridad de Estados Unidos de América, y conduce a la planificación operativa, a fin de llevar a cabo la defensa, por lo tanto, también analiza los recursos disponibles y a futuro, sean tecnológicos, humanos, armamentísticos, entre otros, para los siguientes cuatro años.

Es importante destacar que para lograr la seguridad del Estado es necesario la cooperación y responsabilidad de personas de diferentes niveles de gobiernos, desde el federal hasta los locales, tribales y territoriales, incluyendo al sector privado y organizaciones no gubernamentales, cuya responsabilidad recae "en la seguridad pública, así como poseen y manejan la infraestructura y los servicios críticos del Estado realizando investigaciones y de desarrollo tecnológicos."[89]

Si bien, el entorno cibernético se ha convertido hoy en día, en uno de los medios más demandados por el mundo, por su parte "los Estados Unidos se enfrentan a una gran variedad de amenazas en el ciberespacio, desde el robo de la

[88] El QHSR reconoce la responsabilidad de las acciones del Departamento de cientos de miles de personas a través de los gobiernos federales, estatales, locales, tribales y territoriales, el sector privado y otras organizaciones no gubernamentales, y proporciona un camino a seguir para participar en las asociaciones público-privadas. Las prioridades tienen en cuenta riesgos establecidos en esta revisión conducirá a la planificación operativa, así como el análisis de opciones de recursos y capacidades; y ventajas y desventajas en los próximos cuatro años.

[89] *The 2014 Quadrennial Homeland Security Review, Safeguard and Secure Cyberspace* [en línea], Disponible en: http://1.usa.gov/25VQRKO.

propiedad intelectual a través de EE.UU. intrusiones cibernéticas a ataques de denegación de servicio contra sitios web del lado público e intentos de intrusiones de EE.UU. infraestructura crítica."[90]

Es por ello que el Departamento de Seguridad Nacional (*DHS, por sus siglas en inglés, Department of Homeland Security)* estrecha relaciones con los diferentes socios públicos y privados a fin de reforzar la seguridad cibernética, tareas entre las que se destaca, llevar a cabo el seguimiento de los delitos informáticos, compartir información útil para reforzar dicha seguridad en cuyo contenido va implícitos los derechos y libertades de los ciudadanos estadounidenses en el uso de la red.

Para el Estado es una prioridad, proteger su infraestructura crítica, debido a que a través de ellas se llevan a cabo servicios básicos como el transporte, el agua, la electricidad, las telecomunicaciones, administración, instalaciones del espacio exterior, industria química y nuclear, agua, redes de energía, telecomunicaciones, salud, así como el financiero y tributario, entre otros, y los sistemas de producción como el industrial.

"El alto nivel de desarrollo de las sociedades occidentales descansa en su mayor parte en una serie de servicios básicos y esenciales, sin los cuales no hay capacidad de subsistencia."[91], y que por ser imprescindibles, necesitan ser protegidos. Ésta se desarrolla fundamentalmente en el ciberespacio, "(d)e tal manera que cualquier interrupción no deseada, ya sea debida a causas naturales, técnicas, ya sea por ataques deliberados, tendrían graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, aparte de ser una fuente de perturbaciones graves en materia de seguridad."[92]

Así, la elaboración de un documento que se enfoque en las amenazas que atentan y peligran al Estado, no sólo es necesario para contemplar los medios

[90] *Óp. cit*.

[91] Caro Bejarano, María José, "La protección de las infraestructuras críticas" [en línea], *Instituto Español de Estudios Estratégicos,* 021/2011, 27 de julio de 2011, p. 2, Disponible en: http://bit.ly/2bT1aLv.

[92] *Ibíd.*

precisos para hacerle frente, sino que ayuda a comprender la visión que se tiene sobre determinada amenaza.

En este caso, Estados Unidos particulariza en la ciberguerra con la seguridad cibernética en donde enfatiza los peligros potenciales en el ciberespacio, de acuerdo con el QHSR 2014, dicha seguridad se puede delimitar así: la ciberseguridad es la protección de la infraestructura crítica a través de contrarrestar las amenazas y riesgos informáticos, el desarrollo de tecnología avanzada, así como el desarrollo de leyes informáticas, la investigación de delitos cibernéticos, y la apertura y salvaguarda de Internet.[93]

Aunado a lo anterior, aquellas amenazas que ponen en riesgo la salvaguarda de las personas, las instituciones, el gobierno y su infraestructura crítica, son las mismas a las que el gobierno les ha considerado parte de la ciberguerra, como tal, ésta refiere a lo relacionado con el espionaje o robo de información de todo lo relacionado con la guerra misma, a saber, el número de armamento, la tecnología, los efectivos, etc., en otras palabras, la capacidad de guerra del Estado.

Sin embargo, como antes se mencionó, la guerra no se limita a las armas, mucho menos en la ciberguerra, sino que ahora todo lo que represente la posibilidad de dañar o afectar al Estado a través del ciberespacio, como los ataques a sus infraestructuras críticas, el ciberespionaje, la infiltración de información, se considera como una amenaza, pudiendo tener mayores alcances de daño.

Es importante destacar el liderazgo que el Departamento de Seguridad Nacional desempeña junto al gobierno federal, así como los esfuerzos con el sector privado por prevenir, mitigar y responder a las amenazas cibernéticas. Otro elemento esencial es el ejecutivo federal de quien entre sus aportaciones importantes son las siguientes leyes: *Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity* (Orden Ejecutiva 13636, la mejora de la Infraestructura Crítica de Ciberseguridad) y *Presidential Policy Directive (PPD) -21 Critical*

[93] Elaboración propia.

Infrastructure Security and Resilience (Política de la Directiva Presidencial de la Seguridad de la Infraestructura Crítica y Resiliencia).[94]

> "Éstas refuerzan la necesidad de un pensamiento holístico acerca de la seguridad y gestión de riesgos, como sus nombres lo dicen, están encaminadas hacia una red y sistema de seguridad y resiliencia, así como a mejorar la eficiencia y efectividad del trabajo estadounidense por asegurar la infraestructura crítica y hacerla más resiliente."[95]

La EO 13636, se enfoca en el desarrollo "neutral" tecnológico, en el fomento de prácticas de seguridad cibernética, en el aumento y calidad de la información de las amenazas, incorpora una estricta privacidad y las libertades civiles de protección en todas las áreas para asegurar la infraestructura crítica, asimismo, explorar la regulación existente del uso para promover la seguridad cibernética.

Mientras que la PPD-21, busca elaborar una capacidad de conocimiento de aspectos físicos y cibernéticos en la situación en que funciona la infraestructura, así como conocer sus fallas en cascada, en el aspecto público y privado evaluar y madurar dicha asociación, actualizar el Plan Nacional de Protección de Infraestructuras, desarrollar la investigación en este rubro y un plan de desarrollo.

Estas leyes muestran el compromiso del ejecutivo federal para la fortificación de los sectores público y privado respecto al desarrollo de las "armas" contra la ciberguerra, con el fin de hacerle frente a las amenazas del ciberespacio, es decir, llevar a cabo la defensa nacional, que va desde lo físico y lo virtual, pasando por todas las esferas de la administración gubernamental.

Es claro que los esfuerzos en todos los niveles de gobierno destacan que la seguridad cibernética es una de las más importantes para la nación, lo que representa un real compromiso y coordinación para el desarrollo de las herramientas, la obtención de información y la formación de capacidades requirentes.

---

[94] *EO 13636, PPD -21* [en línea], Homeland Security, Disponible en: http://1.usa.gov/25VQRKO.
[95] *Óp. cit.*

Empero que no haya una definición de ciberguerra *per se*, el gobierno de los Estados Unidos ha demostrado a través de sus documentos oficiales la necesidad y la responsabilidad de afrontar, prevenir y aminorar los peligros a los que se encuentra susceptible en el ciberespacio a través de la ejecución efectiva de planes de acción y políticas específicas.

Así, la ciberseguridad es una tendencia en el gobierno estadounidense, en sus políticas y leyes. De manera que, su identificación y delimitación resulta indispensable a la hora de enfrentar las amenazas cibernéticas, así como para evaluar la vulnerabilidad que poseen frente a ellas.

2.1.2 La ciberguerra como amenaza a la seguridad nacional

El dominio cibernético de las computadoras y las actividades electrónicas relacionas es un entorno complejo diseñado por el hombre, y los adversarios humanos son resueltos e inteligentes. Joseph Nye dice que a diferencia del desarrollo de embarcaciones o fuerzas de operación de dominio naval que le permite influencia a Estados Unidos, las barreras en el dominio cibernético son tan bajas que actores no estatales y hasta pequeños estados pueden desempeñar un papel importante en el conflicto bélico con una baja inversión económica.[96]

A medida que la tecnología de la información se convierte en cada vez más integrado con las operaciones de infraestructura física, existe un mayor riesgo de eventos a gran escala o de graves consecuencias que podría dañar o alterar el estilo de vida norteamericano y la economía.

La existente dependencia a los sistemas cibernéticos de los Estados crea una fuerte vulnerabilidad que puede ser utilizada y aprovechada por oros actores, sean estatales o no estatales para atacar en áreas fundamentales del Estado, como actividades militares, económicas, financieras, entre otras. Y es precisamente en

[96]Nye Joseph*, Cyberwar and peace* [en línea], Disponible en: http://bit.ly/1LMaqx9.

este espacio donde se crea la máxime de vulnerabilidad, donde Estados Unidos lidera la utilización de la estructura cibernética militar y social propiciando así, sea más propenso a un ataque, y que el ciberespacio se haya convertido en una fuente importante de inseguridad porque, en esta instancia del desarrollo tecnológico, allí la ofensiva prevalece por sobre la defensa.

Nye en su libro *The Future of Power e*stablece que la desviación del poder es uno de los grandes giros políticos sobre todo en el ciberespacio. El control de los espacios es uno de los objetivos fundamentales de los países más grandes y poderosos, el ciberespacio es uno en el cual no hay dominio.

Expuesto lo anterior, se puede decir que el control de los espacios es una constante que se ha reflejado a través de la historia entre los países, sin importar el espacio del que se trate, es por ello que se ha desatado guerras. No obstante, el ciberespacio es un todo que controla y contiene mucha información y datos en todo el mundo, por lo que en el momento en que se llegara a construir un control ciberespacial, no sólo desataría una tercera o cuarta guerra mundial, sino que tendría el control absoluto de todos los medios de control.

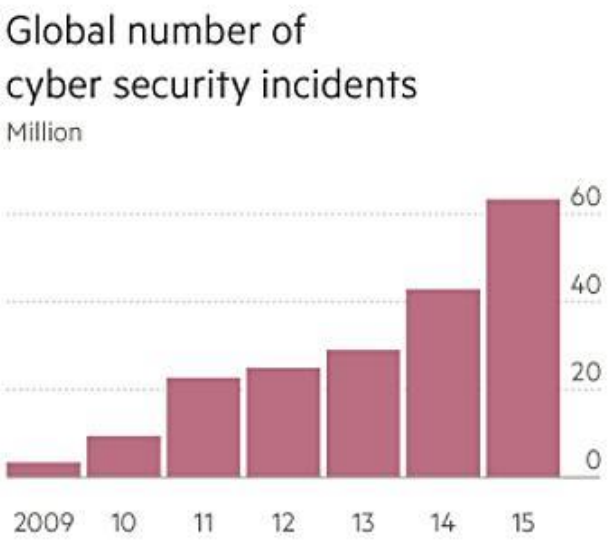
Empero, es por eso que existen y han surgido nuevos actores que van contra del orden establecido, y que ponen en desafío el poder de los países mejor capacitados, en perjuicio de los mismos.

El hecho de que Estados Unidos haya hecho pública la preparación de sus Fuerzas Armadas y de toda su infraestructura a favor de la defensa de la nación en contra de la ciberguerra, representa para sus ciudadanos y el resto del mundo una respuesta ante dicha amenaza, convirtiendo a ésta una de sus prioridades.

Asimismo, el reconocimiento de la existencia de la ciberguerra como una amenaza importante para nación, demuestra la capacidad del gobierno estadounidense para hacerle frente, junto con las instituciones correspondientes sin

importar las consecuencias. Por ejemplo, ello se refleja en el aumento del personal en materia cibernética de 1 800 en 2014 a 6 00 en 2016.[97]

De acuerdo con el Foro Económico Mundial, han incrementado el número de ataques cibernéticos, como se muestra en la siguiente gráfica:

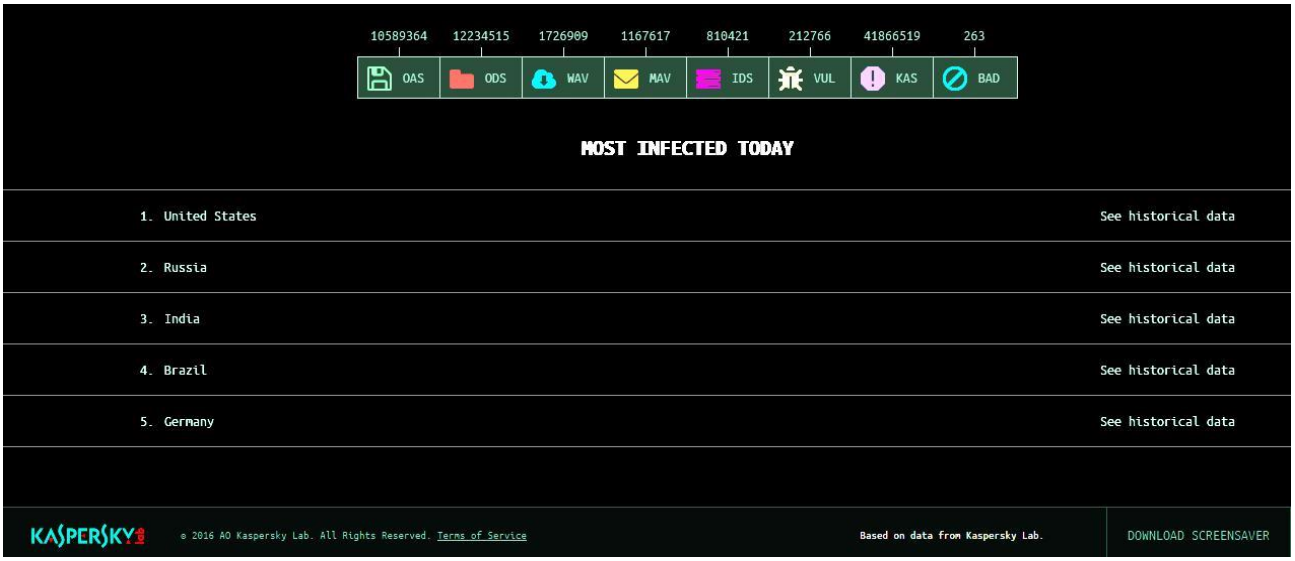


Gráfica 2.1 Número global de incidentes de ciberseguridad. Donde se muestra dicho número por año. Fuente: *Who are the cyberwar superpowers?*, World Economic Forum, Disponible en: http://bit.ly/1NusZlu.

En la cual, de 2009 al 2015 aumentaron aproximadamente 55 millones los ataques. Y diversos países, como Estados Unidos, China, Rusia, Israel y Reino Unido, han sido protagonistas en la respuesta a dichos ataques cibernéticos.

[97] *Who are the cyberwar superpowers?* [en línea], World Economic Forum, 4 de mayo de 2016, Disponible en: http://bit.ly/1NusZlu.

Una demostración actual a lo anterior, es la tabla 2.2, presentada por la página web Kaspersky, donde muestra los países más infectados por ciberataques en septiembre de 2016, presentando a Estados Unidos, Rusia, India, Brasil y Alemania en orden descendente



-Tabla 2.2. Fuente: https://cybermap.kaspersky.com/stats/.

Para noviembre de 2016, la tabla muestra los siguientes países:

Fuente: https://cybermap.kaspersky.com/stats/.

2.2 La Estrategia de Seguridad Nacional de Estados Unidos de América

2.2.1 La Estrategia de Seguridad Nacional 2015

Los Estados al identificar y definir sus principales riesgos y amenazas en el ciberespacio configuran y refuerzan su seguridad a través de un conjunto de acciones y estrategias para la defensa de sus estructuras cibernéticas. La posibilidad de ser atacado cibernéticamente cada vez es más plausible debido a la dependencia que se ha generado, principalmente entre las instituciones y los individuos además de que hace más fácil la vida y la organización de las mismas ya sea a nivel individual o federal.

Asimismo, las amenazas se diversifican y la seguridad de los Estados, en el caso de la ciberguerra, se ve transgredida, por lo tanto lo que las principales potencias mundiales buscan es encontrar estabilidad dando paso a la creación de una ciberestrategia. Ésta "es una constatación más de la necesidad de fijar una base común que pueda hacer frente a un ataque o una acción delictiva sobre ciudadanos, empresas o estados, perpetrada parcialmente o en su totalidad por medios digitales."[98]

En la ciberseguridad,

> "(…) a fin de evitar impactos no previstos derivados de la falta de madurez regulatoria y procedimental y del creciente número de amenazas cibernéticas (…), los Estados soberanos comienzan a disponer de estrategias integrales de ciberseguridad a través de una hibridación jurídico-técnica, tanto en el entorno empresarial como sectorial. (…) la gestación de dichos documentos ha estado rodeada de una creciente expectación ya que otorgan, de forma general, tanto el reconocimiento estratégico que tiene el ciberespacio para los diversos países como el posicionamiento en este nuevo entorno virtual."[99]

[98] Solé Pascual Carles y Adolfo Hernández, *Estrategias nacionales de cibeseguridad en el mundo* (en línea), en redseguridad.com, Disponible en: http://bit.ly/1CAB6cJ.
[99] *Idem.*

Para febrero de 2015, la Casa Blanca dio a conocer la Estrategia de Seguridad Nacional (NSS, por sus siglas en inglés) cuyo texto se centra en la reafirmación del liderazgo de Estados Unidos frente al mundo teniendo una visión futurista, es decir, tomando en cuenta los riesgos y amenazas de la humanidad para posteriormente poder afrontarlos satisfactoriamente.

La NSS establece cuatro grandes intereses nacionales que atienden a las bases de la visión de seguridad multidimensional: seguridad (de la nación, de sus ciudadanos, aliados y socios), prosperidad (económica ante el sistema económico internacional que le genere oportunidades), valores (universales dentro y fuera de la nación) y orden internacional (a través de una base de reglas promovidas por Estados Unidos como líder).

Aunado a lo anterior, ha de señalarse que dichos intereses nacionales son necesarios para lograr el éxito en el desarrollo nacional porque abarcan todos los rubros de la administración que competen y atañen a las instituciones y las personas, aún más si se trata de lograr la paz y estabilidad del bien común.

Así con esto, Estados Unidos manifiesta ante el mundo a través de la National Security Strategy (NSS), nuevos desafíos a la seguridad frente los cuales, mantendrá sus capacidades y los fortalecerá con la confluencia de voluntades. Es importante retomar la NSS de 2010 donde se dio lugar a las "amenazas asimétricas" provenientes de Estados o actores no estatales que operan en diversos escenarios de conflicto en el mundo[100], para las cuales se tiene que desarrollar las capacidades necesarias para enfrentarlas, en asimetría con la actualidad, Estados Unidos no dudará en fortalecerse y emprender la defensa.

La multiplicidad de las amenazas se convierte, hoy en día, para el gobierno estadounidense una prioridad y un punto de enfoque. El rol y la capacidad que el Estado posee son sin duda de gran peso, por lo tanto, se mantiene al tanto de los alcances que puedan llegar a tener dichas amenazas en su seguridad y la de la humanidad como líder mundial. Es por eso que la especialización de sus fuerzas

[100] Yopo Boris, *La nueva estrategia de seguridad de Estados Unidos* [en línea], Friedrich Ebert Stiftung, julio de 2010, pág. 4, Disponible en: http://bit.ly/1ZzRzHN.

armadas resulta necesario. Hacer frente al enemigo no sólo físicamente sino ahora virtualmente representa un gran reto para el gobierno y las instituciones correspondientes.

La protección, defensa y prevención como parte de la ciberestrategia estadounidense atiende a las amenazas como espionaje, sabotaje de servicios, terrorismo informático, operaciones de información y robo de información secreta; acciones delincuenciales cibernéticas que pueden tener efectos caóticos en la organización, estructura y estabilidad de cualquier nación y aún más Estados Unidos por tener una infraestructura muy desarrollada.

Por ende, el Departamento de Defesa de Estados Unidos (DoD, por sus siglas en inglés *Department of Defense*) brazo derecho del ejecutivo y departamento encargado de la supervisión de agencias y funciones del gobierno relativas a la seguridad nacional, es quien tiene a su cargo la creación de una ciberestrategia. Ésta cuyo propósito está encaminado a:

> "(…) guiar el desarrollo de las fuerzas cibernéticas (del DoD) y fortalecer la defensa y ciberdisuación, se centra en la construcción de las capacidades y organizaciones cibernéticas durante tres misiones primarias del DoD: defender redes, sistemas e información, defender el territorio estadounidense y los intereses nacionales contra los ataques cibernéticos de importancia significativa, y proporcionar apoyo cibernéticos a los planos operativos y de contingencia militar."[101]

[101]United States The Departament of Defense [en línea], Disponible en: http://1.usa.gov/1ZRWdDG.

2.2.2 La ciberguerra en la Estrategia de Seguridad Nacional

El 17 de abril de 2015, Estados Unidos dio a conocer la nueva estrategia de seguridad cibernética del gobierno de Barack Obama con la finalidad de disuadir ciberataques. En medio del gran crecimiento y necesidad que ha generado la red de sistemas y datos, llamada Internet, Estados Unidos reconoce su dependencia a ésta debido a que es una herramienta que ayuda a llevar a cabo bienes y servicios en cualquier parte del mundo, además de llevar y traer conocimiento e información que de otro modo carecen de acceso.[102]

Sin embargo, asimismo hace énfasis en la cantidad de amenazas en el ciberespacio a los que dicha dependencia, hace vulnerables a todos aquellos que tienen contacto con Internet, y sobre todo a su infraestructura crítica. En ella, manifiesta la necesidad de crear un medio de defensa en el ámbito ciberespacial en contra de aquellas amenazas que ponen en riesgo la integridad del Estado estadounidense.

La estrategia establece cinco objetivos estratégicos y establece objetivos específicos para el Departamento de Defensa para lograr en los próximos cinco años y más allá Además cuenta con tres ejes rectores importantes, a saber:

1. Incremento de sofisticación y severidad en las ciberamenazas a los intereses de Estados Unidos incluyendo redes, información y sistemas del Departamento de Defensa

Lo que crea una perspectiva a largo plazo que ayudará a prever problemas futuros y por ende, a crear los mecanismos de respuesta a favor de la seguridad y defensa.

[102] *The DoD CyberStrategy,* The Department of Defense [en línea], Disponible en: http://1.usa.gov/1iUMziZ.

2. Nueva estrategia de pensamiento (inteligencia) en la organización y plan de defensa contra ciberataques en concierto con otras agencias del gobierno

El elemento de un nuevo pensamiento o generación de inteligencia le permitirá al gobierno estadounidense avanzar y ver a futuro en la creación de una ciberestrategia, con todas las medidas, sean jurídicas, de Fuerzas Armadas, legislativas, etc.

3. Construcción de la Fuerza Cibermisión (CMF, por sus siglas en inglés *Cyber Mision Force*) cuyo objetivo es llevar a cabo las cibermisiones del Departamento de Defensa. Esta estrategia brinda una clara guía para el desarrollo de la CMF.

Es importante señalar la importancia que dicha institución y sus integrantes cobran en el cumplimiento de su misión cibernética, ya que la generación de profesionales en la materia, harán más fácil y seguro el éxito de sus objetivos y metas.

Asimismo, es preciso mostrar que la estrategia del Departamento de Defensa se apoya en el sector privado. El DoD se encarga de atraer el mejor talento, ideas y la mejor tecnología para el cumplimiento de sus objetivos. En particular, en dicha en la cooperación y coordinación se destacan diferentes centros de producción pensantes (*Think Tanks*), tecnológicos y de seguridad, los cuales le brindan mayor capacidad y fortaleza de preparación y ataque. Como resultado, estas instituciones hacen de Estados Unidos una nación de innovación, de ahí que se encarguen del diseño y la creación de las redes del ciberespacio, proveen servicios de ciberseguridad, investigación y desarrollo de capacidades avanzadas.

Como se ha dicho, la ciberestrategia se caracteriza por la estrategia de la disuasión. El DoD asume que la disuasión en los ciberataques en los intereses estadounidenses será lograda a través de la totalidad de las acciones por parte del

Estado, incluyendo políticas declaratorias, indicaciones sustanciales, capacidades de alerta, postura defensiva, procedimientos de respuestas eficaces y sobretodo de la resiliencia de las redes y sistemas estadounidenses.

Todo lo anterior necesario para mostrarse y estar mayormente capacitado y preparado ante los desafíos de sus amenazas cibernéticas, no sólo militar y tecnológicamente sino también respecto a su posición mundial para la protección de sus ciudadanos, sino también de sus aliados y socios.

Respecto a los objetivos estratégicos y objetivos clave de implementación se enumeran los siguientes:

1. Construir y mantener fuerzas y capacidades listas para conducir operativos en el ciberespacio. Éste implica el entrenamiento del personal del DoD, la construcción de organizaciones efectivas, comando y control de sistemas, así como el desarrollo total de las capacidades que requiere el DoD para operar en el ciberespacio. Y sus objetivos clave son:

    Construir capacidades técnicas para operaciones, incluir una unificada e integrada plataforma operacional

    Acelerar la investigación y desarrollo para proveer al DoD con una ventaja significativa en el desarrollo de tecnologías para defender los intereses estadounidenses en el ciberespacio

    Evaluar la capacidad del CMF para lograr los objetivos de la misión cuando confronten con múltiples contingencias

Al evaluar este objetivo, se puede decir que requiere de una fuerte inversión financiera e intelectual, lo que se traduce en la generación de tecnología de la información para la protección de las redes, así como de las capacidades operacionales.

Asimismo, la consecución de esta objetivo implica el posible surgimiento de tanques pensantes y la creación de nuevas doctrinas que generen ideologías en términos de interoperabilidad por las instituciones, para que en conjunto encuentren

una posible solución o respuesta a desafíos por parte de las amenazas en el ciberespacio.

2. Defender la red de información del DoD, asegurar los datos del DoD y mitigar los riesgos de las misiones del DoD. Donde el DoD debe identificar, priorizar, y defender sus más importantes redes y datos para que así pueda realizar las misiones satisfactoriamente. Sus objetivos clave son:

    Construir el Entorno de Información Conjunta con una arquitectura de seguridad única para cambiar el enfoque de protección de las redes y sistemas de servicio específico para asegurar la empresa DoD

    Implementar una capacidad para mitigar todas las vulnerabilidades conocidas que presentan un alto riesgo al DoD

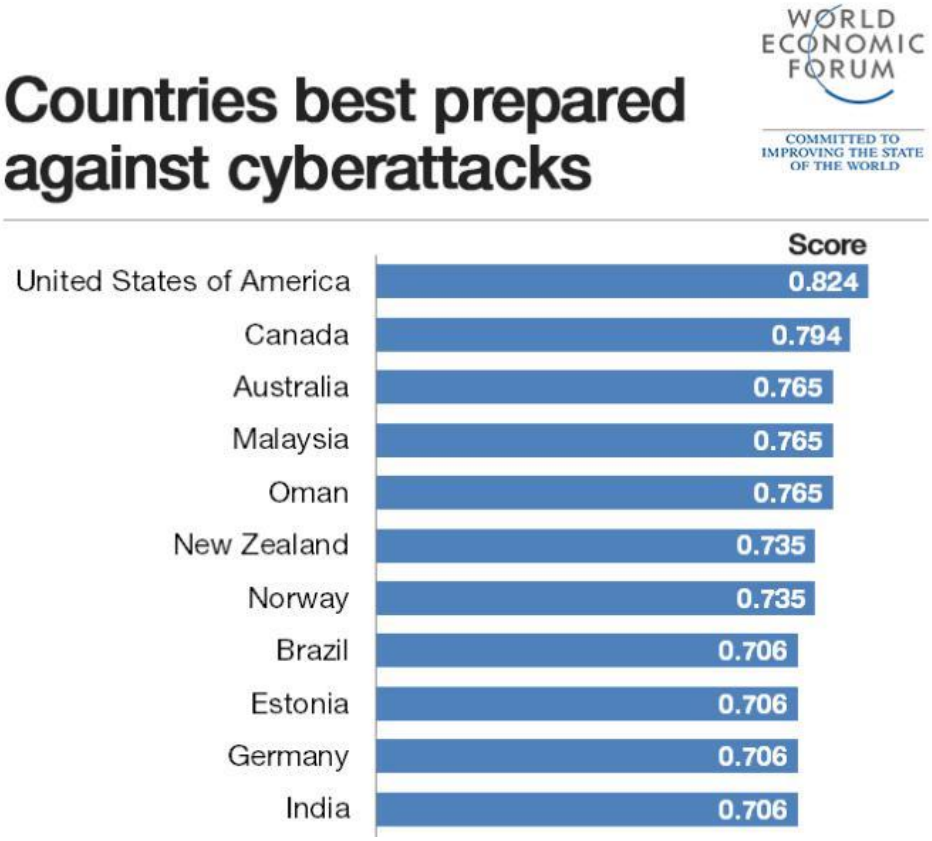
    Identificar, planear y defender las redes y el soporte clave de las misiones del DoD

    Construir una defensa por capas alrededor de la Base Industrial de Defensa a través de una mejor rendición de cuentas, estándares de ciberseguridad, contrainteligencia, y grandes esfuerzos de gobierno para contrarrestar el robo de propiedad intelectual.

Este objetivo refuerza los empeños por la construcción de la infraestructura crítica fuerte, así como de los medios informáticos que coadyuven en la protección de las redes y los sistemas de operación de Internet. Éstos son necesarios para el éxito de los objetivos clave del anterior objetivo estratégico y de los demás, debido a que es necesaria la interoperabilidad de los sistemas para reaccionar ante las amenazas.

De acuerdo con la gráfica 2.3 presentada por el Foro Económico Mundial, los países mejor preparados contra los ciberataques son los siguientes:

Gráfica 2.3 Los paises mejor preparados contra los ciberataques. Donde se muestra su posición de acuerdo a la puntuación asignada por el Foro Económico Mundial.
Fuente: *Why the worlds hould pay attention to cyberrisks* [en línea], World Economic Forum, Disponible en: http://bit.ly/2al1tjl.



3. Estar preparados para defender el territorio nacional y sus intereses vitales de disruptivos y destructivos ciberataques de consecuencias significantes. El DoD debe trabajar conjuntamente con el sector privado, naciones aliadas y socios para impedir y si es necesario defender a Estados Unidos de ciberataques, desarrollando su inteligencia, alerta y capacidades operacionales pata mitigar sofisticados y maliciosos ciberataques. Los objetivos calve son:

    Desarrollar inteligencia y capacidades de alerta para anticipar amenazas

    Asociarse con organizaciones interagenciales para preparar la defensa de la nación en el ciberespacio

Trabajar con el Departamento de Seguridad Nacional (DHS, por sus siglas en inglés *Department Homeland Security*) para desarrollar mecanismos continuos y automatizados para el compartimiento de información

Evaluar la postura de ciberdisuasión del DoD y proveer recomendaciones para su mejorar

Este objetivo es clave para el desarrollo de las armas cibernéticas y junto con ello, la conformación de un equipo de seguridad de alto nivel. Es decir, la mancuerna del gobierno federal con el sector privado significa la unión de habilidades y productos de inteligencia que genera un frente fuerte ante las amenazas. Lo que significa que el gobierno se provee de los medios necesarios para el éxito de sus objetivos.

4. Construir y mantener ciberoperaciones viables y planear usar estas opciones para controlar la escalada del conflicto, y dar forma al entorno del conflicto en todas sus etapas. De acuerdo con éste, el DoD debe proveer al presidente con un amplio rango de opciones para manejar la escalada del conflicto. Como parte del rango de herramientas disponibles para Estados Unidos, el DoD debe desarrollar ciberoperaciones e integrar estas opciones dentro de los planes departamentales. El DoD desarrollará las cibercapacidades para lograr los objetivos de una seguridad clave con precisión, y minimizará las pérdidas de vida, y destrucción de propiedades.

Sin duda, el papel del Ejecutivo Federal para la toma de decisiones es imprescindible, ya que de esta manera, dirigirá el rumbo de las acciones siempre a favor y ventaja de la nación. Sin olvidar que éste puede recibir asesoría y recomendaciones o notas por parte de los expertos en la materia.

5. Construir y mantener robustas alianzas y asociaciones internacionales para disuadir amenazas comunes e incrementar la seguridad y estabilidad

internacional. Donde el DoD busca construir una capacidad de asociación en la ciberseguridad y ciberdefensa.

> La creación de capacidades de asociación se enfocará en regiones de prioridad, incluyendo a Medio Oriente, Asía-Pacífico y Europa. El DoD continuará adaptivo y flexible para construir las alianzas que seas necesarias.

Por último, dichas alianzas significan la creación de dos bandos: “amigos o enemigos”, quienes por el lado positivo “amigos” o asociados, representarán una posible protección en materia cibernética, es decir puede haber intercambio de información o de capacidades para la ciberseguridad de los Estados. Por otra parte, todos aquellos países que no simpaticen en la cooperación con Estados Unidos, podrían ser considerados como principales focos de amenaza respecto a los ciberataques.

Así, en el documento se muestra que Estados Unidos se muestra abierto a los nuevos retos que el mundo del siglo XXI genera, además de querer reafirmar su papel de liderazgo respecto a sus capacidades de defensa frente al mundo, sin ser en el ciberespacio la excepción.

Cabe destacar que dicha estrategia sugiere una nueva generación de tecnologías y preparación intelectual y de nuevas capacidades frente el surgimiento de nuevos actores estatales y no estatales, que ahora cobran fuerza bajo los riesgos que representan, en este caso, las amenazas cibernéticas.

Por ende, y bajo la capacitación de sus Fuerzas Armadas, el gobierno estadounidense espera la prosperidad en la seguridad de sus estructuras cibernéticas, en cooperación con instituciones del sector privado, organizaciones y agencias gubernamentales que prometen trabajar conjuntamente para afrontar el reto.

Asimismo, por mencionar algunos, se destaca que la esfera política y la esfera económica son las afectadas en el marco de las amenazas cibernéticas. La

primera por el robo de información secreta, sabotaje servicios, espionaje, entre otros, y la segunda fundamentalmente por el robo de propiedad intelectual.

No debe olvidarse que los esfuerzos del gobierno estadounidense no sólo se basan en la diversificación en sus Fuerzas Armadas quienes actúan en responsabilidad con las leyes emitidas, por ello, también luchan por lograr cambios en el marco jurídico nacional en materia de ciberseguridad para proteger a la nación, a sus instituciones públicas y privadas, así como el importante sector empresarial que sostiene y fortifica la economía estadounidense, respecto de la privacidad y las libertades civiles ante cualquier amenaza.

2.2.3 El fortalecimiento de las capacidades estadounidenses

Consideremos ahora, que la estrategia de seguridad cibernética hace hincapié en la capacidad del ejército para tomar represalias con armas cibernéticas con lo que se espera disuadir ataques. Como resultado, su trascendencia radica en la cada vez mayor capacidad del ejército estadounidense para combatir y prevenir las amenazas en el ciberespacio.

De acuerdo con el Secretario de Defensa de Estados Unidos de América, Ash Carter: “Estados Unidos debe ser capaz de declarar o mostrar capacidades de respuesta eficaces para disuadir a un adversario de iniciar un ataque”.[103] Lo que significa que la preparación de Estados Unidos es y será superior respecto a cualquier otro. Debido al desarrollo de las nuevas tecnologías y de la capacidad del individuo para inmiscuirse en ellas, resulta evidente que el alcance de los daños a las personas, gobiernos y naciones con el tiempo se maximiza.

Desde el 2010 oficialmente se activó el Ciber-comando de Estados Unidos (*USCYBERCOM, por sus siglas en inglés*), un comando subalterno bajo el

[103] *Estados Unidos presenta hoy nueva estrategia de ciberseguridad* [en línea], en Mediatelecom, 24 de abril de 2015, Disponible en: http://bit.ly/1MWgfHb.

Comando Estratégico de Estados Unidos. "El USCYBERCOM planifica, coordina, sincroniza y realiza actividades para dirigir operaciones militares en el ciberespacio y la defensa de determinadas redes informáticas del Departamento de Defensa."[104]

Más aún el USCYBERCOM trabaja con el Segundo Ejército o ARCYBER quienes dirigen y llevan a cabo las ciberoperaciones y de información, autorizadas o dirigidas para generar la libertad de acción o negarla a los adversarios de la nación. Expuesto lo anterior, se puede decir que la especialización del ejército estadunidense pone en evidencia la el compromiso de asegurar el ciberespacio y mantenimiento de una internet abierta, interoperable, segura y confiable, además de la capacidad de respuesta efectiva e inmediata, sea ofensiva o defensiva.

Cabe destacar que el trabajo de estas instituciones depende fundamentalmente del compromiso de militares y civiles y del apoyo de la Agencia de Seguridad Nacional y el Servicio Central de Seguridad (*CSS, por sus siglas en inglés Central Security Service)* quienes "lideran el gobierno de Estados Unidos en la criptología que abarca señales de inteligencia (SIGINT) e información de garantía de productos y servicios (IA), y permiten operaciones de la red de computadoras (CON) con el fin de obtener ventaja de decisiones para la nación y (…) aliados en todas las circunstancias."[105]

Dicha preparación y especialización del ejército estadounidense refiere a la Revolución Tecnológica Militar (RTM)[106] la cual denota los esfuerzos para cumplir sus objetivos y utilizar los medios necesarios para la consecución de los mismos. Los nuevos hallazgos tecnológicos son utilizados para aventajar y ganar en el campo de batalla, sólo que ahora el campo no es físico sino virtual. De la misma manera este desarrollo conlleva a la creación de nuevas armas de guerra, o bien,

---

[104] *Texto cifrado en el logo del CYBERCOM (Actualizado)* [en línea], Disponible en: http://bit.ly/1QuEwCZ. [105] National Security Agency [en línea], Disponible en: http://1.usa.gov/1ZLzOFp.

[106] Es un concepto empleado por algunos pensadores militares soviéticos, en especial por el mariscal Nicholas Ogarkov entre finales de la década de 1970 y principios de la de 1980 para referirse a los hipotéticos efectos que tendría sobre el campo de batalla la aplicación de los avances tecnológicos en materia de inteligencia, comunicaciones, mando y control, y ataque de precisión. Jordán Javier, *Innovación y revolución de los asuntos militares: una perspectiva no convencional* [en línea], International Security Studies Group, Disponible en: http://bit.ly/1UnbWq5.

lo referente a la Revolución de los Asuntos Militares (RAM)[107], donde para ser una auténtica revolución los avances tecnológicos debían ir en paralelo a cambios profundos en la doctrina, adiestramiento y orgánica de las Fuerzas Armadas.[108]

"La RMA es hija de la era de la información. Su objetivo es ante todo levantar 'la niebla de la guerra'. La tecnología es la materia prima que se consume en los campos de batalla."[109] Con ello, los ejércitos altamente profesionalizados e instruidos y armados con el material más avanzado, serán quienes podrán vencer al enemigo.

Es decir, se crea una nueva concepción, adiestramiento y empleo del poder militar, o bien, un nuevo modelo militar. Dicha Revolución también se expresa en innovaciones de tácticas en el campo de acción, generación de doctrinas y, evidentemente, de tecnología más avanzada.

De acuerdo con

> "(…) el historiador militar Clifford Rogers (…) (se) señaló que una Revolución Militar era un fenómeno que se manifestaba cuando importantes cambios sistémicos en la esfera cultural, política, social, demográfica o económica se articulaban de tal forma que lograban transformar completamente el Estado, la sociedad y su relación con la guerra."[110]

Expuesto lo anterior, la armonización de los intereses nacionales con los asuntos militares responde a una restructuración profunda para una defensa satisfactoria, aún más acompañada de los últimos avances en tecnologías de la información, que en el caso de la ciberguerra, resultan imprescindibles su

[107]Concepto introducido a principios de la década de 1980 por Andrew W. Marshall, director de la Oficina de Net-Assessment del Pentágono. *óp. cit.*

[108]*óp. cit.*

[109] Molina Rabadán, David, *La Revolución de los Asuntos Militares (RMA) en el contexto de la era de la información* [en línea], Revista de Estudios Ciencias Sociales y Humanidades, nùm. 14, 2005, pp.78-79., Disponible en: http://bit.ly/2aACasw.

[110]Colom Piella, Guillem y Josep Baqués Quesada, *El concepto de la Revolución Militar y su empleo en los estudios estratégicos* [en línea], Disponible en: http://bit.ly/1TwLyYZ.

conocimiento, uso y transformación. Además de que representa al adiestramiento efectivo para el cumplimiento de las misiones asignadas, es decir, las cibermisiones.

Claro es el ejemplo del Secretario de Defensa, Ash Carter, quien tiene la responsabilidad de mandar órdenes a los centros de inteligencia competentes y a las empresas para que creen nuevos dispositivos para la defensa de su espacio cibernético.

Simultáneamente, los cambios generados en el campo militar, como en el tecnológico, en lo político y en lo económico, también recaen en la sociedad, quienes son susceptibles a los cambios generados en el modo de concebir la guerra, las amenazas y su adoctrinamiento.

Cabe destacar que la naciente capacitación militar en el campo ciberespacial, representa para Estados Unidos la oportunidad de fortificarse política y militarmente, debido a que ésta eleva su capacidad de defensa, estatus y poderío frente a otros países como China, Arabia Saudita, Reino Unidos, Rusia, y entre otros, quienes buscan ponderarse cada vez en el sector de Defensa. Es importante señalar que el fortalecimiento de Estados Unidos depende del apoyo y coordinación de diversos agentes para lograr su defensa en el ciberespacio, como lo son sus instituciones gubernamentales, agencias federales públicas y privadas, así como de su población.

Capítulo 3. Estados Unidos de América en el contexto de la ciberguerra

La ciberseguridad sufre de constantes cambios y crecimientos a consecuencia de los ataques cibernéticos y su plena diversidad. Estados Unidos de América ha emprendido la lucha en contra de las amenazas cibernéticas a favor de la protección del Estado, incluyendo cualquier tipo de ente sea público o privado cuyas funciones son vitales para salvaguardar su integridad y correcto funcionamiento. Es misión y visión de Estados Unidos mantener su liderazgo mundial, por lo que frente a los riesgos cibernéticos se han dado a la tarea de implementar e innovar medidas para ajustarse a este nuevo desafío y generar un marco de seguridad cibernética.

En el presente capítulo se estudiará a los Estados Unidos de América a partir de las acciones estatales e iniciativa privada que se han implementado a favor de su defensa y seguridad cibernética y cuáles han sido sus repercusiones.

3.1 La ciberestrategia de Estados Unidos de América. Planeación e inversión.

De acuerdo con el Presupuesto de Gastos de Defensa para 2015 del Global Firepower[111], Estados Unidos de América ocupa el primer lugar de 126 países, como máximo inversor en materia de defensa con una cifra de $581 mil millones de dólares, del cual se desprenden diferentes áreas como la tecnológica, la naval, la aérea, la armada, entre otros, para su desarrollo, así como también ahora el área cibernética.

[111] *Presupuesto de Defensa por país* [en línea], Global Firepower, Disponible en: http://bit.ly/1uno1zq.

Detrás de esta inversión, se encuentran los postulados gubernamentales que le dan un sustento a dichas acciones económicas y financieras, y es que Estados Unidos se ha destacado por mantenerse al tanto de los nacientes peligros y desafíos del escenario internacional, asimismo como protector de los más débiles en el mundo. Es por eso que para mantener el orden y control de las amenazas tanto dentro como fuera del país, es necesaria la preparación y reforzamiento de la Defensa nacional.

Los esfuerzos se ven reflejados en la creación de medidas: legales, técnicas, de organización y de construcción de capacidades. Es importante identificar las tareas que corresponden al ámbito jurídico-político, y aquellas que van encaminadas a la ejecución en Fuerzas Armadas. Aquellas iniciativas y Órdenes Ejecutivas que el gobierno ha impulsado a favor de la seguridad cibernética, manifiestan la voluntad y capacidad enfrentar las amenazas que atentan contra la misma.

Dichas medidas demuestran los sectores o áreas en los que Estados Unidos pudiera verse transgredido en su seguridad e integridad. Ejemplo de ello, es la creación del Marco de Ciberseguridad a través de la Orden Ejecutiva 13636 emitida por el Presidente y celebrada en Maryland, en febrero de 2013, que trabaja por la mejora de las infraestructuras críticas de ciberseguridad.

La importancia recalcada en la infraestructura cibernética refleja la prioridad de la nación por trabajar en ella y hacerla competitiva y fuerte ante cualquier eventualidad. Para 2014, el presidente Barack Obama a través de la “Declaración presidencial en el marco de la Ciberseguridad” reconoció que la seguridad cibernética se ha convertido en una de las prioridades del gobierno estadounidense debido a que las amenazas cibernéticas representan uno de los más graves peligros para la seguridad nacional. Para ello, Obama dijo que:

> “Para una mejor defensa de nuestra nación (…), hace un año firmé (BO) una orden ejecutiva que ordena a la Administración a tomar medidas para mejorar el intercambio con el sector privado de la información, aumentar

> el nivel de seguridad cibernética a través de nuestra infraestructura crítica y mejorar la privacidad y las libertades civiles."[112]

Por lo anterior, se perfila la postura estadounidense respecto a su defensa contra las ciberamenazas, claro está que el trabajo gubernamental irá de la mano de la iniciativa privada para lograr juntos eficaz y eficientemente metas y objetivos.

Cabe destacar la relevancia que las plataformas cibernéticas e Internet tienen para el desarrollo y prosperidad económica e intelectual. No sólo se trata de cuidar las redes, sino de crear los medios necesarios que la crean segura, respecto a su interoperabilidad, fiabilidad y apertura. Es por eso que el gobierno estadounidense ha emprendido ya, medidas efectivas en materia de ciberseguridad para instruir a las autoridades correspondientes, entre las que destacan: la industria, la academia y las agencias federales e instituciones privadas para su gestión.

El gobierno federal ha creado instituciones especializadas entre las que destacan: el Instituto de Nacional de Estándares y Tecnología[113] (*National Institud of Standards and Technology, NIST por sus siglas en inglés)* la cual ha trabajado con el sector privado para desarrollar el Marco de Ciberseguridad cuya funcionalidad sirve para que las empresas estadounidenses puedan gestionar mejor el riesgo cibernético a la infraestructura nacional.

Dicho instituto ha sido dirigido asimismo por la OE 13636, en la cual hace pleno reconocimiento de las amenazas cibernéticas a la infraestructura crítica, en la sección 1, número 2:

> **"**Segundo. 2 *Infraestructura Crítica.* Tal como se utiliza en este orden, la infraestructura crítica plazo, los sistemas y activos, ya sea físico o virtual, tan vital para los Estados Unidos de que la incapacidad o destrucción de dichos sistemas y activos tendrían un efecto debilitante sobre la seguridad, nacional la seguridad

---

[112] *Statement by the President on the Cybersecurity Framework* [en línea], The White House, Disponible en: http://bit.ly/29pvewd.

[113] El NIST es uno de los laboratorios de ciencias físicas más antiguas de la nación. El Congreso estableció la agencia para eliminar un obstáculo importante a US competitividad industrial en el tiempo, una infraestructura de medición de segunda clase que iba a la zaga de las capacidades del Reino Unido, Alemania, y otros rivales económicos. Obtenido de *About the NIST* [en línea], NIST*,* Disponible en: http://bit.ly/29kUWmL.

económica, la salud pública o la seguridad nacional, o cualquier combinación de estos asuntos."[114]

Como parte de un esfuerzo por la apertura del control en las áreas más vulnerables ante las ciberamenazas, las políticas públicas y su coordinación, el intercambio de información, la protección a la privacidad y las libertades civiles son algunos de los apartados que contiene la dicha Orden para crear el Marco línea de base para reducir los riesgos a la infraestructura crítica, configurando así, la base para la adopción de futuras políticas e iniciativas.

Es así como Estados Unidos de América ha creado su ciberestrategia, reflejada en el Marco de Ciberseguridad, la cual según la OE 13636:

> Se basa en el rendimiento flexible y repetible, con prioridades y enfoque rentable, incluidas las medidas y controles de seguridad de la información, para ayudar a los propietarios y operadores de infraestructuras críticas identificar, evaluar y gestionar el riesgo cibernético.

Elementos necesarios para un adecuado funcionamiento, con precisión y exactitud acerca de cómo y dónde trabajar planes y estrategias en materia cibernética.

> Se centra en la identificación de las normas y directrices aplicables a la infraestructura crítica de seguridad intersectoriales.

Su importancia radica en la seguridad cibernética intersectorial cuya protección crea una cubertura amplia de la infraestructura, imperiosa para el cumplimiento de los objetivos de dicha orden ejecutiva.

> Identifica las áreas de mejora que debe abordarse a través de una futura colaboración con los sectores y organizaciones de desarrollo de estándares

[114] *La mejora de las infraestructuras críticas de ciberseguridad. Orden Ejecutiva 13636,* [en línea], Federal Registrer. The Daily Journal of the Unites States Goverment, Disponible en: http://bit.ly/1fnluyZ.

> particulares. Para permitir la innovación técnica y dar cuenta de las diferencias de organización, el Marco de Ciberseguridad proporcionará una guía que es tecnológicamente neutral y que permite a los sectores de infraestructura crítica para beneficiarse de un mercado competitivo de productos y servicios que cumplan con las normas, métodos, procedimientos y procesos desarrollados para la dirección riesgos cibernéticos.

Este punto aborda el área empresarial, un actor importante que en cooperación y colaboración con el sector público permite la formulación de nuevas fórmulas de defensa y protección, así como generación de tecnologías competentes.

> Incluye orientación para medir el desempeño de una entidad en la aplicación del Marco de seguridad cibernética.

La evaluación del desempeño es el recurso básico para mejorar la calidad de las medidas de seguridad, así como del cumplimiento de los objetivos.

> El Marco de Ciberseguridad incluye metodologías para identificar y mitigar los efectos del Marco de ciberseguridad y medidas de seguridad de información asociados o controles sobre el secreto comercial, para proteger la privacidad individual y las libertades civiles.[115]

"El enfoque priorizado, flexible, repetible y rentable del Marco ayuda a los propietarios y operadores de infraestructuras críticas para manejar los riesgos relacionados con la seguridad cibernética."[116] En suma, es la base de operación y maniobra de la defensa cibernética estadounidense en cualquiera de sus áreas para todos los sectores de la infraestructura crítica del país.

---

[115] *Ibídem.*

[116] *Cybersecurity Framework* [en línea], NIST, Disponible en: http://www.nist.gov/cyberframework/.

Asimismo, existe una "(…) Hoja de Ruta [que] discute los pasos futuros e identifica las áreas clave del desarrollo de la seguridad cibernética, la alineación y la colaboración."[117] La participación activa y comprometida de las instituciones y operadores de infraestructuras críticas se ve impulsada y motivada por todos los documentos y principalmente por el Instituto Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés).

De acuerdo con el documento "NIST Roadmap for Improving Critical Infrastructure Cybersecurity" o *NIST, Hoja de Ruta para mejorar la ciberseguridad en la infraestructura crítica:*

> "No todas las organizaciones de infraestructuras críticas tienen un programa maduro y la experiencia técnica para identificar, evaluar y reducir los riesgos de seguridad cibernética. Muchos no han tenido los recursos para mantenerse al día con los últimos avances y desafíos de seguridad cibernética, ya que corre el riesgo de equilibrio a sus organizaciones."[118]

Es por eso que, se instiga a grupos industriales, asociaciones y organizaciones no lucrativas a ser parte de la conciencia del Marco de Ciberseguridad. Es decir, se trata de una conjugación entre ambos sectores, público y privado, para hacer del Marco la herramienta básica para la gestión y reducción de los riesgos cibernéticos.

Además, como parte de las "medidas de organización" del gobierno federal, la creación del documento "Marco para mejorar las infraestructuras críticas de ciberseguridad, Versión 1.0", o *Framework for Improving Critical Infraestructure Cybersecurity Version 1.0,* complementa fundamentalmente las actividades de seguridad cibernética:

> "El marco consta de tres partes: the Framework Core (Marco base), the Framework Profile (Perfil del Marco), and the Framework Implementation Tiers (Niveles de implementación del Marco). El Marco de base es un conjunto de actividades de seguridad cibernética, resultados y referencias

[117] *Ibídem.*

[118] *NIST, Roadmap For Improving Critical Infraestructure Cybersecurity* [en línea], NIST, Disponible en: http://bit.ly/29SKEwj.

> informativas que son comunes en todos los sectores de infraestructura crítica, proporcionando las directrices detalladas para el desarrollo de perfiles de organización individuales. A través del uso de los perfiles [Framework Profile], el Marco ayudará a la organización [cualquiera] a alinear sus actividades de seguridad cibernética con sus requisitos de negocio, la tolerancia al riesgo, y los recursos. Los Niveles [F. Implementation Tiers] proporcionan un mecanismo para que las organizaciones vean y entiendan las características de su enfoque de la gestión de riesgos de seguridad cibernética."[119]

La preparación de las infraestructuras con las medidas de seguridad cibernética, dependerán del seguimiento de dicho marco, y el resultado y esfuerzo de los propietarios y operadores, organizaciones e instituciones especializadas en tecnologías de la información y sistemas de control industrial darán como resultado la ciberseguridad nacional.

> "Esta dependencia de la tecnología, la comunicación y la interconectividad de las TI y el ICS ha modificado y ampliado las vulnerabilidades potenciales y un mayor riesgo potencial de operaciones. (…) Para gestionar los riesgos de seguridad cibernética, se requiere una clara comprensión de los impulsores del negocio de la organización y las consideraciones de seguridad específicas para su uso de las TI y el ICS. Debido a que el riesgo de cada organización es única, junto con el uso de las TI y el ICS, las herramientas y los métodos utilizados para lograr los resultados descritos en el Marco variará."

Aunado a lo anterior es importante hacer una diferenciación entre seguridad informática, seguridad cibernética y seguridad de la información. Dado que el Marco de Ciberseguridad se ha preocupado por implementar medidas desde el control industrial hasta la comunicación, y que las amenazas cibernéticas se han diversificado, complejizado y potencializado, la ciberseguridad en su amplio

[119] *Framework for Improving Critical Infraestructure Cybersecurity, Version 1.0* [en línea], NIST, Disponible en: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

espectro se ocupa de equiparar todos aquellos espacios indispensables para lograr una cobertura total de seguridad.

Ergo, la seguridad informática refiere a la infraestructura computacional, en cuanto a software se refiere, verbigracia: programas y plataformas soportadas en Internet, encaminadas al intercambio de información. La seguridad de la información como su delimitación lo dice, refiere a lo circulante en la red, la información y datos que se resguardan y circulan. Dicha protección se hace a través de programas informáticos, y de la preparación de la infraestructura en redes capaces de crear candados, encriptar, entre otros.

La seguridad cibernética engloba las anteriores definiciones de seguridad a través de la protección de las redes frente riesgos y amenazas cibernéticas, principalmente contra la filtración o robo de información importante o confidencial para un Estado.

Puede identificarse, el espectro de una seguridad multidimensional donde la afectación de una esfera de la administración nacional puede traer consecuencias negativas a otra. Asimismo, se refleja la alta prioridad de proteger el espacio cibernético y su infraestructura ante la vulnerabilidad que ésta representa frente los riesgos que le persiguen. Debido a que ya no sólo se habla de un daño sectorial sino de uno intersectorial, cuyos daños pondría afectar gravemente la salvaguarda nacional.

Otro elemento muy importante para la formación de las bases de la seguridad cibernética, es la formación profesional. Se necesita de un centro de investigación y estudio docente que brinde no sólo principios, fundamentos y razonamientos, sino también genere recursos humanos potenciales. Es decir, se necesitan profesionales especializados, capaces de atender las futuras eventualidades de los riesgos y amenazas cibernéticas.

Para ello existe La Iniciativa Nacional para las Carreas y Estudios de Ciberseguridad (*NICCE, por sus siglas en inglés National Initiative For Cybersecurity Careers and Studies)*, la cual:

> "(…) es un esfuerzo de coordinación nacional que comprende más de 20 departamentos y agencias federales, el mundo académico y la industria. La misión de esta iniciativa es mejorar la postura general de seguridad cibernética de los Estados Unidos mediante la aceleración de la disponibilidad de recursos educativos y de formación destinados a mejorar el comportamiento cibernético, las habilidades y conocimiento de todos los segmentos de la población, lo que permite un ciberespacio más seguro para todos."[120]

Cuya importancia radica en que como centro de acreditación de profesionalización en seguridad cibernética, es el motor intelectual que potencializará cualitativamente y cuantitativamente los activos estadounidenses. De esta Iniciativa se desprende el Marco de Fuerza de Trabajo Nacional de Seguridad Cibernética o *National Cybersecurity Workforce Framework (NCWF)*[121] cuya funcionalidad es educar, reclutar, entrenar, desarrollar y retener una fuerza de trabajo altamente calificado, es decir, forma el Marco de fuerza de Trabajo.

Dicho "Marco Fuerza de Trabajo" se compone por el sector privado, la academia y gobierno, de acuerdo con la dirección del Departamento de Seguridad Nacional de Estados Unidos en 2014. El trabajo de Seguridad Cibernética se organiza en 32 áreas de espacialidad, incluyendo Zonas especiales como respuesta a incidentes de Administración de Datos, las cuales a su vez se agrupan en 7 categorías.[122]

La clasificación de áreas de especialidad en la seguridad cibernética hace más hace la división de tareas y conocimiento, destrezas y habilidades permitiéndole a las empresas y organizaciones, industrias de la seguridad cibernética a optar por el mejor tipo de educación, formación, certificaciones y habilidades necesarias para sus adaptarse a sus trabajos y necesidades de ciberseguridad.

---

[120] *About the National Initiative for Cybersecurity Education* [en línea], NICCS, Disponible en: http://bit.ly/29cYogb.

[121] *National Cybersecurity Workforce Framework* [en línea], National Initiative for Cybersecurity Education, Disponible en: http://csrc.nist.gov/nice/framework/.

[122] *Idem.*

Todas estas actividades de iniciativa federal se incorporan a un plan nacional de ciberseguridad que en colaboración con todos los organismos, públicos y privados especializados forman parte a su vez, de la Estrategia Nacional de Ciberseguridad del Departamento de Defensa de Estados Unidos de América. Esta última, como se desarrolló con anterioridad, es el pilar más importante de la lucha contra las amenazas cibernéticas, debido a que son las Fuerzas Armadas, en su mayoría las encargadas de hacerle frente a los peligros del espacio cibernético.

3.2 La ciberdefensa estadounidense. Ejecución: programas y patentes

El compromiso de Estados Unidos: gobierno, empresas, industrias, académicos, Fuerzas Armadas, civiles, entre otros, de llevar a cabo de salvedad y protección de sus infraestructuras críticas de los peligros cibernéticos, está reflejado en las acciones que se llevan a cabo amen de cumplir objetivos encaminados a la ciberseguridad.

Dichas acciones se traducen en una ciberdefensa, entre las que se destacan la creación de instituciones especializadas para capacitación y profesionalización en materia de seguridad cibernética, iniciativas ejecutivas a favor de la protección y mejora de las infraestructuras críticas, así como de las Tecnologías de la Información.

Ejemplo de ello es que, “el Departamento de Defensa (DOD) estableció el Programa de defensa de la base industrial (DIB) Ciberseguridad / Aseguramiento de la Información (CS/IA) que tiene como objetivo proporcionar normas de

seguridad cibernética, las mejores prácticas y directrices que deben aplicarse ya sea en el sector privado o público."[123]

Cabe destacarse que el gobierno estadounidense se preocupa por ambos aspectos importantes de la ciberseguridad, es decir, para poder llevar a cabo una práctica o acción (ciberdefensa), es preciso crear una estrategia o plan que enfrente eficazmente cualquier eventualidad cibernética. Debido a que las ciberamenazas se diversifican con el tiempo, surge la necesidad de ir adaptando y actualizando las medidas de la defensa cibernética, a las complejidades que de ellas se derivan.

Para ello, Estados Unidos tiene oficialmente reconocido *The Industrial Control Systems Cyber Emergency Response Team*, por sus siglas en inglés ICS-CERT, o El Equipo de Respuesta Cibernética a Emergencias de Cibersistemas de Control Industrial, el cual se encarga del trabajo en la asociación de fuerzas del orden y los servicios de inteligencia y la coordinación de esfuerzos entre los federales, estatales, locales y tribales y sistemas de control propietarios, operadores y proveedores.

Además, el ICS-CERT colabora con el sector privado internacional y equipos de respuesta a emergencias informáticas (CERT) para compartir sistemas de control relacionados con los incidentes de seguridad y medidas de mitigación.[124]

La cooperación internacional se ve forjada para una mayor concentración de esfuerzos en la lucha contra la ciberguerra. Sin embargo, cabe destacar que no cualquier empresa privada compartirá sus productos con otra de cualquier nacionalidad. Es decir, ante la disputa y confrontación por liderar la seguridad del espacio cibernético, los países seleccionaran con quienes sí crear convenios de cooperación, y así, estar mejor preparados.

Otro Equipo importante oficialmente reconocido es el *United States Computer Emergency Readiness Team,* US-CERT por sus siglas en inglés, o

---

[123] *Global Cybersecurity Index & Cyberwellness Profiles Report* [en línea], ITU, abril 2015, Disponible en: http://bit.ly/1oERpmG.

[124] *The Industrial Control Systems Cyber Emergency Response Team* [en línea], ICS-CERT, Disponible en: https://ics-cert.us-cert.gov/.

Equipo de Preparación de Emergencia Informática de Estados Unidos. Uno de los más importantes para el frente contra intrusos cibernéticos. Este equipo trata de generar un Internet "más fuerte" para los Estados Unidos, actúa eficientemente ante las eventualidades de las amenazas cibernéticas, en cualquiera que sea el caso.

> "El Equipo de Preparación de Emergencia Informática de Estados Unidos (US-CERT) dirige los esfuerzos para mejorar la postura de seguridad cibernética de la nación, coordinar el intercambio de información cibernética, y gestionar proactivamente los riesgos cibernéticos a la nación al tiempo que protege los derechos constitucionales de los estadounidenses."[125]

Su labor principal consiste en detectar y prevenir intrusos en el espacio cibernético de la rama ejecutiva federal civil, por ejemplo, presencias ajenas a las redes como virus, gusanos informáticos, hackers, y todo aquello que represente una amenaza cibernética emergente. Así con ello, desarrolla información oportuna y procesable para los Departamentos y Agencias Federales, para su análisis y gestión de políticas.[126]

Es por ello que papel de instituciones centrales especializadas como el US-CERT es primordial en las estrategias y defensas cibernéticas porque permiten la preparación de mecanismos y herramientas de contrataque, así como las legales y tecnológicas oportunas frente los intrusos cibernéticos en las redes.

Asimismo es importante recordar que la ciberestrategia estadounidense se "(…) [centra] en tres misiones - principalesladefensadelas redes(…) del Departamento de Defensa, la defensa de la nación contra ataques cibernéticos consecuentes y proporcionando capacidades cibernéticas integrados para apoyar las operaciones militares y planes[127]Donde dela conting disuasión es una parte clave de la estrategia.

---

[125] "About us" [en línea], *United States Computer Emergency Readiness Team, US-Cert,* Disponible en: https://www.us-cert.gov/about-us.

[126] *Idem.*

[127] DoD Cyber Strategy Defines How Officials Discern Cyber Incidents from Armed Attacks, U.S. Department of Defense, 15 de julio de 2016, Disponible en: http://bit.ly/2afFhSL.

La disuasión representa la oportunidad para Estados Unidos de debilitar los adversarios cibernéticos, ya que con ayuda de Agencias, el sector privado, y las naciones aliadas y asociadas, constituye un fuerte enemigo capacitado, difícil de vencer, con la amenaza de alcanzar el umbral de un ataque armado.[128]

> "(…) el Departamento [de Justicia] asume que los ciberataques contra intereses estadounidenses se lograrán mediante "la totalidad de las acciones de Estados Unidos, incluida la política declarativa, indicaciones importantes y capacidades de alerta, la postura defensiva, procedimientos eficaces de respuesta y la capacidad de recuperación global de las redes y los sistemas de los Estados Unidos. "[129]

Todas estas medidas maginifican la capacidad de Estados Unidos, y con ello, su presencia internacional. Como se menciona en su Política Exterior, la Casa Blanca busca reposicionarse ante la escena internacional a través de la fortificación de sus capacidades e influencia. Lucha para construir e integrar pueblos fuertes, en este caso, frente a la ciberguerra, donde la Fuerzas Armadas siempre serán la piedra angular de la seguridad.

En otras palabras, la estrategia está creada con la conexión fundamental entre la seguridad, la competitividad nacional, la resistencia y el ejemplo moral, para lograr no sólo el cumplimiento de su seguridad cibernética, si no para reposicionarse internacionalmente, es decir, ganar prestigio y fortaleza.

Una de las infraestructuras críticas más afectadas es la industrial, de cuya producción y ganancia se sustenta en gran medida la economía estadounidense, es en la que se han introducido medidas más fuertes, a saber, el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) a través del Proyecto de Ciberseguridad para Sistemas Inteligentes (*Smart* Systems) apoya a los fabricantes y proveedores de tecnología y proveedores de solución con directrices

[128] *Idem.*
[129] *Idem.*

de apoyo, métodos, métricas y herramientas con el fin de evaluar y garantizar la seguridad cibernética para los sistemas de fabricación inteligentes.[130]

La fabricación y preparación de proveerá de protección ante las vulnerabilidades que puedan surgir como resultado de su mayor conectividad, uso de redes y sensores inalámbricos, así como el uso de tecnologías de la información difundida.

> "Los fabricantes son reacios a adoptar tecnologías de seguridad comunes, como el cifrado y la autenticación del dispositivo, debido a la preocupación por los posibles efectos negativos en el rendimiento de sus sistemas. Esto se ve agravado por un entorno de amenazas que ha cambiado drásticamente con la aparición de ataques persistentes avanzadas dirigidas específicamente a sistemas industriales, como Stuxnet."

Otro proyecto es el Sistemas Inalámbricos para Entornos Industriales el cual "integra directrices para la selección, implementación y optimización de las tecnologías inalámbricas en entornos de fabricación. Las directrices se basan en la investigación en ciencias de medición para ayudar a los fabricantes en la selección e implementación de tecnologías inalámbricas[131] de manera efectiva por sus aplicaciones industriales."[132]

Su trascendentalidad radica mediante el aumento de la vigilancia y la superficie de control de sus procesos físicos, es decir, a través de las directrices para la evaluación del funcionamiento de la tecnología inalámbrica el gobierno gringo se encargará de asegurar una conectividad sin fisuras del dispositivo físico a la plataforma inalámbrica, dando lugar a una navegación segura, para dejar sin posibilidad a los peligros ciberespaciales de maniobrar en la trasmisión de frecuencias.

---

[130] *Cybersecurity for Smart Munufacturing Systems* [en línea], NIST, Disponible en: http://www.nist.gov/el/isd/cs/csms.cfm.

[131] Con tecnología o Sistemas inalámbricos se entiende por el conjunto de dispositivos en los que la comunicación (emisión y recepción) se da a través de ondas electromagnéticas en el espacio, por ejemplo, celulares, computadoras portátiles, computadoras de bolsillo, etc.

[132] *Wireless Systems for Industrial Invironments* [en línea], NIST, Disponible en: http://www.nist.gov/el/isd/cs/wsie.cfm.

Por su parte, el proyecto "Ciberseguridad para los sistemas de redes inteligentes o *Cybersecurity for Smart Grid*[133] *Systems*" proporciona orientación fundamental de la seguridad cibernética: revisiones, normas y requisitos, alcance y fomento de la colaboración en el tema trasversal de la seguridad cibernética en la red inteligente.

Para la estandarización y desarrollo de la ciberseguridad es necesaria la inclusión de privacidad, políticas, medidas, procedimientos y capacidad de recuperación en la red eléctrica inteligente. Así con las redes inteligentes seguras podrá actuarse eficazmente contra ataques deliberados como el espionaje industrial, el terrorismo, entre otros, como errores del usuario, fallos de los equipos y desastres naturales.

> "La cuadrícula del panel Interoperabilidad inteligente (SGIP) Comité de Seguridad Cibernética (SGCC), que está dirigido y gestionado por la información de laboratorio NIST Tecnología (DIT), División de Seguridad Informática, se está moviendo hacia adelante en FY14 para hacer frente a las necesidades de seguridad cibernética críticos en las áreas de medición avanzada requisitos de seguridad de la infraestructura (IAM), cloud computing, la cadena de suministro, y recomendaciones de privacidad relacionados con los estándares emergentes."[134]

Con todas las metodologías anteriores se busca entender su aplicación en el sector eléctrico, asimismo dentro del proyecto se habla del desarrollo de nuevo metodologías y herramientas que permita la identificación de sus deficiencias y necesidades.

Este proyecto surge de la necesidad de proteger de igual forma la industria eléctrica de las nuevas y cambiantes amenazas a la seguridad cibernética, tanto de

---

[133] Las Smart Grids (o redes inteligentes) son básicamente redes de distribución eléctrica combinadas con modernas tecnologías de información, que proporcionan datos tanto a las empresas distribuidoras de electricidad como a los consumidores, lo que es ventajoso para ambas partes. Obtenido de: http://bit.ly/29PBxe4.

[134] *Cybersecurity for Smart Grid Systems* [en línea], NIST, Disponible en: http://www.nist.gov/el/smartgrid/cybersg.cfm

manera masiva, como en áreas nodales: de criptografía aplicada y la ciberseguridad para microredes.

Así, Estados Unidos ha lanzado un conjunto de leyes e instituciones enfocadas a la seguridad cibernética y tecnologías de la información; donde empresas, instituciones, academia y gobierno se han dado a la tarea de crear las condiciones necesarias, sean tecnológicas y en el marco jurídico para conseguir la salvaguarda de las redes y su infraestructura crítica.

La implementación de un protocolo para la defensa de sistemas comerciales (tecnologías de la información) de los ciberataques, permite, entre otras cosas la integridad, fiabilidad, e interconexión segura de las personas, generando confianza en el gobierno y compañías.

3.3 Roles en la escena internacional

Ante la problemática de las amenazas cibernéticas, países de todo el mundo, principalmente los que sobresalen en el área tecnológica, han creado sus propias medidas en contra de la ciberguerra, por ello dada la relevancia que ha cobrado la ciberseguridad en el mundo, organizaciones internacionales especializadas como la Unión Internacional de Telecomunicaciones (*ITU, por sus siglas en inglés International Telecommunication Union)*, la cual se han encargado de hacer un ranking donde plasma el índice de preparación de un país frente a la ciberguerra.

De acuerdo con la tabla 3.1 presentada por el *Índice Global de Ciberseguridad*, los primeros 3 lugares de los países mejor preparados se encuentran posicionados, en primer lugar: Estados Unidos, precedido en segundo lugar por Canadá, y en tercer lugar a Australia, Malasia y Omán:

Tabla 3.1 Que muestra de posición de cada país por el Índice Global de Ciberseguridad. Fuente: *Global Cybersecurity Index & Cyberwellness Profiles Report* [en línea], ITU, april 2015, Disponible en: http://bit.ly/1oERpmG.

Table 1: Country rank by index

Country	Index	Global Rank
United States of America*	0.824	1
Canada*	0.794	2
Australia*	0.765	3
Malaysia	0.765	3
Oman	0.765	3
New Zealand*	0.735	4
Norway*	0.735	4
Brazil	0.706	5
Estonia*	0.706	5
Germany*	0.706	5
India*	0.706	5
Japan*	0.706	5
Republic of Korea	0.706	5
United Kingdom	0.706	5

Como eventualmente se conoce, países potencia como Francia, Rusia, China y otros, quienes disputan el control y protección de la seguridad cibernética, no parecen en los primeros cinco lugares del Ranking, a excepción de Alemania, Reino Unido y Nueva Zelanda, lo que difiere con quienes lo encabezan.

Empero que el raking no toma en cuenta las capacidades y posibles vulnerabilidades de cada Estado. La tabla demuestra la fortaleza y eficacia que tienen y que puede llegar a alcanzar aquellos países emergentes en materia de ciberguerra.

Por ende, dicha preparación conlleva un arduo trabajo y esfuerzo por idear y crear proyectos que permitan la seguridad, fiabilidad, operatividad e interoperabilidad de las redes y sistemas. Es importante que, para garantizar y mantener las infraestructuras críticas a salvo de los peligros y amenazas

cibernéticas, las instituciones y agencias especializadas implementen medidas para los principales puntos vulnerabilidad.

Desde hace algunos años, con la emergencia de la era tecnológica y su ardua innovación, los Estados más poderosos se han visto inmiscuidos en una serie de conflictos de carácter cibernético. Y junto con ello, se han buscado nuevas formas de atacar y dañar al enemigo, un ejemplo claro, es la confrontación entre Estados Unidos y China, o Rusia, o bien, con países de Medio Oriente.

Se puede decir que le principal enemigo de Estados Unidos es China. De acuerdo con informes y comunicados del Departamento de Defensa y otros, se han encontrado con ataques a empresas, a agencias de la administración pública federal, instituciones públicas y privadas dedicadas a la gestión en áreas como la financiera, de electricidad, de recursos energéticos, de transportes, entre otros, ante los cuales los principales responsables son hackers chinos.

Ejemplos de algunos casos son:

> **"(…)** «operación Aurora» de 2009, un ataque chino contra los servidores de Google y que terminó con la salida del gigante informático de la nación asiática. O el caso de 2007 y 2008, cuando atacantes chinos se colaron en la red de satélites de los Estados Unidos para interceptar sus comunicaciones. En 2011, un programa de la TV china llegó a mostrar un software para llevar a cabo ciberataques, con una lista que incluía un ataque en curso contra una universidad norteamericana.**"**[135]

Sin embargo, ante la imposibilidad de saber el origen de dichos ataques, la definición del objetivo a atacar o disuadir se vuelve obsoleta. Aunque se sabe de dónde provienen los ataques de acuerdo con las características o ciertas particularidades del ataque, resulta difícil identificar si se trata de un sujeto privado o de un gobierno en específico.

Cabe destacar que existen organizaciones dedicadas a los delitos cibernéticos que se cuelan entre empresas privadas, y que así como Estados

[135] Nieves, José Manuel, "La primera ciberguerra mundial ha estallado ya" [en línea], ABC Tecnología, 15 de junio de 2015, Disponible en: http://bit.ly/1BcWet0.

Unidos mismo, otros Estados tiene agencias especializadas dedicadas especialmente al ciberespionaje.

Ante estas figuras y actores cibernéticos, no debe olvidarse el papel que ha desempañado Estados Unidos a través de la historia, es decir, las relaciones con América Latina y el Caribe, con Medio Oriente (los grupos terroristas), así como con Asia-Pacífico (China, India, Corea del Sur) y África. Es importante tomar en cuenta esto ya que a consecuencia de rivalidades, disputas territoriales, empresariales, económicas, gubernamentales e ideologías es que pueden responderse por medio del ciberespacio con ataques a objetivos específicos, cuyos alcances son mayores al de una guerra física.

Por otra parte, también es importante hacer referencia a los acuerdos de cooperación en materia cibernética, como el que hay entre Estados Unidos y la Unión Europea sobre "nuevo marco jurídico que regirá en la transferencia de los datos personales con fines comerciales cuyo objetivo es proteger los derechos de los ciudadanos europeos frente a las derivas del espionaje masivo"[136] conocido como "Privacy Shield".

Otro ejemplo es que "China y Estados Unidos ratificaron su consenso en asuntos de ciberseguridad en un diálogo de alto nivel en Pekín en el que trataron de acercar posturas sobre una de las áreas que ha generado mayor conflicto entre ambos estos últimos años."[137] Ante la confrontación de ambos países, acordaron colocar la ciberseguridad un asunto dentro de la cooperación internacional.

Asimismo China y EEUU "se comprometieron a priorizar la cooperación para combatir el robo de propiedad intelectual con fines comerciales y a organizar un seminario en China centrado en el uso indebido de la tecnología y de las comunicaciones para actividades de terrorismo"[138] Lo que significa un gran avance

---

[136] "La Unión Europea y Estados Unidos lanzan el nuevo acuerdo para proteger la privacidad en Internet" [en línea], *El Mundo,* 12 de julio de 2016, Disponible en: http://bit.ly/29T5v1U.

[137] "China y EEUU ratifican consenso en ciberseguridad en Pekín" [en línea], *La Vanguardia,* 15 de julio de 2016, Disponible en: http://bit.ly/2bCCrgu.

[138] *Ibíd.*

en la seguridad de sus infraestructuras críticas, gobierno, empresas, instituciones públicas y privadas, y personas.

Dichos acuerdos, entre otros, representan para Estados Unidos la posibilidad de crear aliados a favor de su seguridad cibernética, así como de la consecución de la ciberdefensa en varios puntos del mundo. Y con ello, maximizar su influencia y reposicionarse a nivel mundial, repuntar su liderazgo.

Investigadores de seguridad de FireEye[139], crearon el ThreatMap, una representación de la comunicación entre comando y control (C&C) y los ordenadores de las víctimas. En el siguiente mapa, se aprecian los ataques desde y hacia Estados Unidos, donde sus atacantes son: Portugal, Iraq, Ucrania y Letonia, ene el caso de Suiza (en verde) aparece como objetivo de los Estados Unidos.

Es importante señalar que FireEye resalta que los ataques se muestran de acuerdo con su frecuencia observada, por lo que dichos ataques son una pendiente constante, asimismo, estas relaciones representan información útil para las organizaciones y agencias de ciberseguridad estadounidenses para identificar con mayor facilidad la procedencia de los ataques y saber cómo defenderse o contratacar.

.

Mapa 3.2. Ciberataques representados en el Mapa de Amenazas. Fuente: Cyber-Attacks Represented in Threat Map [en línea], Disponible en: http://bit.ly/2aeqzxM.

[139] Una empresa líder en seguridad cibernética, la protección de las organizaciones de malware avanzado, ataques de día cero, APT, y otros ataques cibernéticos. Obtenido de: www.fireeye.com.

Mapa 3.3 por FireEye, en el que se muestran los grupos de Amenzas Avanzadas Persistentes, (ATP, por sus siglas en inglés, *Advanced Threat Persistent) con* posibles de ataques a Corea del Norte, Canadá y Estados Unidos. Asimismo es posible visualizar los ataques de Rusia a Estados Unidos, cuya relación de ciberguerra esta fuertemente activa. Con las declaraciones del Secretario de Defensa, Ash Carter, respecto al reforzamiento de la ciberseguridad hacia este país o China o Irán, supone una declarativa de guerra cibernética y junto con ello una mejor preparación de su ciberdefensa. Disponible en: http://bit.ly/2aeqzxM.

La preparación para la ciberguerra, es sin duda, una de las bases para la efectiva defensa de los ataques cibernéticos sin importar su procedencia. Las relaciones a través del ciberespacio se han vuelto más constantes y necesarias, por lo que el cuidado, ordenamiento y salvaguarda de las redes y las infraestructuras críticas a través de agencias especializadas públicas o privadas, necesitan de mayor incentivo, ante ello, el Secretario de Defensa señaló que: "'El presupuesto da prioridad a la financiación de nuestra estrategia cibernética [por lo que se invertirá]

(…) un total de 6.700 millones de dólares en el año fiscal 2017'"[140]

Esta mayor inversión permitirá generar nuevas tecnologías y software de ciberseguridad. E impondrá una nueva esfera de poder ante los demás países cuya fortaleza dependerá de la preparación y avance tecnológico y militar.

De la misma manera, es importante señalar el papel que desempeñan empresas como *Google, Cisco, Oracle*, entre otros, ya que por sí solas están innovando sus productos con la oferta de seguridad y protección ante futuras vulnerabilidades cibernéticas e informáticas. En conjunto con el gobierno, instituciones, industria y otras empresas, maximizaran las ganancias frente al mundo y la ciberguerra.

[140] M. Adalid Carolina, "El Pentágono refuerza la 'ciberguerra' contra el Estado Islámico" [en línea], El Mundo, España, 27 de febrero de 2016, Disponible en: http://bit.ly/1VJo1Xv.

Consideraciones finales

La ciberguerra es un fenómeno de poca antigüedad pero de largo alcance. A consecuencia de los grandes beneficios y ventajas de Internet para la economía y organización del mundo, se ha encontrado un nuevo espacio para delinquir y generar daños a un Estado y sus integrantes, como lo son empresas, instituciones y organizaciones públicas y privadas, y a la población.

Es a través de los ordenadores y tecnologías de la información y comunicación con los que los hackers o ciberatacantes llevan a cabo dichas acciones en perjuicio de las infraestructuras críticas de un Estado, debido su fácil acceso, eficacia, rendimiento, velocidad, capilaridad y ubicuidad, así como anonimato. Características propias del espacio cibernético.

Debido a que a mayoría de las actividades se llevan a cabo por la red, sean económicos, financieros, electorales, o cualquier índole, en cualquier nivel de gobierno o individual, el ciberespacio es un nuevo espacio para atacar y generar daños con cualquier alcance.

Los ataques cibernéticos van desde fraudes bancarios, usurpación de identidad, infiltración de bases de datos, espionaje, hasta el ciberterrorismo. Dichas acciones de acuerdo al número de ataques y daño creado en un determinado Estado, entre otros factores, se convertirá en su principal amenaza cibernética, algunas veces plasmada en un Informe Nacional de Seguridad Cibernética.

Ante cada amenaza cibernética se creará una estrategia cibernética y posterior defensa cibernética, encargadas de prevenir, defender, atacar, aminorar la ciberamenaza, resarcir los daños, incluyendo la disuasión del ciberatacante.

Los actores ciberespaciales son los encargados de forjar el avance tecnológico ya que a consecuencia de los peligros en el ciberespacio se tienen que crear los recursos necesarios, sean intelectuales o tecnológicos, para conseguir una efectiva seguridad cibernética.

Como en la guerra tradicional, en la ciberguerra también existe la Geopolítica, es importante destacar que cada Estado sostiene una lucha por mantenerse al margen de las amenazas y riesgos cibernéticos, por lo que percibe e identifica sus posibles rivales y enemigos, y aliados, para así actuar efectivamente en su ciberdefensa. De esta identificación se desprenden las tácticas de enfrentamiento, ya sea cooperación entre contrincantes o bien, ataque, contrataque u ofensa.

Es el caso del gobierno estadounidense quien se preocupa por ambos aspectos importantes de la ciberseguridad, es decir, para poder llevar a cabo una práctica o acción, es preciso crear una estrategia o plan que enfrente eficazmente cualquier eventualidad cibernética que se convierte en ciberdefensa. Debido a que las ciberamenazas se diversifican con el tiempo, surge la necesidad de ir adaptando y actualizando las medidas de la ciberdefensa a las complejidades que de ellas se derivan.

Para Estados Unidos de América, entre sus principales rivales se encuentran China, Rusia, Alemania, Reino Unido, la Unión Europea, así como Irak y todos aquellos países cuyos objetivos vayan en detrimento de la estabilidad y liderazgo estadounidense.

Para las últimas administraciones de Barack Obama, Estados Unidos de América se ha encargado de renovar su Política Exterior a través de la reconstrucción de su fuerza e influenza, así como de sus capacidades para lograr la consecución de sus intereses, bienestar e integridad.

Ante la eventualidad que significa la guerra en el ciberespacio, los Estados Unidos de América se enfrentan un mundo de incertidumbre, no sólo porque son el país más propenso a ataques sino también por su gran poder y posición internacional, por ello se enfrente a grandes retos como

1. Politización: Impacto de la ciberguerra en el ámbito político y en sus políticas públicas. Trascendencia en los intereses de la nación.

   La cual refiere también a la securitización en la política. Darle importancia en el discurso, y así presentar a la nación y frente al mundo la preparación y postura

ante la ciberguerra. Asimismo, dicha politización conlleva la creación de políticas y acciones alternativas en la ciberdefensa. Ejemplos de ello, se encuentran reflejados en los discursos del presidente B. Obama, el de los secretarios de Defensa y Seguridad Nacional, así como en las órdenes ejecutivas 13636 para la Mejora de la Infraestructura Crítica de Ciberseguridad y la Política de la Directiva Presidencial de la Infraestructura Crítica y Resiliencia.

2. Protección: optimizar leyes de protección de datos e información, así como de elaboración y construcción de tecnologías de la información para la ciberseguridad; e,
3. Innovación: productos y tecnologías para conseguir una mayor preparación tecnológica y de capacidad militar

No sólo es necesario preparar las armas, sino también se requiere de un marco legal fuerte para proteger a los ciudadanos de cualquier abuso, robo o usurpación de la identidad personal.

El marco jurídico estadounidense de legislación criminal que cubre los fraudes y las actividades relacionadas con conexiones a computadoras, correo electrónico, dispositivos de acceso, sobre el Control del Asalto de la pornografía no solicitada y Marketing.

Otros instrumentos jurídicos son:

- Ley Uniforme de operaciones electrónicas

- Firma Electrónica en Global y la Ley Nacional de Comercio

- Ley de Seguridad Nacional - Ley de Desarrollo de Seguridad Cibernética Investigación y

- La protección de los niños en la Ley de siglo 21

- Ley de Protección de Niños en Internet

- Adam Walsh de Protección del Niño y la Ley de Seguridad

- Mantener el Desprovisto de Internet Sexual - Ley de depredadores

- Libertad de Información - Ley de Privacidad

Uno de los elementos del poder es la capacidad tecnológica, y si Estados Unidos quiere recuperar poderío y liderazgo en la escena internacional, tiene que lanzarse fuere y altamente capacitado. La armonización de leyes y tecnologías permiten una mayor eficacia en la seguridad cibernética.

4. Inversión: en la investigación y estudio de diferentes tipos de ataques cibernéticos, sean antiguos o por desarrollarse, para así encontrar los medios de su abatimiento; y,
5. Capacitación: del ejército y del personal cibernético a través de una mayor especialización

Al contar con un mayor conocimiento de los enemigos cibernéticos y sus riesgos, el equipo cibernético será capaz de desarrollar cada vez más y mejores capacidades de defensa a favor de la seguridad cibernética. De la misma manera el desarrollo de habilidades resulta necesario para la consecución de objetivos y metas. Tareas que competen al US-CERT y al ICS-CERT, y al gobierno e instituciones educativas y empresariales con la creación de nuevas figuras académicas, en materia militar y avance tecnológico.

6. Lograr una nueva perspectiva del ciberespacio en la sociedad para conseguir un cambio en el uso de las tecnologías de información.

Un cambio de visión o doctrina social significan la posibilidad del cambio conducida al bien. Es necesaria una concientización de del daño y peligro en el ciberespacio, y con ello, generar una nueva perspectiva de seguridad en el nivel más simple y propenso: el individual. Ejemplo claro es la respuesta generada de personas y sitios web, con la Ley Sopa, la cual atentaban contra la libertad de expresión dado que el gobierno tenía la autorización de bloquear el sitio web por una infracción.

7. Formación de una visión local, regional, global y planetaria en la ciberestrategia y en la ciberdefensa, a través de la cual pueda crear alianzas y bloques de poder.

De esta manera, Estados Unidos de América debe tener en cuenta la dimensión del problema a nivel internacional, junto con ello identificar y crear posibles alianzas. No sólo se trata de la preparación y fortificación interna, sino también externa en cuya fortaleza prevalezcan bloques de poder en materia de ciberseguridad. Mantenerse al tanto de los desafíos y amenazas cibernéticas por regiones, así como estrechar y recibir apoyo.

La preparación para la ciberguerra, es sin duda, una de las bases para la efectiva defensa de los ataques cibernéticos sin importar su procedencia. Es por eso que, los Estados Unidos de América ante la incertidumbre de las amenazas cibernéticas debe tomar en cuenta lo siguiente:

1. La capacidad y alcance de otros Estados (sea sus y los actores en el ciberespacio para afectarlo y defenderse.
2. Los ataques no siempre provienen de “afuera”, éstos pueden suceder desde el interior del país, por lo que debe tomar control y protección de sus infraestructuras críticas empleando medidas que rectifiquen la identidad del individuo que utiliza las tecnologías de la información.
3. El anonimato de las redes, pero que aun así, puede identificar ciertas características de los ataques para saber su procedencia. En su defecto, los ataques tienen un *modus operandi*, y utilizan diferentes herramientas según sea el objetivo.
4. Debe tener un plan de emergencia ante cada tipo de ciberataque cuyo riesgo sea el máximo para su integridad y estabilidad. Éste es una de las tareas básicas en caso de un fuerte ataque. El que sea considerado su mayor peligro cibernético, Estados Unidos debe tener un abanico de posibles soluciones para sostener su liderazgo y fortalecer su seguridad nacional en el siglo XXI.

La hipótesis de la investigación se comprueba porque se demostró que el dominio de los actores en el ciberespacio pone a prueba la fortaleza y estructura de los Estados más fuertes, en este caso de Estados Unidos. Los actores ciberespaciales lo vuelven cada vez más vulnerable dado el descontrol que posee en el ciberespacio aunado a los posibles ataques a su gobierno. Se identificó que son los actores ciberespaciales los que dinamizan la evolución tecnológica para que Estados Unidos refuerce sus capacidades de defensa y seguridad, logrando su reposicionamiento a nivel mundial.

Fuentes de información

(bibliografía, ciberografía, hemerografía, documentos oficiales)

¿Cuáles son los principales riegos globales para 2016? [en línea], World Economic Forum, Disponible en: http://bit.ly/1ZIW4RD.

¿Qué es el IETF en español claro? [en línea], en Internet Society, Disponible en: http://bit.ly/1N9Oasy.

¿Qué hace ICANN? [en línea], en ICANN, Disponible en: http://bit.ly/1Qe0E5B.

¿Qué hacemos en Internet Society? [en línea], Disponible en: http://bit.ly/1XKdih5.

¿Qué son el malware, el spyware, el spam, el phishing, el pharming, etc.? [en línea], en Totalbank, Disponible en: http://bit.ly/1Tbkwbb.

"About us" [en línea], *United States Computer Emergency Readiness Team, US-Cert,* Disponible en: https://www.us-cert.gov/about-us.

"Agenda de Política Exterior de los Estados Unidos de América", *Periódico electrónico del Departamento de Estado de Estados Unidos,* Vol. 7, Núm. 4, p. 2, Disponible en: http://bit.ly/2bCiuR8.

"China y EEUU ratifican consenso en ciberseguridad en Pekín" [en línea], *La Vanguardia,* 15 de julio de 2016, Disponible en: http://bit.ly/2bCCrgu.

"Discurso de Barack Obama en la Academia Militar de West Point" [en línea], *Red Voltaire,* 28 de mayo de 2014, Disponible en: http://bit.ly/2bAVaWV.

"Internet for all. A framework for accelerating Internet access and adoption" [en línea], *World Economic Forum,* abril 16, Disponible en: http://bit.ly/20Z44hD.

"L'Agenzia A.R.P.A."[en línea], Le origini di Internet, Disponible en: http://bit.ly/1LOA7sz.

"La OTAN y la UE aumentan la cooperación en ciberseguridad" [en línea], *Departamento de Seguridad del Gobierno de España,* Disponible en: http://bit.ly/2c33nTn.

"La Unión Europea y Estados Unidos lanzan el nuevo acuerdo para proteger la privacidad en Internet" [en línea], *El Mundo,* 12 de julio de 2016, Disponible en: http://bit.ly/29T5v1U.

"Newaweek y Delta sufren ciberataques en las redes sociales" [en línea], Doctor Shoper, Disponible en: http://bit.ly/2bQnPYL.

"Un ataque saca a la luz los datos de 4 millones de funcionarios en EEUU" [en línea], E*l Confidencial,* Disponible en: http://bit.ly/2c2XKV6.

About the National Initiative for Cybersecurity Education [en línea]*,* NICCS, Disponible en: http://bit.ly/29cYogb.

About the NIST [en línea], NIST*,* Disponible en: http://bit.ly/29kUWmL.

Armending Gisela, *Una mirada hacia la Declaración de las Américas,* Centro Argentino de Estudios Internacionales, Programa Defensa y Seguridad, Disponible en: http://bit.ly/1PXNETW.

Arquilla, John; David Ronfeldt, Redes y guerras en red: El futuro del terrorismo, el crimen organizado y el activismo político, Alianza Editorial, 2003, p. 34.

Barry M. Leiner (et. al) "A brief history of the Internet" [en línea], en Internet Society, Disponible en: http://www.internetsociety.org/es/breve-historia-de-internet.

Blin Arnaud y Gustavo Marín (Ed.), "Seguridad", *Diccionario del poder mundial,* Foro por una Nueva Gobernanza Mundial, París, Francia, 2013, p. 277.

Buzan Barry, "The national security problem in International Relations*",* p. 22 en *People States and Fear: An agenda for international security studies in the Post-Cold War Era,* London: Harvester, Wheatsheaf, 1991, pp 1-34.

Caro Bejarano, María José, "La protección de las infraestructuras críticas" [en línea], *Instituto Español de Estudios Estratégicos,* 021/2011, 27 de julio de 2011, p. 2, Disponible en: http://bit.ly/2bT1aLv.

Castells Manuel, *The Internet Galaxy. Reflections on the Internet, business and society,* Ed. Oxford University Press, Estados Unidos*,* 2011, citado en Herrera Capetillo, Héctor Ernesto, *"*Historia y desarrollo de Internet", *Evolución del pensamiento geopolítico en la estudio del ciberespacio,* México, 2014, FCPyS, UNAM, p. 133

Chanona Alejandro, "El debate teórico sobre la construcción de las comunidades de seguridad", en *La comunidad de seguridad en América del Norte, una perspectiva*

comparada con la Unión Europea, México: Facultad de Ciencias Políticas y Sociales, UNAM, 2010, p. 12.

Chardon, Anne-Catherine y Juan Leonardo González, "Amenaza, vulnerabilidad, riesgo, desastre, mitigación, prevención...", *Programa de información e indicadores de gestión de riesgos,* Banco Interamericano de Desarrollo, CEPAL, Universidad Nacional de Colombia, IDEA, Dic. 2012, p. 3.

Ciberseguridad [en línea], en Actualidades de la UIT, Disponible en: http://bit.ly/1QPmqNo.

Cited and Arnold Wolfers, *Discord and Collanoration,* Baltimore: John Hopkins University Press, 1962, p. 150, en Buzan Barry, *The national security problem in International Relations,* p. 20.

Colom Piella, Guillem y Josep Baqués Quesada, El concepto de la Revolución Militar y su empleo en los estudios estratégicos [en línea], Disponible en: http://bit.ly/1TwLyYZ.

Cyber-Attacks Represented in Threat Map [en línea], Disponible en: http://bit.ly/2aeqzxM.

Cybersecurity for Smart Grid Systems [en línea], NIST, Disponible en: http://www.nist.gov/el/smartgrid/cybersg.cfm

Cybersecurity for Smart Munufacturing Systems [en línea], NIST, Disponible en: http://www.nist.gov/el/isd/cs/csms.cfm.

Cybersecurity Framework [en línea], NIST, Disponible en: http://www.nist.gov/cyberframework/.

D. Davies, Internet Hall of Fame [en línea]*, Disponible en: http://bit.ly/24Yu7qk.*

Definición de Riesgo [en línea], Centro Internacional para la Investigación del Fenómeno de El Niño, Disponible en: http://bit.ly/2awi7wG.

Definición del Riesgo [en línea]*,* CIIFEN, Disponible en: http://bit.ly/1hRPdCP.

Definición extraída del glosario de términos informáticos, Whatis, Disponible en http://whatis.techtarget.com/, citado en Caro Bejarano María José, *Alcance y ámbito de la seguridad nacional en el ciberespacio* [en línea], Disponible en http://bit.ly/1MCU3Eh.

DoD Cyber Strategy Defines How Officials Discern Cyber Incidents from Armed Attacks, U.S. Department of Defense, 15 de julio de 2016, Disponible en: http://bit.ly/2afFhSL.

El concepto de seguridad humana [en línea], United Nations Trust for Human Security, Disponible en: http://bit.ly/1KivEkv.

EO 13636, PPD -21 [en línea], Homeland Security, Disponible en: http://1.usa.gov/25VQRKO.

Estados Unidos presenta hoy nueva estrategia de ciberseguridad [en línea], en Mediatelecom, 24 de abril de 2015, Disponible en: http://bit.ly/1MWgfHb.

Joint Publication 1-02. Department of Defense. Dictionary of Military and Associated Terms. (2009) [en línea], Disponible en: http://www.dtic.mil, óp. cit.

Félix Badia, *Internet: situación actual y perspectivas.* Ed. La Caixa, Barcelona España, 2002, p. 17, citado en Herrera Capetillo, Héctor Ernesto, "Historia y desarrollo de Internet", *Evolución del pensamiento geopolítico en la estudio del ciberespacio,* México, 2014, FCPyS, UNAM, p. 133.

Framework for Improving Critical Infraestructure Cybersecurity, Version 1.0 [en línea], NIST, Disponible en: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

García David, La "Doctrina Obama", la teoría de la Guerra Limitada y la nueva política exterior de EEUU: ¿Hacia una política neo-nixoniana? [en línea], UNISCI, Universidad Complutense de Madrid, No. 18, Enero 2012, Disponible en: http://bit.ly/23pwZhT.

Global Cybersecurity Index & Cyberwellness Profiles Report [en línea], ITU, abril 2015, Disponible en: http://bit.ly/1oERpmG

Global Risks Repot 2016 [en línea], World Economic Forum, Disponible en: http://bit.ly/1RvWKZK.

Global Trends: 2030: Alternative Worlds [en línea], National Intelligence Council, Estados Unidos de América, diciembre 2012, Disponible en: http://bit.ly/1CSdG5K.

Gross Stein Janice, *The Oxford Handbook of Political Psichology,* 2ª Ediciónpoy Leonie Huddy, David O. Sears, y Jack S. Levy. Oxford University Press, 2013, p.p. 23-25.

Hernández Enrique, "Sufren ciberataques más del 53% por ciento" [en línea], *Forbes,* junio de 2016, Disponible en: http://bit.ly/1O6sSmw.

Jordán Javier, Innovación y revolución de los asuntos militares: una perspectiva no convencional [en línea], International Security Studies Group, Disponible en: http://bit.ly/1UnbWq5.

L. G. Roberts, Internet Hall of Fame [en línea], Disponible en: http://bit.ly/21t3CIz.

L. Kleinrock, The University of California, ULCA*, [en línea], Disponible en: http://bit.ly/1PAfiTM.*

La estructura de internet [en línea], Disponible en: http://bit.ly/1Oc96nv.

La mejora de las infraestructuras críticas de ciberseguridad. Orden Ejecutiva 13636, [en línea], Federal Registrer. The Daily Journal of the Unites States Goverment, Disponible en: http://bit.ly/1fnluyZ.

La Renovación del liderazgo estadounidense [en línea], Nuevo Orden Mundial, 9 de febrero de 2009, Disponible en: http://bit.ly/23iTcwP.

M. Adalid Carolina, "El Pentágono refuerza la 'ciberguerra' contra el Estado Islámico" [en línea], El Mundo, España, 27 de febrero de 2016, Disponible en: http://bit.ly/1VJo1Xv.

Misión permanente de México ante la OEA [en línea], Disponible en: http://bit.ly/1PEav3f.

Molina Rabadán, David, *La Revolución de los Asuntos Militares (RMA) en el contexto de la era de la información* [en línea], Revista de Estudios Ciencias Sociales y Humanidades, nùm. 14, 2005, pp.78-79., Disponible en: http://bit.ly/2aACasw.

National Cybersecurity Workforce Framework [en línea], National Initiative for Cybersecurity Education, Disponible en: http://csrc.nist.gov/nice/framework/.

National Security Agency [en línea], Disponible en: http://1.usa.gov/1ZLzOFp.

Nieves, José Manuel, "La primera ciberguerra mundial ha estallado ya" [en línea], ABC Tecnología, 15 de junio de 2015, Disponible en: http://bit.ly/1BcWet0.

NIST, Roadmap For Improving Critical Infraestructure Cybersecurity [en línea], NIST, Disponible en: http://bit.ly/29SKEwj.

Nye Joseph*, Cyberwar and peace* [en línea], Disponible en: http://bit.ly/1LMaqx9.

Paul Barand, Rand Corporation [en línea]*, Disponible en: http://bit.ly/1tvpkRa.*

Prabir Purkayastha, *¡Haz la ciberpaz y no la ciberguerra*! [en línea], Alaii, Disponible en: http://bit.ly/1LMiOgi.

Presupuesto de Defensa por país [en línea], Global Firepower, Disponible en: http://bit.ly/1uno1zq.

Programa de Seguridad Nacional 2014-2018 [en línea], SEGOB, Disponible en: http://bit.ly/1iDi3BK.

Raimundi, Maria Julia; Molina, Maria Fernanda, et. al., ¿Qué es un desafío? Estudio cualitativo de su significado subjetivo en adolescentes de Buenos Aires. Rev. latinoam. cienc. soc. niñez juv, [en línea], 2014, vol.12, n.2, pp. 521-534, Disponible en: http://bit.ly/1ShUd5O.

Richad H. Ullman 'Redefining security', *International Security,* 1983, note 32, p. 133 en Buzan Barry, *The national security problem in International Relations,* p. 20 en *People States and Fear: An agenda for international security studies in the Post-Cold War Era,* London: Harvester, Wheatsheaf, 1991, pp 1-34.

Rodríguez Ávila Abel, *Iniciación a la red Internet, Concepto, funcionamiento, servicios y aplicaciones de Internet,* Ed. Ideas propias, España, 2007, p. 2, citado en Herrera Capetillo, Héctor Ernesto, "Historia y desarrollo de Internet", *Evolución del pensamiento geopolítico en la estudio del ciberespacio,* México, 2014, FCPyS, UNAM, p. 131.

S/ autor, *Ciberdefensa-Ciberseguridad: Riesgos y Amenazas* [en línea], CARI, noviembre 2013, disponible en: http://bit.ly/1N3cj97.

S/ autor, Cybersecurity and cyberwar [en línea], Disponible en: http://bit.ly/1LEbbpl.

Sánches Tapia Salvador, Política exterior y de seguridad de los Estados Unidos: la "Pax americana" después de Afganistán [en línea], Instituto Español de Estudios Estratégicos, 43/2014, Disponible: http://bit.ly/1JD6IWU.

Sánchez Medero, Gema. "Ciberguerra y ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica". Amérigo Cuervo-Arango, Fernando; Peñaranda Algar, Julio. Dos décadas de Posguerra Fría. Instituto Universitario General Gutiérrez Mellado, 2009. Tomo I, p. 215-241, óp. cit.

Sancho Hirane Carolina, Ciberespacio: delitos, amenazas a la seguridad y ¿guerras? [en línea], en Academia Nacional de Estudios Políticos y Estratégicos (ANEPE), Disponible en: http://bit.ly/1OcTy36.

Seguridad humana para todos [en línea], Fondo Fiduciario de las Naciones Unidas para la Seguridad Humana, Disponible en: http://bit.ly/1F712BR.

Solé Pascual Carles y Adolfo Hernández, Estrategias nacionales de cibeseguridad en el mundo (en línea), en redseguridad.com, Disponible en: http://bit.ly/1CAB6cJ.

Solé Pascual, Carles y Adolfo Hernández, *Estrategias nacionales de seguridad en el mundo* [en línea], Home Red Seguridad. Revista Especializada en Seguridad TIC, 23 de septiembre de 2014, Disponible en: http://bit.ly/2brTmOw.

Statement by the President on the Cybersecurity Framework [en línea], The White House, Disponible en: http://bit.ly/29pvewd.

Tendencias de seguridad cibernética en América Latina y el Caribe, Organización de los Estados Americanos, junio de 2014, p. 10, Disponible en: http://bit.ly/2a3Kr3t.

Texto cifrado en el logo del CYBERCOM (Actualizado) [en línea], Disponible en: http://bit.ly/1QuEwCZ.

The 2014 Quadrennial Homeland Security Review, Safeguard and Secure Cyberspace [en línea], Disponible en: http://1.usa.gov/25VQRKO.

The defence cyberstrategy [en línea], en Netherlands Ministry of Defence, 2012, Disponible en: https://ocdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf.

The DoD CyberStrategy, The Department of Defense [en línea], Disponible en: http://1.usa.gov/1iUMziZ.

The Industrial Control Systems Cyber Emergency Response Team [en línea], ICS-CERT, Disponible en: https://ics-cert.us-cert.gov/.

Toro Ibacahe, Lenisset, *El enfoque multidimensional de la seguridad hemisférica,* Estudios Latinoamericanos, N° 22, Año 1, Segundo semestre 2009, pp. 67-75.

Trejo Delarbre, Raul, *Derecho, delitos y Libertades en internet* [en línea], Disponible en: http://bit.ly/1X2W27n.

United States of America Military Strength [en línea], Disponible en: http://bit.ly/1K3i4z4.

United States The Departament of Defense [en línea], Disponible en: http://1.usa.gov/1ZRWdDG.

Wegener Henning, “La guerra cibernética” [en línea], *Política Exterior*, Vol. 15, No. 80 (Mar. - Apr., 001), pp. 131-142, 145-149, Publicado por: Estudios de Política Exterior S. A, Dirección URL: http://bit.ly/1LMiOgi.

Who are the cyberwar superpowers? [en línea], World Economic Forum, 4 de mayo de 2016, Disponible en: http://bit.ly/1NusZIu.

Why the worlds hould pay attention to cyberrisks [en línea], World Economic Forum, Disponible en: http://bit.ly/2al1tjI.

Wireless Systems for Industrial Invironments [en línea], NIST, Disponible en: http://www.nist.gov/el/isd/cs/wsie.cfm.

Yopo Boris, La nueva estrategia de seguridad de Estados Unidos [en línea], Friedrich Ebert Stiftung, julio de 2010, pág. 4, Disponible en: http://bit.ly/1ZzRzHN.

Anexo

Mapa en tiempo real de las ciberamenazas donde se proporciona información sobre los Estados Unidos de América, entre ellos el malware, el robo de información, la vulnerabilidad, entre otros. Para mayor información consúltese:

https://cybermap.kaspersky.com/, obtenido en septiembre, 2016.