UNIVERSIDAD NACIONAL AUTONOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

LA RESPUESTA DE ESTADOS UNIDOS ANTE EL CIBERTERRORISMO

T E S I S

QUE PARA OBTENER EL TÍTULO DE

L I C E N C I A D O E N RELACIONES INTERNACIONALES

P R E S E N T A:

AMAIRANI AKETZALLI MARTÍNEZ DUQUE

ASESOR: ÓSCAR NOÉ TORRES TECOTL

100 años de la fundación de las Relaciones Internacionales como disciplina científica

Ciudad Nezahualcóyotl, Estado de México, de 2021

INDICE

INTRODUCCIÓN

La sociedad internacional a lo largo de la historia ha sido testigo de diversas crisis, de las cuales se originarán una serie de problemáticas.

Actualmente en el S. XXI existe una crisis en seguridad internacional, como es la falta de respuesta ante nuevos fenómenos, resultado de distintos factores que ponen en peligro la estabilidad de los Estados, como: los religiosos, políticos, económicos o sociales, que originan choques de ideas entre grupos de presión y gobiernos.

La falta de una estrategia acertada a los nuevos fenómenos, ha provocado la agrupación de gobiernos en; foros, convenciones, tratados u organizaciones con el fin de mitigar los efectos de las problemáticas actuales, como el caso de Naciones Unidas, quien atiende diversos temas que preocupan a los gobiernos con el fin de mantener la paz y seguridad internacional, a través de órganos como el Consejo de Seguridad. Asimismo, del Consejo de Seguridad de Naciones Unidas surge el “Comité contra el Terrorismo”, quien aplicará resoluciones en materia de terrorismo.

Además de Naciones Unidas a la de seguridad internacional se suman organizaciones como; La Organización para la Seguridad y la Cooperación en Europa (OSCE), Comité Internacional de la Cruz Roja (CICR), El Foro Global contra el Terrorismo (FGCT), La Unión Europea.

Los Foros Internacionales son un instrumento que contribuye en la lucha contra fenómenos como; el terrorismo. Dentro de estos foros destaca el Foro Global contra el Terrorismo, que plantean medidas para detener la proliferación de los grupos terroristas alrededor del mundo, quienes son autores de escenarios catastróficos.

Pese a esfuerzos por mitigar el terrorismo, este sigue propagándose alrededor del mundo y fortaleciéndose a través del reclutamiento de jóvenes. Además, hoy en día migra a ámbitos como el digital, a través del cual amplifica sus efectos: ciberterrorismo.

El ciberterrorismo aprovecha características del ciberespacio, para causar afectaciones; tales como la velocidad a la que interactúa, el anonimato, los bajos costos a los que se realiza un ciberataque, la simultaneidad, entre otras. Asimismo, aprovechara la dependencia de la sociedad a la tecnología, misma que se lleva a Infraestructuras Críticas, las cuales su funcionamiento depende de sistemas informáticos, además

Cabe resaltar que dichas infraestructuras, son esenciales para la estabilidad nacional porque a través de ellas se puede causar daños severos, al disolver la línea que divide el ámbito digital del físico, por esta razón hoy en día es posible tener efectos en el ámbito físico a través del ciberespacio.

La red eléctrica es un ejemplo de la interdependencia alcanzada en sistemas sensibles para los Estados, debido a que controlan otros sistemas esenciales para la sociedad, es decir, afectar la red eléctrica podría tener efectos en serie.

Sin embargo, los daños ocasionados por ciberataques no siempre serán violentos ya que las herramientas digitales también se utilizan para obtener información estratégica de individuos, empresas o gobiernos, razón por la que también los propios gobiernos utilizan dichas herramientas para obtener ventaja sobre otros Estados o sabotearlos.

El sabotaje se dirigirá en diferentes vertientes, una de ellas la comercial, de la cual se origina la llamada guerra comercial por la que atraviesa la sociedad actual. Situación que no solo preocupa a las empresas sino también a los gobiernos ya que la economía se considera un pilar de la Seguridad Nacional.

El sector militar también se verá afectado por el ciberterrorismo, ataques que se han caracterizado por el robo de secretos industriales, como planos de naves militares o proyectos nucleares.

Para las Relaciones Internacionales el análisis del ciberterrorismo será importante porque dicho fenómeno atenta contra la seguridad nacional, derivado de las vulnerabilidades originadas en las Infraestructuras Críticas. Además, el estudio de este fenómeno digital también toma importancia dado que también los gobiernos utilizan la tecnología como un medio para posicionarse estratégicamente ante otros gobiernos, a través del robo de información.

La problemática se sitúa en la debilidad de la respuesta de los gobiernos ante el ciberterrorismo, al no ser suficiente para mitigar los efectos de dicho fenómeno el cual demanda un cambio de paradigma a la hora de plantear medidas de protección para el ciberespacio. Además, la ciberseguridad se convertirá en un reto por factores como; la velocidad a la que interactúa el ciberespacio. Cualidad que permite desarrollar nuevos programas maliciosos en poco tiempo, es decir, mientras las autoridades trabajan por detener un programa, diez más se desarrollan en otro punto de la red.

Para el gobierno de los Estados Unidos, el tema de la ciberseguridad también resultará un reto y su respuesta será insuficiente. Por ello esta investigación se desarrolla bajo la hipótesis de que;

"El ciberterrorismo constituye un fenómeno que atenta contra la estabilidad económica, financiera y social de los Estados Unidos y sobrepasa su capacidad de respuesta del gobierno estadounidense y sus agencias de inteligencia, en el ciberespacio”

Para ello se destacan los siguientes objetivos generales;

1. Dar algunos de los acontecimientos que marcan el inicio del fenómeno digital.
2. El Impacto del Ciberterrorismo para los diferentes actores de la sociedad.
3. La respuesta de los Estados Unidos hacia el Ciberterrorismo.

Además de los objetivos generales se desarrollarán los siguientes objetivos particulares;

1. El ciberterrorismo, como una nueva forma de desestabilizar una nación.
2. El término ciberespacio, el cual se considera un arma de doble filo para la sociedad del siglo XXI, porque además de beneficios traerá vulnerabilidades para esta.
3. Los Ciberataque, y el inicio de la carrera armamentista en el ciberespacio.
4. La Ciberguerra, que se considera como la guerra fría de la actualidad.
5. El Espionaje como una herramienta estratégica de la Guerra Fría que ha trascendido hasta el siglo XXI.
    - El ciberespionaje, herramienta indetectable que utilizarán tanto criminales como empresas y gobiernos.
    - Las practicas que las empresas implementan para incrementar sus ganancias; E-commerce.
6. La ciberseguridad como una forma de prevenir y mitigar las amenazas del siglo XXI.

7. El 11 de septiembre desde una perspectiva ciberterrorista.

8. El caso de Estonia, el cual muestra las consecuencias del alto grado de interconectividad en la sociedad.

9. Operación Buckshot Yankee como ejemplo de respuesta de Estados Unidos ante una crisis digital.

10. El impacto de la carrera armamentista digital. Donde se analiza:

- El caso de Stuxnet, quien se considera por especialistas en seguridad informática como el rostro de la guerra digital y se caracteriza por ser invisible, anónimo y devastador.
- Flame el código que reconceptualiza los retos de ciberseguridad.
- El caso de Gauss, amenaza que afecta al sector bancario y el cual señala a Estados Unidos como principales sospechosos de su creación.

11. La importancia de la Información la cual es considerada como el Petróleo de la era digital, dado el valor que adquiere.

12. Las consecuencias para los Estados Unidos de tener un ciberespacio inseguro.

13. El Ciberterrorismo como un enemigo de las grandes empresas, quienes son uno de los principales objetivos de los criminales.

14. Las Infraestructuras Críticas quienes se consideran como un medio de Desestabilidad Nacional.

15. La lucha que surge entre Estados Unidos y China por el poderío mundial. Donde además se analizan acontecimientos como;

- La Operación Aurora, un caso de ciberespionaje económico con intereses políticos.
- El Grupo Shanghái considerado una de las bases militares chinas a través de la cual busca dominar la información.

16. Las acciones que el gobierno de los Estados Unidos implementa para mitigar los efectos del ciberterrorismo.

17. Los Planes, proyectos y acciones de la inteligencia estadounidense contra el ciberterrorismo. En donde se revisará agencias como;

- La NSA y su línea de acción contra el ciberterrorismo.
- El FBI que destaca como organismo líder en la investigación de ciberdelitos.
- El Departamento de Seguridad Nacional, y sus acciones para la detección y prevención de las amenazas que surgen en el ciberespacio.
- Los alcances del Pentágono en materia de ciberseguridad.
- El Centro de Integración de Inteligencia contra la Amenaza Cibernética, considerado como un organismo de investigación y atención para la nueva era del terrorismo.

Con base a los objetivos anteriores, el primer apartado de esta investigación se integrará por una serie de conceptos fundamentales para entender el fenómeno del ciberterrorismo. El cual será considerado como la transición del terrorismo al ámbito digital, donde el ciberespacio es la herramienta clave para alcanzar sus fines.

El ciberespacio se considerará un arma de doble filo, porque eficientiza procedimientos de servicios básicos para la sociedad y sistemas que conforman la estructura de los países donde se generará una dependencia con dicho medio, dependencia que originará vulnerabilidades en los sistemas que su funcionamiento depende de los sistemas informáticos. Las vulnerabilidades que surgen pondrán en peligro a la sociedad, empresas y gobiernos, como consecuencia de la carrera armamentística que surge en el ciberespacio.

También se observará la inversión de los países en la carrera armamentista digital, lo cual justificaran como un medio de defensa ante las amenazas digitales. Situación que ha generado escenarios de ciberguerra entre algunos países.

El término ciberguerra, forma parte del primer capítulo y representará uno de los conceptos que hace hincapié en el cambio de paradigma que demanda el ámbito digital. Porque para clasificar un acto como actos de ciberguerra no se tomarán en cuenta los mismos elementos que se consideran en la guerra tradicional.

De igual manera se plantearán prácticas que trascendieron a lo largo de la historia de las Relaciones Internacionales, por sus aportaciones como el Espionaje quien, además, se

considera una herramienta estratégica de la Guerra Fría, que en actualidad migra al ámbito digital, de quien se apoyará para lograr sus propósitos.

El ciberespionaje se utilizará contra empresas y gobiernos con el fin de obtener información estratégica, donde la popularidad de las empresas como objetivo para ciberataques radicara en el valor de estas para la economía de los Estados la cual, además, es uno de los pilares de seguridad nacional.

La ciberseguridad, es otra de las definiciones planteadas en esta investigación, la cual surgirá de la necesidad por hacer frente al fenómeno informático. Donde la respuesta de los gobiernos deberá estar dirigida a medidas de prevención y no de contraataque debido a que en ámbito digital contraatacar no es eficiente, como podría serlo los ámbitos físicos.

Para el segundo apartado de esta investigación, se describirán algunos acontecimientos que marcarán el inicio y la evolución del fenómeno digital que experimenta la sociedad actual.

El 11 de septiembre de 2001 será uno de los acontecimientos que, aunque no se considera un ataque ciberterrorista, demuestra la importancia de los sistemas informáticos en infraestructuras esenciales de la sociedad tales como el sistema de telecomunicaciones. Con este acontecimiento se exponen algunos de los efectos que, interrumpir el funcionamiento de estas infraestructuras, puede ocasionar. Además, el 11 de septiembre marcará el comienzo de una era de dependencia de la sociedad a la tecnología.

La dependencia tecnológica quedará reflejada con acontecimientos como los ocurridos en Estonia, quien se caracterizará por ser una nación altamente dependiente de la tecnología. Al grado que una falla en la red informática del país, podría dejar a este aislado del mundo exterior, como en 2007.

Con los atentados a Estonia se demostrará que, el ciberterrorismo puede estar motivado por diversos factores como, los políticos, culturales, económicos e incluso una mezcla de todos los anteriores, como será el caso de la Operación Aurora, de la cual se hablará más adelante.

Dentro del tercer capítulo se analizarán los efectos del ciberterrorismo, donde se expondrá el impacto que este tiene dentro de la sociedad. Se iniciará revisando el impacto que la carrera armamentista digital tiene para la sociedad y en general para los Estados.

Dentro del apartado que corresponde a la carrera armamentista se plantearán algunos ejemplos de las armas cibernéticas que se han detectado actualmente, y que lograrán poner en riesgo algunos puntos sensibles de los países.

Dentro de las armas digitales destacarán casos como el de Stuxnet, Flame o Gauss, quienes no representan todo el universo de ciberarmas registradas en la historia, pero, que son algunos de los casos que sobresalen por el impacto que alcanzarán.

Los ciberataques mostrarán el valor que la información ha adquirido en la era digital, valor que se podría comparar con el valor que el petróleo tiene para las naciones. Analogía dirigida en el sentido de que, por obtener estos recursos, las naciones podrían terminan en guerras. Asimismo, los ciberataques generarán pérdidas que se dirigen en distintas vertientes, como pueden ser económicas o intelectuales.

El ámbito militar registrará robos de planos de vehículos, armamento e incluso el robo de programas informáticos que desarrolla la inteligencia de los países. Las empresas también se volverán objetivo de los ciberataques, las cuales registrarán a diario pérdidas intelectuales que se traducen en pérdidas económicas, pérdidas que implicarán repercusiones en la economía del país, cuando se trata de empresas nacionales.

Las Infraestructuras Criticas representarán otro medio a través del cual se podrá causar daños a los Estados ya que se consideran como el sistema nervioso de los Estados, de ahí la importancia por protegerlas ante el fenómeno digital.

El ciberterrorismo generará tensiones entre los gobiernos como en el caso de Estados Unidos y China, quienes serán protagonistas de la denominada guerra comercial que se desarrolla en el ciberespacio. La guerra comercial se caracterizará por el interés de China por alcanzar el desarrollo económico que necesita para posicionarse como una potencia mundial, poder que pretende obtener a través del robo de información y proyectos principalmente de países como Estados Unidos, quien ha representado en los últimos años un modelo del desarrollo.

El interés de China por obtener información clave para constituirse como potencia mundial, originará proyectos del gobierno como; Grupo Shanghái, quien se rige por una política de dominio de la información y surge con el fin de formar un ciberejército, que tiene como objetivo reclutar y entrenar jóvenes para la ciberguerra. Otra función de dicho grupo será investigar como interactúa el ciberespacio para poder protegerlo.

El ataque a Google denominado Operación Aurora se relaciona con el Grupo Shanghái y mostrará que distintos factores motivan los ciberataques, como los intereses políticos y económicos que caracterizaron dicha operación.

En el último capítulo se planteará la respuesta de Estados Unidos y sus agencias ante el ciberterrorismo. Donde destacan agencias establecidas desde acontecimientos como el 11 de septiembre en 2001 y otras que surgen en la actualidad, de la necesidad por proteger el ciberespacio.

TEORIA DE LA INTERDEPENDENCIA COMPLEJA

Para esta investigación se empleará la teoría de la interdependencia compleja. Teoría creada por Keohane y Nye en los años 70. La intención de dicha teoría proponer una alternativa para explicar la complejidad de las relaciones trasnacionales, relaciones que sobrepasan el planteamiento realista, donde se propone al Estado como el único ente que trabaja por la seguridad nacional.

Respecto al tema del Estado como principal actor que trabaja para la Seguridad Nacional, Keohane y Nye plantean los múltiples canales, que es uno de los principales elementos que caracterizan la Teoría de la interdependencia compleja. Los múltiples canales plantean, como la sociedad en la actualidad se conectan en una multiplicidad de ámbitos, donde existe una participación tanto de entes gubernamentales como no gubernamentales, provocando el surgimiento de nuevos actores distintos al Estado, mismos que han ido ganando relevancia en asuntos internacionales y nacionales como es el tema de seguridad nacional.

Entre estos nuevos actores que la interdependencia compleja menciona, que han surgido y ganado relevancia tanto en las relaciones internas como externas de un país, se encuentran actores como los bancos y empresas multinacionales. El surgimiento de nuevos actores ha originado la disolución de la línea divisora entre el sector público y el privado en cuestiones de política. Aunado a esto la interdependencia plante el cómo los Estados han encontrado la forma de incrementar su poder a través de alianzas. Alianzas que pueden ser con otros Estados o incluso como se menciona con otros actores de la sociedad internacional.

Esta teoría también se caracteriza por la ausencia de jerarquía entre los distintos asuntos internacionales, característica donde existe un desplazamiento de la seguridad militar, es decir, la seguridad militar ya no domina la agenda de los Estados y aunado a ello se da la última característica que es la reducción del uso de la fuerza militar.

Este último elemento que caracteriza la interdependencia se plantea que la fuerza militar ya no es un medio utilizado por los Estados para obtener sus objetivos, al ser una acción que no asegura su eficacia y que suele ser costosa, además, existen otras prácticas que permiten tomar acciones contra otros Estados sin el riesgo de recibir represalias, como el terrorismo o el factor económico.

Por ejemplo, la teoría de la interdependencia compleja considera el uso de la fuerza una acción innecesaria para conseguir el bienestar económico o ecológico, los cuales son posibles a través del uso de otras herramientas tales como la tecnología, como ocurre en el ciberterrorismo.

El ciberterrorismo es un fenómeno que cambia la manera de entender y efectuar la guerra, el terror y el ejercer presión hacia las figuras de poder, entre los cambios provocados por dicho fenómeno, se encuentra un desplazamiento de la figura del Estado como actor principal, tal y como se menciona en la teoría de la interdependencia compleja, tanto en el alta como en la

baja política. Dicho desplazamiento se debe al surgimiento de nuevos actores, que han adquirido mayor participación en la sociedad, como pueden ser las empresas, grupos de presión, entre otros.

A lo largo de esta investigación se podrá observar los nuevos actores que surgen dentro del escenario internacional, tales como las empresas, quienes, en la actualidad tienen una participación más allá del factor económico y hoy en día son parte de la toma de decisiones de los gobiernos e incluso, en casos como en el de Estados Unidos son un pilar para la Seguridad Nacional.

Cabe mencionar, que el sector económico es parte de los pilares de Seguridad Nacional a partir de los acontecimientos del 11 de septiembre de 2001. Al observarse los efectos que un ataque a dicho sector puede ocasionar al país, por dicha razón el gobierno hizo a las empresas participes en la seguridad nacional a través del “Act Patriot”, donde se planteó la necesidad de la colaboración gobierno – empresas, sin dejar opción de elección a las empresas, es decir, aquellos que no colaboren con el gobierno se declaran en contra de este.

La participación del sector empresarial en los temas de seguridad nacional, es la muestra de las incapacidades de un gobierno respecto a ciertos temas, situación que se podrá visualizar en esta investigación, con la ciberseguridad, donde son las empresas uno de los principales proveedores de servicios para mantener seguro el ciberespacio.

Respecto a la seguridad nacional las empresas han destacado con su participación en fenómenos como el ciberterrorismo, debido a que este demanda nuevas estrategias de seguridad que protejan el ciberespacio y la infraestructura nacional, porque así como entre los países y los diferentes actores se ha originado una independencia para su funcionamiento, de la misma manera ocurre entre la tecnología y las diferentes partes que componen la estructura interna de un país, debido a que hoy en día una cantidad considerable de cosas dependen de la tecnología para su funcionamiento.

Además, el uso de la tecnología como un elemento en la seguridad ha producido una reducción del uso de la fuerza tanto por parte de criminales como de gobiernos, como lo menciona la Teoría de la Interdependencia Compleja, la cual plantea un desplazamiento de la seguridad militar, que es un método costoso y poco certero, donde un enfrentamiento militar representa pérdidas económicas y humanas.

Es decir, actualmente los gobiernos prefieren el uso de herramientas, como el ciberespacio, para conseguir sus objetivos o atacar a otras naciones, porque dicha herramienta les da la certeza de no recibir represalias como en un ataque físico, ya que, en el ciberespacio, al contar con el anonimato, significa que el afectado tardara en descifrar quien es el atacante e incluso es posible que nunca lo sepa con exactitud.

Sin embargo, pese a la disminución del uso de la fuerza militar dentro de los gobiernos, no significa que dicho elemento se haya eliminado por completo de las estrategias de seguridad, incluso en casos como el de Estados Unidos se trabajan en iniciativas que involucren al ejército dentro del tema de ciberseguridad, como es el caso de los cibercomandos.

Finalmente, otra de las características de la Teoría de la interdependencia compleja, es la disolución de fronteras entre los Estados, resultado de la dinámica internacional actual, además, existen elementos, como el ciberespacio, que influyen en la disipación de dichas fronteras, debido a que, en el ciberespacio no existen divisiones o límites entre un país u otro, el ciberespacio es una herramienta que globaliza la información incluso el comercio y desde cualquier punto del globo terráqueo se puede buscar información, comprar o incluso atacar a otras naciones a través de Internet.

Por estas razones se ha elegido la teoría de la interdependencia para explicar esta investigación, porque, si bien es cierto la teoría de la interdependencia compleja, plantea, una cooperación económica entre naciones, también es cierto que en la actualidad existe una cooperación entre los gobiernos y otros actores como son las empresas para cumplir sus objetivos.

1. MARCO TEÓRICO CONCEPTUAL.

Este primer apartado se compone por una serie de conceptos base para definir y entender el ciberterrorismo; transición del terrorismo al ámbito digital, para aprovechar las cualidades del ciberespacio y alcanzar sus objetivos mediante el daño de sistemas que, componen la estructura de los Estados a través de las cuales se desestabiliza los gobiernos.

También se planteará el concepto de ciberespacio; considerado un arma de doble filo porque además de facilitar la vida cotidiana con la automatización de procesos, igualmente genera vulnerabilidades que afectan a la sociedad. Dichas vulnerabilidades afectan la información depositada en el ciberespacio y ciertas infraestructuras en donde fenómenos como el ciberterrorismo o los ciberataques podrían poner en peligro la vida de las personas.

El término ciberataque hace referencia a los programas maliciosos que hoy en día son parte de la carrera armamentista desarrollada en el ámbito digital, misma que es posible por las características del ciberespacio como; la velocidad a la que interactúa dicho ámbito, la simultaneidad y el anonimato, que permiten el desarrollo de ciberarmas.

Pese al anonimato existente en el ciberespacio, se acusa a los gobiernos de la creación de ciberarmas, lo cual se deduce de las características de los programas. Acusaciones que generan tensiones entre los Estados y en ocasiones estados de ciberguerra.

La ciberguerra representa un cambio de paradigma, porque no cumple todos los elementos que se consideran en la guerra tradicional. Como ocurre con la violencia, la cual puede o no existir en un ciberataque, incluso la ciberguerra se caracteriza por reducir el uso de la fuerza en los enfrentamientos.

El espionaje es una herramienta que trascenderá a lo largo de la historia de las Relaciones Internacionales, que migra al ámbito digital originando el ciberespionaje; el cual amplia las capacidades del espionaje a través del uso de la tecnología y es un elemento clave en la estructura de programas maliciosos que pone en peligro la información de gobiernos y empresas.

Del espionaje digital se deriva el ciberespionaje empresarial, quien se mueve en dos direcciones; en la primera participa las empresas que recurren a estas practicas con el fin de sabotear proyectos de la competencia. Mientras que en la otra dirección se encuentran los gobiernos quienes se infiltran en la información de las empresas con el fin de favorecer la industria nacional.

Además, las empresas a través de la tecnología han logrado obtener beneficios mediante métodos como; el E-commerce, a través del cual se da la globalización de los productos, llevándolos a más personas alrededor del mundo, lo que se traduce en un incremento de ingresos.

1.1. EL CIBERTERRORISMO, UN MEDIO PARA DESESTABILIZAR UNA NACIÓN.

Como parte del marco teórico de esta investigación, el primer concepto a revisar es el de ciberterrorismo, fenómeno que es considerado como un medio de desestabilidad nacional.

Mark Pollit, agente especial del Buró Federal de Investigaciones (FBI), es uno de los primeros en definir el ciberterrorismo y lo define como; "El ciberterrorismo es el ataque premeditado y políticamente motivado contra la información, los sistemas informáticos, los programas de computadora y los datos, que provoca violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos."[1] Sin embargo, hoy en día existen diversos factores que, además del factor político, motivan el ciberterrorismo.

Mauricio Meschoulam menciona que; "El ciberterrorismo no es otra cosa más que una subcategoría de terrorismo; es simplemente el empleo de herramientas distintas para conseguir los mismos fines; la provocación de un estado de shock o terror colectivo con el objetivo de trasmitir mensajes o reivindicaciones políticas utilizando ese terror como canal, para, así inducir afectaciones a opiniones, conductas y/o toma de decisiones en determinado sector de una sociedad".[2] Es decir, es la transición del terrorismo al ámbito digital para lograr sus fines a través del robo de información y del uso de la tecnología.

Dorothy Dennigal complementa mencionando que el ciberterrorismo; "es la convergencia entre el terrorismo y el ciberespacio, una conjunción de fuerzas que, utilizando las ventajas y capacidades del terrorismo físico, ahora basado en fallas y vulnerabilidades tecnológicas, logran intimidar o presionar a un Estado y sus ciudadanos."[3] Sí el ciberterrorismo se ha convertido en un medio de presión para los Estados se debe a la dependencia hacia los medios digitales, para el funcionamiento de los sistemas que conforma la estructura nacional.

Dan Verton describe el ciberterrorismo como; "la ejecución de un ataque sorpresa por parte de un grupo (o persona) terrorista extranjero subnacional con objetivos políticos utilizando tecnología informática e Internet para paralizar o desactivar las infraestructuras electrónicas y físicas de una nación, provocando de este modo la pérdida de servicios críticos, como energía eléctrica, sistemas de emergencia telefónica, servicio telefónico, sistemas bancarios, Internet

---

[1] Verton D. (2004). *Black Ice: Los Peligros Ocultos del Ciberterrorismo*. En Black Ice: La Amenaza Invisible del Ciberterrorismo (p.29). Madrid: McGraw-Hill.

[2] Meschoulam M. (octubre 30, 2015). *Ciberguerra y Ciberterrorismo: ¿Presente o Futuro?*. Septiembre,19, 2017, de El Universal Sitio web: http://www.eluniversal.com.mx/entrada-de-opinion/articulo/mauricio-meschoulam/mundo/2015/10/30/ciberguerra-y-ciberterrorismo.

[3] Estévez A. (marzo 22, 2011). *La Lucha Contra el Ciberterrorismo*. enero 5, 2018, de Red Safe World Sitio web: https://redsafeworld.wordpress.com/2011/03/22/la-lucha-contra-el-ciberterrorismo/.

y otros muchos. El objetivo de un ataque ciberterrorista no es solo impactar la economía de una región o país, sino amplificar los efectos de un ataque terrorista físico tradicional provocando confusión y pánico adicionales en la población en general"[4]

En resumen, el ciberterrorismo para esta investigación se entenderá como un medio para desestabilizar una nación, al ser un fenómeno que atenta contra infraestructuras esenciales en el funcionamiento de los Estados.

1.2. EL CIBERESPACIO, EL ARMA DE DOBLE FILO DEL SIGLO XXI.

Para que el ciberterrorismo sea posible es necesario la existencia de herramientas como el ciberespacio, el cual se define como; "El espacio virtual determinado por la conexión de personas a través de redes, la primera vez que se mencionó esta palabra, fue por el escritor norteamericano William Gibson en una de sus novelas, esto fue en el año 1984" [5], novela denominada "Neuromante".

El "**Ciberespacio.** Se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. En el ciberespacio, los operadores del equipo pueden interactuar de manera similar al mundo real, a excepción que la interacción en el ciberespacio no requiere del movimiento físico más allá que el de escribir. La información se puede intercambiar en tiempo real o en tiempo diferido, y la gente puede comprar, compartir, explorar, investigar, trabajar o jugar".[6] Es decir, es un medio que permite realizar una serie de actividades y funciones debido a los elementos que lo componen.

El ciberespacio no solo hace referencia a un monitor y conexión a internet, el autor Julián Alfonso menciona que; "más allá de internet existe aún todo un conjunto de redes que teóricamente están separadas de ella, redes transaccionales de flujos de dinero, operaciones del mercado de valores, transacciones de las tarjetas de crédito, redes de control de servicios, transporte, seguridad, redes dotadas de dispositivos de sensorización y control. El conjunto de todas estas redes conforma el ciberespacio."[7] Dichas redes permiten que el ciberespacio sea multifuncional.

---

[4] Verton D. (2004). *Introducción*. En Black Ice: La Amenaza Invisible del Ciberterrorismo (p. xxvii). Madrid: McGraw-Hill.

[5] Tecnologicon. (julio 6, 2015). *Definición de Ciberespacio*. marzo 3, 2019, de Tecnologicon Sitio web: https://tecnologicon.com/definicion-de-ciberespacio-informatica/.

[6] EcuRed. *Ciberespacio*. marzo 6, 2019, de EcuRed Sitio web: https://www.ecured.cu/Ciberespacio

[7] Alfonso J. (septiembre 2015). *Ciberespacio e Internet.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema Nacional de Seguridad. (p.49) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.

El ciberespacio también se define como una dimensión sin fronteras y poco regulada donde las amenazas pueden materializarse. María José Caro complementa diciendo; “En el mundo actual ha surgido una nueva dimensión donde pueden materializarse las amenazas: el ciberespacio. Si antes en el ámbito de la defensa estaba claro que nos movíamos en las tres dimensiones de tierra, mar y aire, e incluso el espacio, ahora contamos con una dimensión adicional, y más intangible que las anteriores. El ciberespacio no tiene fronteras, es un nuevo campo de batalla del siglo XXI, aunque ya se intuyó a finales del siglo XX.”[8]

El espacio virtual, también se caracteriza por el anonimato y la inexistencia de fronteras físicas que permiten, la información fluya sin restricciones de un punto a otro. Romero Nerea menciona que; “El **ciberespacio** es hoy el ejemplo más claro de un ámbito accesible, poco regulado y de difícil control … El ciberespacio, un nuevo ámbito de relación que ha proporcionado el desarrollo de las nuevas tecnologías de la información y las comunicaciones, ha diluido las fronteras, permitiendo una globalización sin precedentes, que propicia nuevas oportunidades, pero conlleva serios riesgos y amenazas.”[9]

En resumen, el ciberespacio es medio poco regulado a través del cual la información fluye de un punto a otro sin restricciones, y permite el desarrollo de otras tecnologías que aportan beneficios y vulnerabilidades para la sociedad, por lo que se considera un arma de doble filo.

1.3. CIBERATAQUES, EL INICIO DE LA CARRERA ARMAMENTISTA EN EL CIBERESPACIO.

El término ciberataques es uno de los conceptos que con mayor frecuencia se repetirá a lo largo de esta investigación, por ello es necesario definirlo.

De acuerdo al Manual de Tallin sobre el Derecho Internacional en Ciberguerra los ciberataques son; “Aquella operación cibernética, ofensiva o defensiva, de la que se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas o daños o destrucción de bienes.”[10]

En complemento al Manual de Tallin, un ciberataque es una acción digital o informático con posibles consecuencias en el ámbito físico, tal como lo define el gobierno de los Estados

---

[8] Caro M. *Alcance y Ámbito de la Seguridad Nacional en el Ciberespacio*. (p.5). junio 14, 2017, Sitio web: http://www.ieee.es/Galerias/fichero/cuadernos /CE_149 _Ciberseguridad.pdf.

[9] Romeo N. (agosto 8, 2016). *La Amenaza Cibernética: Ciberguerra y Ciberdefensa*. octubre 31, 2017, de CISDE Sitio web: https://observatorio.cisde.es/archivo/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa/.

[10] Soesanto S. (octubre 1, 2016). *No todos los ataques son ciberataques*. octubre 3, 2017, de EL País Sitio web: https://elpais.com/tecnologia/2016/09/28/actualidad/1475059265_198963.html.

Unidos; “Una acción deliberada para alterar, interrumpir, engañar, degradar, o destruir sistemas informáticos o redes de información y/o programas alojados o en tránsito por esos sistemas o redes … los ciberataques se diferencian de los ataques convencionales en sus medios y sus fines. En lugar de emplear herramientas cinéticas (por ejemplo, el puño, una bomba o una espada), un ciberataque utiliza herramientas digitales (básicamente, ordenadores y otros dispositivos inteligentes). Un ciberataque siempre golpea primero un sistema informático, en lugar de un blanco físico. Es posible que de ese golpe se derive un daño físico para alguien o para algo, pero el primer impacto siempre es sobre un ordenador.”[11]

Los ataques digitales tienen la capacidad de realizarse a distancia sin la necesidad del agresor exponerse físicamente. En este sentido Francisco Ureña señala lo siguiente; “Puede producir daños en cualquier escala y en cualquier lugar: a través de Internet, el alcance de los ataques se puede realizar en cualquier escala y además sobre infraestructuras situadas en cualquier parte del mundo, sin ningún tipo de restricción por la distancia a la que se encuentre el objetivo. Pueden paralizar servicios básicos: tanto para la población en general, como las infraestructuras de cualquier país, que a su vez puedan producir un efecto dominó en otros servicios dependientes de los primeros, hacen de los ciberataques un peligro mucho mayor que cualquier método de ataque convencional.”[12]

Alejandro Suárez en su libro “El quinto elemento” cita a los autores Peter W. Singer y Allan Friedman, quienes resaltan algunas de las características de los ciberataques. “Tal como señalan Peter W. Singer y Allan Friedman en su libro Cybersecurity and cyberwar, un ciberataque se mueve, literalmente, a la velocidad de la luz y no se detiene ante fronteras físicas o políticas. Además, sin ser divino, es ubicuo: puede tener lugar en varios lugares al mismo tiempo … Un ciberataque es mucho más difícil de identificar y atribuir que un ataque convencional. En muchas ocasiones, sólo se puede tener la sospecha de que el ciberataque se ha iniciado en un determinado país, pero resulta muy complicado asegurar quién es el responsable.”[13]

En síntesis, por ciberataques se entenderá, aquel ataque implementado mediante un medio informático, el cual puede tener efectos en el espacio físico. Así mismo este tipo de ataques, por sus características, se vuelve menos riesgoso y costosos para los criminales.

---

[11] La Razón. (mayo 15, 2017). *El próximo 11-S empezará con un click*. octubre 3, 2017, de La Razón Sitio web: https://www.larazon.es/blogs/cultura/todo-esta-en-los-libros/el-proximo-11-s-empezara-con-un-click-EB15147641/.

[12] Ureña F. (enero 16, 2015). *Ciberataques, la mayor amenaza actual*. (p.14). mayo 15, 2020, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf.

[13] Suárez A. (2015). *Cibercrimen*. En El Quinto Elemento (pp.39,94). España: Deusto S.A. Ediciones.

1.4. CIBERGUERRA, LA GUERRA FRÍA DE LA ACTUALIDAD.

A continuación, se definirá el término ciberguerra, quien es la continuación de la guerra en el ámbito digital y la reconceptualización de lo tradicional. “Si, como dijo Clausewitz, la guerra es la continuación de la política por otros medios, la ciberguerra es la continuación de la guerra tradicional por otros medios. La ciberguerra aúna elementos de los conflictos clásicos con elementos de sabotaje, hacking, espionaje y ataques cibernéticos que facilita internet.”[14]

En complemento al autor Clausewitz, la ciberguerra busca cumplir los objetivos de la guerra mediante el uso de la tecnología, sus principales armas son los programas maliciosos quienes son de producir apagones en ciudades enteras, que representa un problema cuando dicha acción afecta otros sistemas como el bancario o sistemas que controlan infraestructuras sensibles, como plantas nucleares. “La guerra cibernética es una nueva forma de guerra, pero silenciosa. Sobre todo, por el secreto con el que la llevan los gobiernos. Sus principales armas, aunque no son reconocidas como tales, son programas maliciosos capaces de apagar las luces de una ciudad entera, bloquear los circuitos de una central energética o dejar sin recursos a un hospital.”[15]

Además, la ciberguerra es una guerra silenciosa derivado de la capacidad de las ciberarmas de camuflajear los cambios que realizan en los sistemas infectados y que parezca que trabajan con normalidad.

En este sentido Alejandro Suárez define el ciberespacio como un elemento más donde la guerra puede materializarse; “La irrupción de internet como quinto campo de batalla, como quinto elemento, ha hecho la guerra más compleja que nunca. La ciberguerra es un gran conflicto en el que a menudo no sabemos quién es el enemigo que nos ataca, y esta incertidumbre ha conducido a los Estados a tomar una medida concreta de precaución: considerar que todos son enemigos.”[16] La complejidad de esta faceta de la guerra se deriva de elementos que caracterizan a las ciberarmas como; el anonimato, el ser indetectables y la velocidad a la que actúan.

“Richard Clarke, especialista en seguridad del gobierno de Estados Unidos, define la guerra cibernética como el conjunto de acciones llevadas por un Estado para penetrar en los

[14] Suárez A. (2015). Ciberguerra. En El Quinto Elemento (p.176). España: Deusto S.A.

[15] Bañuelos E. (marzo 10, 2016). *La Próxima Guerra Mundial Será Cibernética*. noviembre 11, 2017, de Código Nuevo Sitio web: https://www.codigonuevo.com/sociedad/proxima-guerra-mundial-cibernetica.

[16] Suárez A. (2015). Ciberguerra. En El Quinto Elemento (p.176). España: Deusto S.A.

ordenadores o en las redes de otro país, con la finalidad de causar prejuicio o alteración."[17] En complemento para clasificar un acto como ciberguerra también se consideran características como; los sistemas que afectan y sus fines, que a diferencia del cibercrimen no se basa en el robo de dinero.

El cambio que representa la ciberguerra es que su principal fin no es la violencia, sin embargo, esta puede ser una consecuencia cuando las ciberarmas atacan sistemas sensibles para un país. Se considera un fenómeno no violento porque su principal objetivo es el robo de información estratégica, aunque, en ocasiones también busca causar daños a infraestructuras críticas. "Tal como apuntó Walter Laqueur, consejero del Centro de Estudios Internacionales y Estratégicos, en Washington quizá no sea de importancia primordial la cuestión de que «la guerra implica violencia» si los ataques cibernéticos logran infligir daños inaceptables al enemigo aun sin matar a nadie. El fin último de un Estado que libra una guerra no es el de producir la violencia por la violencia, sino el de alcanzar un objetivo político y/o económico. La guerra siempre se ha tratado de eso: intereses; y la violencia es sólo un medio en el camino hacia su consecución. Históricamente, no todas las guerras han implicado violencia física directa. La guerra fría se basó en una carrera de armamentos nucleares que garantizaba la destrucción mutua asegurada de los dos polos rivales; es decir, estaba movida en mayor medida por la disuasión que por la violencia."[18]

En resumen, la ciberguerra es la guerra fría del siglo XXI al no existir un ataque declarado, pero, que la sociedad internacional es consciente de que existe la amenaza y se puede tener efectos violentos derivado de la dependencia de la sociedad hacia la tecnología, para su funcionamiento. Es decir, se puede colapsar a un Estado a través de interrumpir el funcionamiento de sistemas básicos que formen parte de la estructura nacional.

1.5. EL ESPIONAJE, UNA HERRAMIENTA ESTRATÉGICA DE LA GUERRA FRÍA.

El espionaje como se mencionó es una herramienta base para la creación de nuevas amenazas en el medio digital, por ello la importancia de definirlo. El valor que cierta población da a dicha práctica radica en la información estratégica (de individuos, empresas o gobiernos) que a través de ella se puede obtener.

---

[17] Romeo N. (agosto 8, 2016). La Amenaza Cibernética: Ciberguerra y Ciberdefensa. octubre 31, 2017, de CISDE Sitio web: https://observatorio.cisde.es/archivo/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa/.

[18] Suárez A. (2015). Ciberguerra. En El Quinto Elemento (p.176). España: Deusto S.A.

Adolfo Arreola plantea; “El espionaje es tan antiguo como el hombre mismo, comprende una serie de actividades para negar el acceso a información estratégica y descifrar los más preciados secretos del enemigo a través de conseguir información clasificada, misma que es obtenida por métodos, técnicas y medios de una amplia variedad, pero principalmente de la observación. Un programa de espionaje/ inteligencia se define como una serie ordenada de actividades, secretas o no, que están encaminadas a obtener información estratégica sobre un Estado, organismo o individuo en los diversos campos del poder, a fin de lograr el objetivo planificado en las relaciones con dichos actores.”[19] Además se define como una herramienta que a lo largo de la historia ha contribuido en la toma de decisiones como el establecer relaciones o no entre Estados. “El espionaje ha sido y es esencial para el desarrollo de las actividades del ser humano, ya que toda decisión de gobierno se basa en el conocimiento y comprensión plena de la situación, lo que se obtiene a través de la vigilancia, observación y análisis del entorno.”[20]

Asimismo, es un elemento de las agencias de inteligencia de los gobiernos como, en el caso de Estados Unidos. “Cuando las actividades de inteligencia están orientadas a tomar ventaja y robar información personal, industrial, económica, secreta o vital, utilizando principalmente medios clandestinos o ilegales, se define como espionaje.”[21]

En síntesis, el espionaje es una herramienta de la guerra fría que se ha implementado a lo largo de la historia de las Relaciones Internacionales como un medio para obtener información estratégica de otros, esto con el fin de tomar decisiones, establecer o no relaciones u obtener alguna ventaja sobre los demás.

Finalmente, al igual que otras prácticas migra al ámbito digital con el fin de ampliar los medios a través los cuales obtiene sus objetivos, dando origen al ciberespionaje.

---

[19] Arreola A. (2015). *En Ciberespionaje: La puerta al mundo virtual de los estados e individuos, una revisión de los programas de espionaje digital de los Estados Unidos* (pp. 211, 214). México: Siglo XXI editores.

[20] Arreola A. (2015). *Criptografía*. En Ciberespionaje: La puerta al mundo virtual de los estados e individuos, una revisión de los programas (p.52). México: Siglo XXI editores.

[21] Arreola A. (2015). *¿Inteligencia o Espionaje?*. En Ciberespionaje: La puerta al mundo virtual de los estados e individuos, una revisión de los programas de espionaje digital de los Estados Unidos (p.23). México: Siglo XXI editores.

1.5.1. CIBERESPIONAJE, EL SECRETO DE SER INDETECTABLE EN EL CIBERESPACIO.

Como se introdujo, el ciberespionaje es el resultado del uso de la tecnología en prácticas como el espionaje. “En internet, el espionaje o ciberespionaje, consiste en la misma obtención de información y datos, pero utilizándose como medio la tecnología a través de internet, para acceder a informaciones que se encuentran en soportes informáticos o tecnológicos. Los datos que se persiguen obtener con más frecuencia son los relativos a propiedad intelectual e industrial, patentes, y datos bancarios o económicos, de empresas o industrias.”[22]

El ciberespionaje, también tiene como objetivo obtener información de manera clandestina con el uso de la tecnología, misma que permite a los criminales la mayoría de las veces no ser detectado. Además, se caracteriza por elementos como los que Adolfo Arreola plantea; “El secreto, ser indetectables, y la persistencia son las características primordiales de los sistemas de inteligencia y espionaje digital, por lo que los sistemas de espionaje no escatiman esfuerzos para evitar ser detectados o evidenciados, siendo la criptología la herramienta preferida para mantener intacto el secreto de los mensajes.” [23]

La tecnología empleada en el ciberespionaje se caracteriza por ser sofisticada para mantener en el anonimato a los criminales, razón por la que dicho fenómeno se asocia con empresas y gobiernos en la creación de programas maliciosos. “Generalmente, los programas de espionaje/ inteligencia digital tienen por características principal el secreto, pero también incluyen detalles únicos como:

- Ser intrusivos.
- Consistir de implante físico, virtual o una combinación de ambos.
- Ser patrocinados generalmente por las agencias de seguridad estatales o grandes empresas.
- Contar con gran capacidad de almacenamiento de datos.
- Atentar contra la seguridad nacional.

Manipular, alterar, destruir, negar o degradar la información contenida en computadoras, redes de computadoras o en la red de Internet misma.”[24]

---

[22] CiberDerecho. *¿Qué es el ciberespionaje Industrial?*. marzo 11, 2019, de CiberDerecho Sitio web: http://www.ciberderecho.com/que-es-el-ciberespionaje-industrial/.

[23] Arreola A. (2015). *En Ciberespionaje: La puerta al mundo virtual de los estados e individuos, una revisión de los programas de espionaje digital de los Estados Unidos* (p. 34). México: Siglo XXI editores.

[24] Arreola A. (2015). *En Ciberespionaje: La puerta al mundo virtual de los estados e individuos, una revisión de los programas de espionaje digital de los Estados Unidos* (pp. 30, 31). México: Siglo XXI editores.

El espionaje informático se dirige en dos direcciones, así como las empresas y los gobiernos son los principales actores en efectuar ciberataques, también destacan como objetivo de los criminales. En este sentido Alejandro Suarez destaca que; “Se trata de un espionaje multinivel, que tiene lugar tanto en el plano horizontal como en el eje vertical. En el plano horizontal tenemos un espionaje de carácter industrial, que tiene lugar normalmente entre empresas competidoras. Sin embargo, encontramos otro tipo de espionaje, de carácter vertical, en el que los gobiernos intervienen directamente en las actividades empresariales, bien para favorecer a las compañías de sus países, bien para evitar que la industria nacional sea perjudicada por la intervención, honesta o no, de un segundo Estado o empresa, bien para garantizar la seguridad económica de la nación.”[25]

Finalmente, se entenderá como ciberespionaje la acción de obtener información de manera clandestina mediante la tecnología. Además, es una práctica empleada por empresas y gobiernos, además de utilizarlo con el fin de obtener información de otros gobiernos también lo emplea para obtener información de empresas y favorecer la industria nacional e impulsar su economía.

1.5.2. 1.5.2. EL PAPEL DEL E-COMMERCE EN EL MUNDO ACTUAL.

Como se observó las empresas desempeñan un papel importante en el ámbito digital, el cual utilizan para obtener información y favorecerse ante otras empresas, también para globalizar sus productos, dando origen el E- commerce.

El concepto e-commerce ha evolucionado con el tiempo y hoy en día hace referencia a una actividad distinta a la que hacía referencia cuando surgió. “Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos, como por ejemplo el intercambio electrónico de datos. Sin embargo, con el advenimiento de la Internet a mediados de los años 90, comenzó el concepto de venta de servicios por la red, usando como forma de pago medios electrónicos como las tarjetas de crédito. Por otra parte, personas han visto en esta nueva manera de hacer negocios una gran oportunidad para emprender y tener una actividad comercial propia en la que triunfan cuando entienden que en el e-commerce no existen barreras ni fronteras, y que el espacio geográfico no es el que determina el target; que se deben tener presentes muchos aspectos y ver la otra cara de la moneda; que

[25] Suárez A. (2015). Espionaje económico e industrial. En El Quinto Elemento (p. 42). España: Deusto S.A. ediciones.

sin creatividad y sin ofrecer una propuesta de valor realmente diferenciadora se hace complicado surgir en este amplio mundo como unos grandes vencedores."[26]

El comercio electrónico es una forma de optimizar y globalizar el comercio a través de herramientas tecnológicas, pero, como menciona la Organización para la Cooperación y el Desarrollo Económico este también genera riesgos para quienes lo utilizan. "El comercio electrónico es definido por los estudios de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) como el proceso de compra, venta o intercambio de bienes, servicios e información a través de las redes de comunicación. Representa una gran variedad de posibilidades para adquirir bienes o servicios ofrecidos por proveedores en diversas partes del mundo. Las compras de artículos y servicios por internet o en línea pueden resultar atractivas por la facilidad para realizarlas, sin embargo, es importante que los ciberconsumidores tomen precauciones para evitar ser víctimas de prácticas comerciales fraudulentas."[27]

Existen términos similares al E-commerce, pero, este se diferencia porque mantiene la esencia del concepto original, es decir, es el cambio de un bien o producto por dinero a través de Internet. "El e-commerce es un término anglosajón que se refiere al comercio realizado electrónicamente, el comúnmente llamado comercio online. Aunque existen conceptos similares, como el e-business, debemos tener claro que el e-commerce o comercio electrónico se refiere a la propia transacción comercial como tal, esto es, al cambio de un bien, producto o servicio por dinero u otro bien similar."[28]

En resumen, el E-commerce es el método que las empresas desarrollaron para llevar sus productos a cualquier parte del mundo a través de Internet y hacer crecer sus ganancias.

[26] Rodríguez C. (agosto 12, 2015). *¿Qué es e-commerce o comercio electrónico?*. agosto 25, 2019, de Marketing Digital Sitio web: https://marketingdigital.bsm.upf.edu/e-commerce-comercio-electronico/

[27] PROFECO. (2016). *El comercio electrónico*. julio 30, 2018, de PROFECO Sitio web: https://www.profeco.gob.mx/internacionales/com_elec.asp.

[28] Sistemas. Definición de e-commerce. marzo 11, 2019, de Sistemas Sitio web: https://sistemas.com/e-commerce.php.

1.6. CIBERSEGURIDAD; MITIGACIÓN Y PREVENCIÓN A LAS AMENAZAS DEL SIGLO XXI.

Como se observó los fenómenos originados en el ciberespacio representan un peligro para la sociedad por ello se requieren medidas para mitigar y prevenir sus efectos, surgiendo así el término; ciberseguridad, que mantiene la esencia del término de origen, es decir; seguridad.

La seguridad se define como; "Seguridad es un conjunto de sistemas, medios organizativos, medios humanos y acciones dispuestas para eliminar, reducir o controlar los riesgos y amenazas que puedan afectar a una persona a una entidad a una instalación o a un objeto. La seguridad proporciona las condiciones para afrontar el peligro, en síntesis, seguridad es la minimización del riesgo."[29]

Dado lo anterior ciberseguridad; se refiere a la estrategia que se emplea para proteger la información depositada en el ciberespacio, en complemento; "La **Ciberseguridad** es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante."[30]

Por su parte el autor Alberto Olmos define la seguridad digital como; "Aunque resulta difícil dar una breve definición de ciberseguridad, podríamos decir que se trata del conjunto de políticas, herramientas, tecnologías, salvaguardas, formación, buenas prácticas, etc. dirigidas a proteger los activos de las organizaciones, los países y los usuarios del ciberentorno."[31] Cabe agregar que estas medidas no solo son diseñadas por gobiernos, las empresas también se encargan de desarrollar programas de ciberseguridad, en los cuales encuentran un potencial negocio.

En síntesis, la ciberseguridad son aquellas medidas implementadas para evitar el robo de información y daños a otros sistemas que pudiesen tener repercusiones severas para la sociedad y en general para los países. Además, la ciberseguridad debe basarse en un método de prevención más que de contraataque el cual no siempre es posible debido a las características del ciberespacio.

---

[29] Ballesteros A. *Seguridad de Instalaciones*. marzo 8, 2019, de Escuela Penitenciaria Nacional Sitio web: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/index.html.

[30] INDEADIVERSITY. (diciembre 13, 2016). *Introducción a la Ciberseguridad: ¿Qué es y porque es importante?*. octubre 3, 2017, de INDEADIVERSITY Sitio web: http://indeadiversity.com/tag/ciberataques/

[31] Olmos A, Seco F. Sistemas de gestión para minimizar ciberamenazas. (p.12) Marzo 13, 2018 AENOR, Sitio web: http://www.aenor.es/revista/pdf/ene15/12ene15.pdf.

2. ¿QUÉ MARCÓ EL INICIO DEL CIBERTERRORISMO?

En este segundo apartado se expondrán algunos acontecimientos que marcaron el inicio del ciberterrorismo y su desarrollo.

El 11 de septiembre de 2001, a quien también se referirá como el 11S, es uno de los acontecimientos, que pese a no ser catalogado como un acto ciberterrorista, muestra la importancia del ámbito digital para el funcionamiento de la sociedad, como el sistema de emergencias y la red eléctrica. Además, en 2001 comienza a incrementar la dependencia tecnológica dentro de la sociedad, la cual no será únicamente de la sociedad hacia el ámbito digital, sino también de un sistema a otro, interdependencia que en casos de crisis provocaría un efecto domino, es decir, si un sistema se ve afectado en consecuencia otro u otros también lo serán.

El acontecimiento de Estonia en 2007 es ejemplo del nivel de interconectividad que algunas sociedades han alcanzado, entre sus infraestructuras y la tecnología, donde una falla en ellas podría paralizar al país entero. Con el 11S, además, de mostrar la importancia del factor tecnológico para el funcionamiento del país también se mostró el peligro de la dependencia tecnológica en la sociedad.

También se planteará el caso de la Operación Buckshot Yankee donde se observarán los principales sectores que los criminales buscan afectar, entre los cuales desatacan las denominadas infraestructuras críticas consideradas el sistema nervios de un país.

2.1. EL 11 DE SEPTIEMBRE, UNA PERSPECTIVA CIBERTERRORISTA.

En este apartado se planteará el 11S, acontecimiento que marca la historia de los Estados Unidos. Dicho acontecimiento es fundamental para la dirección del país en Seguridad Nacional y expone las necesidades sus ante el terrorismo.

La Seguridad Nacional, se volvió una prioridad para el país después de los atentados de septiembre del 2001 y el gobierno comenzó una lucha contra el terrorismo. “En muchos sentidos, la guerra de EE.UU. contra el terrorismo, inicia poco después de los ataques del 11 de septiembre de 2001 en América, está ayudando a acelerar la rápida adopción de cibertácticas por parte de las organizaciones terroristas.” [32]

[32] Verton D. (2004). AL QAEDA: En Busca de los Hackers de Bin Laden. En Black Ice: La amenaza invisible del ciberterrorismo (p. 106). Madrid: McGraw-Hill.

Posterior al 2001 surge la idea de una guerra digital, debido a la importancia que la tecnología comenzó a tomar en la sociedad. En complemento Michel Schmitt menciona; “Los trágicos ataques terroristas del 11 de septiembre de 2001 y sus secuelas son el tema dominante en las noticias en estos comienzos del nuevo siglo. En el futuro, quizá sea tan digno de destacar el desarrollo de “guerra de la información” como medio de debate.”[33]

Además, de los gobiernos y la sociedad los grupos criminales también han comprendido la importancia de la tecnología en la estructura de los Estados y también su importancia como medio para obtener sus objetivos y causar daños. En complemento Álvaro Ortigosa menciona que; “Y es precisamente a raíz de los atentados del 11-S, cuando los diferentes entes gubernamentales, tanto de los Estados Unidos como de los países occidentales, se generalizó la percepción de la amenaza desde el ciberespacio; inicialmente orientada hacia la potencial actuación de organizaciones terroristas, de ahí que tomara fuerza el concepto de ciberterrorismo como una amenaza global.”[34]

La culminación del atentado de las Torres Gemelas es el resultado de la falta de atención al terrorismo y sus efectos, por parte de las autoridades, ya que, fue hasta dicho acontecimiento que los gobiernos comenzaron a elaborar una estrategia, aun cuando existían advertencias previas, desde entonces se contemplaba el tema de ciberseguridad;

1. El establecimiento y reordenación de las Responsabilidades relativas a la Seguridad Nacional, con la creación del Ministerio de Seguridad del Territorio Nacional (“Department of Homeland Security, DHS”), entre las cuales se encuentran también las relacionadas con la Ciberdefensa. El desarrollo de legislación relativa a la Seguridad Nacional y a la Ciberdefensa, entre la que destaca:

- Aquella relacionada con la Protección de Infraestructuras Críticas: La Ley sobre Información de Infraestructuras Críticas (“Critical Infrastructure Information (CII) Act of 2002”), en la que se especifica qué tipo de información es clasificada como Información de Infraestructuras Críticas.

[33] Schmitt M. (junio 30, 2002). La guerra de la información: Los ataques por vía informática y el just in bello. Octubre 31, 2017. de Comité Internacional de la Cruz Roja Sitio web: https://www.icrc.org/data/rx/es/resources/documents/misc/5tecg3.htm.

[34] Ortigosa A, Hernández L. (2016). *Las nuevas amenazas cibernéticas del S.XXI, ciberterrorismo: Nueva forma de subversión y desestabilización*. octubre 10, 2018, de Cuaderno de la Guardia Civil Sitio web: https://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/18272.pdf.

- La Directiva de Identificación, Priorización y Protección de Infraestructuras Críticas (“Critical Infrastructure Identification, Priorization, and Protection”, HSPD-7), de diciembre de 2003. ¸
- La Regla Final del Programa de Protección de Información de Infraestructuras Críticas (“PCII Program Final Rule”), de septiembre de 2006, para el desarrollo de procedimientos de protección de la información de infraestructuras críticas. o La Directiva sobre la Iniciativa de Ciberseguridad Nacional. (“National Cyber Security Initiative”, HSPD-23), de enero de 2008.

2. El desarrollo de Planes y Estrategias relativas a la Seguridad Nacional como son: o La Estrategia para la Seguridad del Territorio Nacional (“National Strategy for Homeland Security”) o La Estrategia Nacional para la Seguridad del Ciberespacio (“National Strategy to Secure Cyberspace”), que forma parte de la estrategia anterior. o La ejecución de Ejercicios periódicos de Ciberseguridad (Cyber Storm I y Cyber Storm II) o La ejecución de Seminarios periódicos sobre Concienciación en la Ciberseguridad o El Plan Nacional de Protección de Infraestructuras (“National Infrastructure Protection Plan”, NIPP).[35]

La creación de instituciones también formo parte de las medidas tomadas a consecuencias de los atentados de septiembre del 2001, con la finalidad de tener instituciones para respaldar las leyes en materia de Seguridad Nacional. “El especialista Javier Candau menciona que: Tras los ataques de 2001 se impulsaron las estrategias de una defensa territorial más activa y coordinada que finaliza en la creación de un Departamento de Seguridad del Territorio Nacional (noviembre de 2002). Así mismo se desarrolla una amplia legislación relacionada con la ciberseguridad y la protección de infraestructuras críticas.”[36]

A raíz del atentado a las Torres Gemelas, se inició una vigilancia masiva de los usuarios de Internet con el fin de detectar actividad inusual o casos sospechosos que pusieran en peligro al país. En este sentido el autor Alejandro Suárez destaca que; “Nacionales o extranjeros, lo cierto es que, desde 2001, se ha producido un giro en las políticas de vigilancia sobre los ciudadanos. Por un lado, las amenazas contra la seguridad del mundo contemporáneo

[35] Pastor O, Pérez J, Arnáiz D, Taboso P. (octubre 2009). *Seguridad Nacional y Ciberdefensa*. (p. 52) noviembre 3, 2017, de ISDEFE Sitio web: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

[36] Candau J. (febrero 2011). *Estrategias Nacionales de Ciberseguridad. Ciberterrorismo*. En Ciberseguridad. Retos y Amenazas a la Seguridad Nacional (p. 275). España: Ministerio de Defensa.

provienen de grupos e individuos más que de Estados, lo cual obliga a que el objetivo de la vigilancia sea más el público que los gobiernos."[37]

Cabe mencionar que, con la Era de la Información la cual culmino con la fundación del Internet global, se dio un crecimiento del número de individuos con acceso a Internet y medios digitales, mismos individuos que representaban una posible amenaza para otros usuarios, empresas e incluso para los gobiernos.

La ciberseguridad toma importancia al aumentar las vulnerabilidades en diversos ámbitos, consecuencia del grado de dependencia tecnológica alcanzado por la sociedad actual. "En los últimos 20 años la informática ha evolucionado mucho, pasando de ser una herramienta administrativa para optimizar procesos de oficina a un instrumento estratégico para la industria, la administración y las fuerzas armadas. Antes del 11-S los riesgos y retos de seguridad cibernéticos sólo se trataban dentro de pequeños grupos de expertos, pero a partir de esa fecha resultó evidente que el ciberespacio introduce graves vulnerabilidades en unas sociedades cada vez más interdependientes."[38]

El peligro que el ciberespacio representa, se observó desde antes de los atentados del 11 de septiembre, donde al igual que con el terrorismo el minimizar sus efectos obtuvo como resultado acontecimientos como el de Estonia en 2007, donde se visualizó la amenaza del ámbito digital. "Un año antes del 11-S la OTAN hizo un importante llamamiento para la mejora de sus <<capacidades para defendernos de los ciberataques>> dentro del Compromiso de Capacidades de Praga, aprobado en noviembre de 2002. Sin embargo, en los años siguientes la organización se concentró sobre todo en la implementación de las medidas de protección pasiva solicitadas por los militares … Hizo falta el 11-S para cambiar esa percepción. Y hubo que esperar incluso a los incidentes del verano de 2007 en Estonia para que se prestara una atención política plena a esta creciente fuente de amenazas contra la seguridad pública y la estabilidad estatal. Tras tres semanas de ciberataques masivos quedó claro que las sociedades de los países de la OTAN adolecían de una elevada vulnerabilidad digital."[39]

---

[37] Suárez A. (2015). Espionaje económico e industrial. En El Quinto Elemento (p. 82). España: ED. Deusto S.A.

[38] Theiler O. Nuevas amenazas: El ciberespacio. junio 7,2017, de OTAN Sitio web: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm.

[39] Theiler O. *Nuevas amenazas: El ciberespacio*. junio 7,2017, de OTAN Sitio web: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm.

El atentado a las Torres Gemelas, también expuso la dependencia entre las infraestructuras donde una situación de crisis puede tener consecuencias en serie, es decir, un efecto domino como menciona Dan Verton, “Los ataques terroristas del 11 de septiembre demostraron claramente la interdependencia que existe entre las infraestructuras físicas y cibernéticas y cómo la destrucción o la degradación de una de ellas puede tener consecuencias catastróficas sobre la otra.”[40]

Dan Verton en su obra “Black Ice” narra como la interdependencia entre las infraestructuras provocan escenarios catastróficos, como ocurrió en 2001. “La parte baja de Manhattan no sólo era el lugar donde había tenido lugar el peor ataque terrorista de la historia de la Humanidad, sino también era el lugar donde se encontraba una de las instalaciones más importantes de EE.UU. Y eso le convirtió en el lugar del peor ataque ciberterrorista de la historia. Sin embargo, el 11 de septiembre los más de 1.700 ocupantes del edificio lo conocían como la principal de comunicación de Verizon Communications y el latido digital de la economía de la nación en Wall Street. Las computadoras y el equipamiento de conmutación del edificio eran los responsables de administrar miles de millones de llamadas telefónicas cada día. Y eso en un día normal. Con la desintegración de las dos torres del World Trade Center y el derrumbe del edificio 7 posteriormente por la tarde, ese latido digital comenzó a convertirse en una línea plana.”[41]

En 2001 se expuso la importancia de las Infraestructuras Críticas y los escenarios que se pueden provocar un ataque físico que afecte a estas, efectos que en la actualidad pueden lograrse a través de ciberataques. “Los ataques del 11 de septiembre de 2001 demostraron que los ataques físicos masivos que inutilicen las infraestructuras críticas de energía y telecomunicaciones pueden detener en seco la actividad financiera de la nación.”[42]

Las pruebas forenses, realizadas en aeropuertos de Estados Unidos, detectaron elementos como, daños en la red inalámbrica durante el atentado de 2001, lo que suscito una perspectiva ciberterrorista de dicho acontecimiento, como describe Dan Verton; “Exactamente un año después de los ataques terroristas del 11 de septiembre de 2001, autoridades de seguridad de

[40] Verton D. (2004). *9/11: El ataque ciberterrorista*. En Black Ice: Una amenaza invisible del ciberterrorismo (p. 175). Madrid: Hill, Madrid.
[41] Verton D. (2004). *AL QAEDA: En busca de los hackers de Bin Laden*. En Black Ice: Una amenaza invisible del ciberterrorismo (p. 161). Madrid: Hill, Madrid.
[42] Verton D. (2004). *Terror en la Red: Internet como arma*. En Black Ice: Una amenaza invisible del ciberterrorismo (p. 53). Madrid: Hill, Madrid.

las redes inalámbricas utilizadas en aeropuertos de todo EE.UU. revelaron aún más problemas. Una inspección de seguridad realizada por AirDefense, Inc., con base en Alpharetta, Georgia de redes inalámbricas en funcionamiento en los aeropuertos más importantes de Atlanta, San Diego, San Francisco y en el O´hare de Chicago, descubrió que los sistemas de facturación de pasajeros y transferencia de equipajes estaban funcionando sin las protecciones de seguridad más básicas, como puede ser el cifrado."[43]

El interés del Buró Federal de Investigaciones (FBI) por mantener la seguridad en el ámbito informático, surge al entender la vulnerabilidad del país posterior a lo ocurrido en 2001, misma que los criminales aprovecharían para desestabilizarlo mediante otros medios como el ciberespacio. "En la quinta planta del Centro de Operaciones e Información Estratégica, en el cuartel general del FBI en Washigton, D.C., Ron Dick, el anterior director del Centro Nacional de Protección de Infraestructuras (NIPC) y con una experiencia de 24 años en el FBI, comenzó el proceso de creación de un Equipo de Acción de 24 horas ante una Cibercrisis (24-hour Cyber-Crisis Action Team, C-CAT) responsables no sólo de ayudar en el esfuerzo físico de recuperación de Breton Greene en Nueva York sino de controlar también la infraestructura de Internet en busca de señales de un ciberataque relacionado que pudiera tener como objetivo otros sectores de la economía. <<Había muchas incógnitas >>, recuerda Dick. Para el NIPC, el 11 de septiembre y los días posteriores serían un momento definitorio, más que ningún otro incidente relacionado con la seguridad en Internet."[44]

"Con los ataques del 11 de septiembre de 2001, Al Qaeda demostró al mundo que la estrategia del terrorismo había evolucionado hasta un nuevo nivel. El 11 de septiembre fue un ataque económico que tuvo el beneficio añadido para Al Qaeda de matar a miles de personas inocentes. Y la evidencia de este cambio en el interés estratégico puede encontrarse en las propias palabras de Bin Laden, pronunciadas solo unos meses después de 2001: <<Es importante golpear a la economía de Estados Unidos, que es la base de su poder militar>>dijo Bin Laden, <<Si la economía resulta dañada, entonces se preocuparan>>." [45] En el terrorismo, además, de los intereses también los medios para lograr sus objetivos han evolucionado con ayuda de la tecnología, dando origen al ciberterrorismo.

---

[43]Verton D. (2004). *Terror en el aire: La amenaza inalámbrica*. En Black Ice: Una amenaza invisible del ciberterrorismo (p. 74,75). Madrid: Hill, Madrid.

[44] Verton D. (2004). *9/11: El ataque ciberterrorista*. En Black Ice: Una amenaza invisible del ciberterrorismo (p. 106). Madrid: Hill, Madrid.

[45] Verton D. (2004). *9/11: El ataque ciberterrorista*. En Black Ice: Una amenaza invisible del ciberterrorismo (p. 92). Madrid: Hill, Madrid.

Posterior al acontecimiento de las Torres Gemelas, gobiernos y empresas prestaron mayor atención al ciberespacio, esto reflejado en los programas de seguridad informática que iniciaron a desarrollarse, de donde surgen negociosos potenciales como el espionaje y la ciberseguridad. “Otro negocio complementario al de las empresas que ofrecen servicios de espionaje es el de las compañías que desarrollan y venden software espía a gobiernos y a otras empresas. Este mercado, como el anterior, vive una época floreciente desde los atentados del 11 de septiembre de 2001, y mueve cada año miles de millones de dólares.”[46]

El 11S no se considera un ataque ciberterrorista, sin embargo, el elemento tecnológico se hizo presente y mostró el papel de tecnología en la sociedad y el funcionamiento de esta, con lo que se vislumbró que el ciberterrorismo sería una realidad como Alejandro Suárez menciona; “La potencialidad de un «ciber 11-S» o un «ciber Pearl Harbor» es absolutamente real. De hecho, ya en 2001, fueron descubiertos en Afganistán unos ordenadores pertenecientes a Al Qaeda en los que aparecieron modelos de presas y software de ingeniería que simulaba un fallo catastrófico en los controles.”[47]

En resumen, el 11 de septiembre resaltó la importancia del ámbito digital, tanto para el funcionamiento de la sociedad, donde una falla en cualquier sistema de las Infraestructuras Criticas puede paralizar al país entero. Aunque dicho acontecimiento no fue un ataque ciberterrorista, se observó la necesidad de vigilar el ciberespacio porque los siguientes atentados serían a través de este.

2.2. ESTONIA; EL PRECIO DE LA INTERCONECTIVIDAD.

El caso de Estonia es ejemplo de lo que puede ocasionar el ciberterrorismo y la dependencia tecnológica. Aquello que parecía ficticio se convirtió en realidad, las próximas batallas tendrán lugar en el ciberespacio. “Desde el primer momento en que empecé a trabajar con el concepto de la Nueva Guerra Fría, resultó evidente cómo chocaban la memoria histórica de unos pueblos y otros respecto a aquella experiencia. Uno de los primeros incidentes que anticiparon esta nueva era fue la crisis entre Rusia y Estonia en abril-mayo de 2007.”[48]

[46] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (p. 73). España: Deusto S.A. Ediciones.

[47] Suárez A. (2015). *Ciberterrorismo*. En El Quinto Elemento (p. 73). España: Deusto S.A. Ediciones.

[48] Guerras Posmodernas. (abril 28, 2017). Rumbo a Letonia. Y España entro en la nueva guerra fría. septiembre 20, 2017, de Guerra Posmodernas Sitio web: https://guerrasposmodernas.com/2017/04/28/rumbo-a-letonia-y-espana-entro-en-la-nueva-guerra-fria/.

Lo acontecido en Estonia se considera un acto ciberterrorista debido a los objetivos del ataque porque, aunque no se puso en peligro estructuras sensibles, se atacó instituciones con información confidencial. “Abril de 2007: El estado del mar Báltico de Estonia sufre un ciberataque continuado perpetrado por un amplio conjunto de botnets (redes de robots informáticos que se ejecutan de manera autónoma y automática) procedentes de todo el mundo. La mayoría fueron ataques de denegación de servicio que inundan un servidor con tal aluvión de peticiones en línea que el servidor se ve incapaz de aceptar nuevas conexiones y en esencia queda inhabilitado. Los principales objetivos fueron las páginas web del presidente de Estonia, del Parlamento, de los ministerios gubernamentales y de las organizaciones de noticias. Sin embargo, varios bancos también sufrieron ataques y uno informó de haber sufrido a consecuencia pérdidas que ascendían al millón de dólares (unos 900.000 euros). El país finalmente se aisló del internet exterior para poner fin a los ataques.”[49]

El ataque fue relacionado con Rusia debido a la crisis cultural originada posterior a la decisión de Estonia de trasladar a su territorio “el soldado de bronces” (estatua simbólica de la segunda guerra mundial para ambos países). “En la primavera de 2007 el gobierno de la República de Estonia anuncia su decisión de realizar excavaciones en la plaza de Tonismäe, con motivo de encontrar restos de soldados caídos durante la segunda guerra mundial enterrados en el subsuelo y posteriormente identificarlos y enterrarlos en el cementerio militar de Tallin. La decisión del gobierno incluía el traslado y emplazamiento, de forma permanente, de la estatua conocida como «el soldado de bronce» a la entrada del mencionado cementerio militar.”[50]

El anuncio de trasladar “El Soldado de Bronce” provocó en Rusia sentimientos nacionalistas, reflejados en movilizaciones de la población y en una serie de ataques informáticos contra el gobierno estonio. “En la mañana del 26 de abril de 2007, numerosas personas se congregaron de manera pacífica en la plaza del soldado de bronce para protestar por la decisión del gobierno de trasladar el monumento, pero por la tarde se unió un grupo con una actitud violenta, el cual se enfrentó a la policía y horas más tarde comenzaron actos vandálicos por la ciudad, rompiendo escaparates. El 27 de abril de 2007 mientras proseguían los enfrentamientos callejeros entre la policía y grupos violentos de la comunidad rusa, varios

[49] The Physics Arxiv Blog. (septiembre 13, 2015). *Los 20 ciberataques más perversos del S.XXI*. junio 10,2017, de MIT Technology Review Sitio web: https://www.technologyreview.es/s/7413/los-20-ciberataques-mas-perversos-del-siglo-xxi.
[50] Ganuza N. (febrero 2011). *Situación de la ciberseguridad en el ámbito internacional y en la OTAN; El ciber caso de Estonia 2007*. En Ciberseguridad. Retos y Amenazas a la Seguridad Nacional (p. 174). España: Ministerio de Defensa.

hechos significativos surgieron simultáneamente: a) comenzaron los ciber ataques a sistemas de información de la infraestructura pública y privada estonia."[51]

Como se mencionó, la economía es un elemento clave para la estabilidad nacional debido a que actualmente los sistemas de bolsas de valores y bancarios dependen de herramientas tecnológicas, por ello en dicho acontecimiento los bancos destacaron como blancos. "9 de mayo: «Día de la Victoria»; es la fiesta rusa que conmemora la victoria de la Unión Soviética de la Alemania nazi y rinde honores a los soldados del Ejército Rojo muertos en dichos combates. Cerca de la medianoche ocurrió el mayor ataque, logrando desconectar todo el sistema bancario y bloquear las páginas web; los cajeros electrónicos dejaron de funcionar y el tráfico en la Red se incrementó más de 1.000 veces del normal … Los ataques surgieron de todo el mundo, pero los funcionarios de Estonia expertos en seguridad informática señalan que, especialmente durante la fase inicial, se identificó a algunos atacantes por sus direcciones de Internet, muchos de los cuales eran rusos, y algunos miembros de instituciones estatales rusas."[52]

Estonia refleja como la interconectividad es contraproducente de no contarse con programas de ciberseguridad adecuados, ya que un ciberataque puede dejar inhabilitado al país para tomar acciones y evitar que el ataque se siga expandiendo, por ello gobierno solicitó apoyo al extranjero para detener el ataque. "Durante este tiempo, se han atacado bancos, periódicos, redes académicas y páginas web de varias instituciones. Tan virulentos fueron los ataques que prácticamente colapsaron el país, teniendo que pedir ayuda a sus aliados. En total se han identificado 128 ataques DDOS sobre las webs de Estonia, de los cuales 115 fueron ICMP, 4 TCP SYNC y 9 overflows genéricos."[53]

El ciberterrorismo, se ha convertido en un tema de Seguridad Nacional por ello surge la necesidad en los gobiernos de desarrollar medidas en seguridad informática, además, muestra a estos sus debilidades tecnológicas. "Estonia es un país con una dependencia grande de las tecnologías de la información con lo que un ciber ataque puede ser una buena elección si se quiere causar mucho daño sin obtener a cambio ninguna baja, perjuicio o imputación legal. Estonia es un país de dimensiones reducidas y perteneciente a la OTAN, con lo que un ciber

[51] Ganuza N. (febrero 2011). *Situación de la ciberseguridad en el ámbito internacional y en la OTAN; El ciber caso de Estonia 2007*. En Ciberseguridad. Retos y Amenazas a la Seguridad Nacional (p. 175). España: Ministerio de Defensa.

[52] Flores H. (mayo 2012). *Los ámbitos no terrestres en la guerra futura: Ciberespacio*. En Los ámbitos no terrestres en la guerra futura: Espacio (p. 38). España: Ministerio de Defensa.

[53] Acero F. (mayo 30, 2007). *Consecuencias de los ciberataques a Estonia*. septiembre 28, 2017, de LIVEJOURNAL Sitio web: https://fernando-acero.livejournal.com/40250.html.

ataque masivo puede dar lugar a una situación de crisis de seguridad nacional y así de paso comprobar y estudiar la fortaleza y la capacidad cibernética de las alianzas internacionales."[54]

El terrorismo y los medios a través de los cuales hoy en día se puede provocar daños han evolucionado, al grado que se puede causar daños estructurales desde un monitor, por ello las necesidades en seguridad también han cambiado. "La OTAN considera que los ataques contras las redes informáticas de Estonia demuestran que el concepto de defensa ha cambiado profundamente y que en la actualidad es necesario considerar otras posibilidades y otros frentes, como el Ciberespacio."[55]

El anonimato, como se ha planteado es un elemento clave del ciberterrorismo que vuelve complejo dicho fenómeno, porque dificulta conocer a los responsables de un ataque, por ello para detectar la participación de gobiernos se consideran ciertos elementos. "Viik aseguró que ataques tan sofisticados y con objetivos tan complejos como los que afectaron a su país no pueden ejecutarlos simples internautas. "Se requirió de medios técnicos que rebasan la iniciativa personal y a las mismas organizaciones criminales", comentó. Esos ciberataques sólo pudieron efectuarse con la cooperación de un Estado y de varios operadores de telecomunicaciones.[56]

Con las pruebas forenses Estonia comprobó la participación del gobierno ruso en el ataque, tal como lo narra Néstor Ganuza; "El 10 de mayo de 2007, la oficina del fiscal general de Estonia, tramitó un escrito oficial a su homólogo de la Federación Rusa, en base al acuerdo de ayuda legal mutua entre los dos países firmado en 1993, en la que se exhortaba a identificar a las personas que habían tomada parte en los ataques. En el escrito se incluía información detallada de direcciones IP, sitios web y foros de internet localizados en territorio de la Federación Rusa que estaban involucrados en los ataques. Una de las direcciones IP implicadas pertenecía al gobierno de la Federación Rusa (59) y fuentes oficiales estonias declaraban que en la investigación forense habían identificado direcciones IP que pertenecían a la administración presidencial y agencias estatales rusas."[57]

---

[54] Ganuza N. (febrero 2011). *Situación de la ciberseguridad en el ámbito internacional y en la OTAN; El ciber caso de Estonia 2007*. En Ciberseguridad. Retos y Amenazas a la Seguridad Nacional (p. 186). España: Ministerio de Defensa.

[55] Acero F. (mayo 30, 2007). *Consecuencias de los ciberataques a Estonia*. septiembre 28, 2017, de LIVEJOURNAL Sitio web: https://fernando-acero.livejournal.com/40250.html.

[56] Appel M. (agosto 2, 2017). *La guerra silenciosa de Moscú*. septiembre 28, 2017, de Europafocus Sitio web: http://www.europafocus.com/2017/08/02/la-guerra-silenciosa-de-moscu/.

[57] Ganuza N. (febrero 2011). *Situación de la ciberseguridad en el ámbito internacional y en la OTAN; El ciber caso de Estonia 2007*. En Ciberseguridad. Retos y Amenazas a la Seguridad Nacional (p. 192). España: Ministerio de Defensa.

En 2009 culminaron las investigaciones y se dio a conocer dos de los responsables de dicho ataque. Uno de los involucrados se relacionó con el grupo Nashi. “Un joven de 20 años y de origen ruso, Dimitri Galoshkevich, fue detenido y multado con mil euros por haber participado en la ciberguerra contra Estonia. Fue en marzo de 2009 que otro informático ruso, Konstantin Goloskokov, líder del grupo hacker Nashi, se adjudicó tal ataque.”[58]

Nashi es un grupo de jóvenes hackers quienes no están asociados oficialmente con el gobierno ruso, sin embargo, son simpatizantes de Vladimir Putin y persiguen actividades antipatriotas. Con ello se confirma la influencia que, provocó la decisión de Estonia de trasladar el “Soldado de bronce”, sobre el ataque. “El líder parlamentario Sergei Markov le sugirió a los estonios que no miraran con dudas al Kremlin. «Sobre el ciberataque a Estonia, no busquéis más: el ataque fue llevado a cabo por mi ayudante», declaró. Efectivamente, el joven asistente de Markov no tuvo problema en reconocer su autoría. El muchacho era el líder de Nashi (que puede traducirse como «Lo Nuestro»), un movimiento ruso de 120.000 jóvenes entre diecisiete y veinticinco años que, aunque no pertenece oficialmente al Gobierno, fue organizado por los seguidores de Putin para perseguir las actividades antipatrióticas.”[59]

En este acontecimiento destaco la participación de la OTAN y su interés por el tema digital, para el que externo las necesidades de una política de ciberdefensa, proyecto materializado en enero de 2008. “La OTAN elaboró por primera vez en su historia una “Política sobre ciberdefensa” oficial, aprobada en enero de 2008 y que definía los tres pilares básicos de su política respecto al ciberespacio:

1.Subsidiariedad: la ayuda se proporciona únicamente ante una petición, y en caso de no haberla se aplica el principio de responsabilidad exclusiva de cada país soberano.
2.No duplicación: evitar duplicaciones innecesarias de estructuras o capacidades a nivel internacional, regional y nacional.
3.Seguridad: una cooperación basada en la confianza, teniendo en cuenta lo sensible que puede ser la información de los sistemas a la que se debe ofrecer acceso, y sus posibles vulnerabilidades.”[60]

Como parte de las medidas en ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN) se tiene lo siguiente; “El ‘frente’ informático estonio está coordinado desde 2008 por una agencia militar internacional denominado NATO CCDCOE (siglas en inglés de Coperative Cyber Defence Centre of Excellence o Comité de Dirección de Excelencia de

[58] Appel M. (agosto 2, 2017). *La guerra silenciosa de Moscú*. septiembre 28, 2017, de Europafocus Sitio web: http://www.europafocus.com/2017/08/02/la-guerra-silenciosa-de-moscu/.
[59] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p. 187). España: Deusto S.A. Ediciones.
[60]Theiler O. *Nuevas amenazas: El ciberespacio*. junio 7,2017, de OTAN Sitio web: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm.

Cooperación en Ciberdefensa de la OTAN), destinada a la investigación y al estudio de la guerra y la seguridad cibernética, cuyo cuartel general se encuentra en el interior de una base militar de Tallin … su cometido es prevenir, vigilar y, en caso necesario, responder a ataques de ciberterroristas."[61]

En conclusión, lo ocurrido en Estonia muestra el desarrollo de una era que ofrece beneficios a la sociedad, pero también brinda herramientas a los criminales para conseguir sus objetivos y ampliar sus efectos sin correr los mismos riesgos que en el terrorismo tradicional.

2.3. OPERACIÓN BUCKSHOT YANKEE: UN ACTO DECISIVO PARA LA CIBERSEGURIDAD

En este apartado se planteará la denominada Operación Buckshot Yankee que, aunque algunos autores la denominan como el inicio de la ciberguerra, cabe mencionar que anteriormente a dicha operación han existido otros acontecimientos que muestran la evolución del ámbito digital, sus vulnerabilidades, amenazas y efectos de este.

Con la evolución del fenómeno digital también se observó un cambio en los intereses de los criminales tal como ocurrió en el terrorismo. En ese sentido, los casos planteados en este apartado muestran dicho cambio. En complemento a lo anterior Yolanda Quintana destaca la importancia del sector militar; "La ciberguerra actual quedó oficialmente inaugurada tras la entrada en acción de Agent.btz, un espía que fue capaz de causar lo que se dio a conocer como "la peor violación de los equipos militares estadounidenses de la historia"."[62]

Los ataques que provocaron la Operación Buckshot Yankee se caracterizaron por infiltraciones en la rede del gobierno de Estados Unidos, a través de la cual fluye información confidencial. "Los analistas de la NSA ("los mejores guerreros cibernéticos del gobierno", según los describió el periódico norteamericano de referencia) habían descubierto a Agent.btz en la red SIPRNET (Secret Internet Protocol Router Network) que los departamentos de Defensa y de Estado utilizan para transmitir material clasificado, pero no información sensible."[63]

---

[61] XL SEMANAL. (s/a). *Los cibersoldados de la OTAN*. septiembre 28, 2017, de XL SEMANAL Sitio web: http://www.xlsemanal.com/actualidad/20141123/cibersoldados-otan-7850.html

[62] Quintana Y. (junio 25, 2016). *El espía que inauguró la ciberseguridad*. septiembre 29, 2017, de eldiario.es Sitio web: http://www.eldiario.es/internacional/espia-inauguro-ciberguerra_0_529847934.html.

[63] Quintana Y. (junio 25, 2016). *El espía que inauguró la ciberseguridad*. septiembre 29, 2017, de eldiario.es Sitio web: http://www.eldiario.es/internacional/espia-inauguro-ciberguerra_0_529847934.html.

Con los ataques a Estados Unidos se obtuvo información sensible como la que el autor William Lynn destaca; “La intrusión en el 2008 que culminó en la Operación Buckshot Yankee no fue la única penetración exitosa. Los adversarios han adquirido miles de archivos de las redes estadounidenses y de las redes de aliados de Estados Unidos y socios en la industria, inclusive copias de planos de armamentos, planes operacionales y datos de vigilancia.”[64]

Desde los ataques del 11S los especialistas destacaron la necesidad de proteger el ciberespacio, sin embargo, es hasta 2008 que se marca un momento decisivo en la historia de la ciberseguridad de Estados Unidos, como lo afirma William Lynn; “La operación del Pentágono para contrarrestar el ataque, conocida como Operación Buckshot Yankee, marcó un momento decisivo para la estrategia de ciberdefensa de Estados Unidos.”[65] Dicho momento decisivo se marca con la creación del Mando Cibernético de los Estados Unidos, tal como lo menciona Yolanda Quintana; “El 23 de junio de 2009 se produce la primera consecuencia de alcance del caso "Agente.btz": El secretario de Defensa, Robert Gates, ordena la creación de una nuevo “Mando Cibernético de los Estados Unidos”.”[66]

En síntesis, la Operación Buckshot Yankee fue necesaria para la creación de instituciones especializadas en materia de ciberseguridad en Estados Unidos y comenzar a actuar acorde a las necesidades del ciberespacio y las vulnerabilidades que en este se desarrollan.

[64] Lynn W. *Defendiendo un nuevo ámbito, la ciberestrategia del Pentágono*. abril 10, 2018, de air&space power journal Sitio web: http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/1524/Defendiendo%20un%20nuevo%20%C3%A1mbito.%20La%20ciberestrategia%20del%20Pent%C3%A1gono.pdf?sequence=1&isAllowed=y.

[65] Lynn W. *Defendiendo un nuevo ámbito, la ciberestrategia del Pentágono*. abril 10, 2018, de air&space power journal Sitio web: http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/1524/Defendiendo%20un%20nuevo%20%C3%A1mbito.%20La%20ciberestrategia%20del%20Pent%C3%A1gono.pdf?sequence=1&isAllowed=y.

[66] Quintana Y. (junio 25, 2016). *El espía que inauguró la ciberseguridad*. septiembre 29, 2017, de eldiario.es Sitio web: http://www.eldiario.es/internacional/espia-inauguro-ciberguerra_0_529847934.html.

3. EL IMPACTOS DEL CIBERTERRORISMO.

A continuación, se planteará el impacto del ciberterrorismo en países como Estados Unidos. Cabe resaltar que los efectos de un ciberataque varían según el nivel de dependencia tecnológica en el país. Asimismo, el impacto de este fenómeno puede ser negativo (generalmente para las víctimas de estos ataques) o positivo (para quienes implementan dichos métodos).

El ciberterrorismo es un método que optimiza el terrorismo al reducir costos de elementos que no son necesarios como en un ataque tradicional, como es la cantidad de personas que se requieren para un ataque. “Los grupos terroristas de nuestros días utilizan el ciberespacio como un medio de bajo coste y bajo riesgo para reunir información de inteligencia. Si bien es cierto que un grupo terrorista no dispone de la financiación necesaria para desarrollar y lanzar al espacio satélites espía que les permitan alcanzar objetivos con precisión milimétrica, también lo es que no lo necesitan. Pueden utilizar los satélites que desarrollan los gobiernos de los países y utilizarlos para sus fines.[67]

Esta forma de ataque también ha tenido impacto en reducir el riesgo para los criminales, debido a que no se exponen físicamente durante la agresión, por lo tanto, no se exponen a pérdidas humanas, como resalta Alejandro Suárez; “El gran cambio y la gran diferencia que aporta la era cibernética es que permite un espionaje masivo, sin apenas coste y, desde luego, sin riesgos.” [68]

Además, al no existir una exposición física se reduce el nivel de violencia que se experimenta en una situación de guerra tradicional, porque no implica heridos o muertes, sin embargo, esto no deja de ser una posibilidad, en particular cuando se afecta la red de algún sistema sensible, por ejemplo, la energía nuclear. “Expertos consideran que los ciberataques pueden reducir la violencia mundial existente al permitir a los Estados y a los individuos alcanzar sus objetivos políticos sin tener que recurrir a la violencia física … Este tipo de delitos, aunque muy costosos en términos económicos, cuentan con la ventaja de que no implican violencia física contra las personas. [69]

Asimismo, las características del ciberespacio como; el anonimato, provocan que estas prácticas vayan en aumento, al ser el principal elemento en reducir el riesgo para los criminales al ocultar su identidad. “La facilidad de delinquir desde la distancia y el anonimato, la ausencia

---

[67] Suárez A. (2015). *Ciberterrorismo*. El Quinto Elemento (p. 142). España: Deusto S.A. Ediciones.
[68] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (p. 33). España: Deusto S.A. Ediciones.
[69] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (pp. 198, 260). España: Deusto S.A. Ediciones.

de sensación de peligro o la dificultad de la atribución de los delitos que hace previsible un incremento de los ciberdelitos. Algunos expertos aseguran que resulta mucho más barato robar un proyecto industrial o empresarial que emprenderlo desde cero."[70]

El ciberespacio también impacta en el tiempo al que se desarrollan las ciberarmas, el cual es menor al que conlleva elaborar un arma convencional. "Las armas cibernéticas, en cambio, sólo necesitan recursos modestos (apenas se necesitan instalaciones físicas para producirlas y su manejo es completamente seguro); y «un equipo de menos de un centenar de personas muy cualificadas lograría crear una devastadora gama de armas en sólo dos o tres años. Varios centenares de personas podrían producir un arsenal de ciberarmas extremadamente destructivas en cuestión de meses» (todo ello con una inversión presupuestaria mucho más pequeña que la necesaria para proliferar armamento nuclear)."[71]

El impacto de un ciberataque puede ser mayor al de los ataques tradicionales porque en la red la mayoría de las ocasiones se desconoce cuándo se es atacado, dando oportunidad al malware de avanzar. En complemento Dan Verton menciona; "Se pueden utilizar muchos camiones bomba y no hacer gran daño a la infraestructura económica de EE.UU. porque es muy diversa. Pero si se ataca el ciberespacio, se tiene la oportunidad de dañar toda la red, toda la red de servicios financieros, por ejemplo. Mediante los ataques físicos, haría falta mucha gente y una gran red de apoyo y tendríamos una buena oportunidad de darnos cuenta de lo que ocurre, Pero con los ciberataques, ni si quiera se tiene que venir a EE.UU."[72]

En síntesis, los impactos del ciberterrorismo son diversos y algunos pueden ser considerados un cambio positivo en el ámbito de la guerra; como el tema de la violencia la cual se reduce al no existir un enfrentamiento físico, sin embargo, no elimina que sea un crimen que debe ser controlado. Además, para los criminales existe una disminución de riesgo al poder realizar este tipo de ataques a distancia sin exponer su identidad e integridad, características que han provocado el interés de gobiernos en estas prácticas.

[70] Olmos A, Seco F. Sistemas de gestión para minimizar ciberamenazas. (p.14). Marzo 13, 2018 AENOR, Sitio web: http://www.aenor.es/revista/pdf/ene15/12ene15.pdf.

[71] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p. 209). España: Deusto S.A. Ediciones.

[72] Verton D. (2004). *9/11: El ataque ciberterrorista*. En Black Ice: Una amenaza invisible del ciberterrorismo (p. 176). Madrid: McGraw-Hill.

3.1. EL IMPACTO DE LA CARRERA ARMAMENTISTA DIGITAL.

Una vez señalado el impacto del ciberterrorismo en general, es importante resaltar el impacto de las armas digitales en la sociedad, para ello se expondrán algunos de los casos sobresalientes en la historia del ciberterrorismo debido al peligro que representaron.

El impacto de las ciberarmas depende de sus funciones y fines y del sistema que afecten, es decir, el impacto puede ir desde la pérdida de información valiosa hasta la explosión de una planta nuclear. En complemento el autor Alfonso Julián menciona que; “En su forma más básica una bomba lógica es un procedimiento de borrado de la información, pero en sus formas más avanzadas pueden primero ordenar al hardware hacer algo que lo dañe, como ordenar a la red eléctrica un aumento de tensión que funda transformadores y equipos, o aumentar puntualmente la presión de una red de distribución de gas, como ya se ha visto, confundir el sistema de señales de la red de trenes de alta velocidad, u ordenar a las superficies de control de un avión que lo pongan en picado, y, a continuación, borrarse y eliminar toda prueba.”[73]

La gravedad del fenómeno digital radica en la disolución de la línea entre el mundo físico y el digital porque existen ataque ejecutados en la red que tienen consecuencias físicas, como lo describe Michael Gallagher; "Pueden ocasionar apagones, no sólo desconectando la electricidad sino dañando permanentemente los generadores, lo que llevaría meses reparar. Podrían hacer explotar tuberías de petróleo o gas. Podrían derribar aviones … En el epicentro del problema están los elementos que hacen de enlace entre el mundo físico y el digital. Actualmente estos controladores sistematizados hacen una gran cantidad de trabajos, desde abrir válvulas de tuberías a controlar las señales de tráfico.”[74]

En resumen, el impacto de la carrera armamentista está relacionado al nivel de interconectividad de la sociedad a la tecnología, además, de la interdependencia entre los sistemas que conforman la estructura del país, situación que podría provocar un efecto domino debido a que actualmente de un sistema depende el funcionamiento de otros, como ocurre con la red eléctrica de un país.

---

[73]Alfonso J. (septiembre 2015). *Hacking, hacktivismo, ciberactivismo.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema Nacional de Seguridad. (p.34) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.

[74] Gallagher M. (abril 30, 2012). *Ciberguerra: Las víctimas reales que puede dejar un conflicto virtual*. marzo 21, 2018, de BBC Sitio web: http://www.bbc.com/mundo/noticias/2012/04/120430_tecnologica_ciber_armas_aa

3.1.1. STUXNET, EL ROSTRO DE LA CIBERGUERRA. INVISIBLE, ANONIMO Y DEVASTADOR.

A continuación, se describirá Stuxnet la ciberarma que marcó el inicio de la carrera armamentística digital, cabe mencionar que antes de su aparición ya existían ataques informáticos. Sin embargo, Stuxnet mostró una evolución en la informática, dando la posibilidad de causar daños físicos a través medios digitales. “Stuxnet, que se dio a conocer en 2010, es el primer virus que se conoce cuyo objetivo es atacar infraestructura en el mundo real, como plantas eléctricas, indicó el reportero de asuntos tecnológicos de la BBC, Jonathan Fildes.”[75]

La peligrosidad de Stuxnet radica en los sistemas que afecta, los cuales son parte de infraestructuras críticas, de las cuales depende el funcionamiento de otros sistemas indispensables para la sociedad y la estabilidad nacional. “En el año 2010, los expertos en seguridad digital entraron en pánico con la aparición de una nueva modalidad de virus informático. Un tipo de gusano mucho más sofisticado y peligroso de lo que el mundo había conocido hasta la fecha. Lo bautizaron Stuxnet, y está considerado como la primera arma de guerra digital a gran escala. Casi podríamos denominarlo como un arma de destrucción masiva digital. Stuxnet es el rostro de la guerra del siglo XXI: invisible, anónimo y devastador.”[76]

Las Infraestructuras Criticas son importantes porque, controlan sistemas sensibles como, la energía nuclear, un ataque en ellas puede tener consecuencias mortales, por ello Stuxnet se consideró un arma de destrucción masiva. “El gusano Stuxnet que apareció en 2010 marcó un nuevo nivel cualitativo en las capacidades destructivas de la ciberguerra. En verano de ese año se extendió la noticia de que unos 45.000 sistemas de control de Siemens de todo el mundo estaban infectados por un troyano específico que podía manipular procesos técnicos esenciales para las centrales nucleares iraníes. Aunque la evaluación de los daños producidos sigue sin estar clara, quedaron demostrados los posibles riesgos de un software malicioso que afectase a sistemas informáticos críticos que controlan el suministro de energía o las redes de tráfico. Por primera vez había evidencias de ciberataques que podían provocar daños físicos y poner en peligro vidas humanas.” [77]

Desde 2001 se previó el peligro que el ciberespacio representa, consecuencia de la relación que comenzó a surgir entre la tecnología y la sociedad, finalmente demostrado con la aparición

---

[75] BBC MUNDO. (febrero 15, 2011). *Revelan radiografía de Stuxnet, "el arma de la ciberguerra"*. agosto 3, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2011/02/110215_1448_stuxnet_virus_iran_symantec_dc.shtml

[76] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p. 192). España: Deusto S.A. Ediciones.

[77] Theiler O. *Nuevas amenazas: El ciberespacio*. Junio 7,2017, de OTAN Sitio web: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm.

de Stuxnet. “En junio de 2010 se conoció la existencia del virus “Stuxnet”, una especie de “bomba anti búnker digital” contra el programa nuclear iraní. De este modo se han cumplido las predicciones de los expertos que desde 2001 avisaban que antes o después se usaría la dimensión digital para perpetrar atentados importantes con consecuencias mortíferas en el mundo real.”[78]

Algunos especialistas consideran que Stuxnet pudo ocasionar un escenario incluso como el ocurrido en Chernóbil, lo cual demuestra las capacidades del ámbito digital. Razón por lo que se le considera el inicio de la ciberguerra porque marca la diferencia entre ciberarmas y programas de cibercrimen. “Dicho ataque a las instalaciones nucleares de Irán demostró fehacientemente que las armas pueden venir en formato electrónico, creando grandes masacres como, por ejemplo, lo que ocurrió en Chernóbil. Stuxnet es considerado por Kaspersky Lab como el prototipo funcional de una “ciber-arma”, que dará el pistoletazo de salida a una nueva guerra armamentística en el mundo.”[79]

Las ciberarmas persiguen objetivos específicos, es decir, saben exactamente que atacar y se caracterizan por perseguir sistemas sensibles de los Estados, a diferencia del cibercrimen su objetivo es infectar masivamente y el robo de capital. “Los expertos coinciden en que durante décadas ha habido ataques a sistemas de cómputo, pero creen que Stuxnet es el primer virus destinado a destruir un blanco específico, tal y como ocurre en una guerra tradicional.”[80]

Además, se considera las ciberarmas son desarrolladas por gobiernos o grupos que reciben apoyo de estos, dicha afirmación se deriva de los recursos que conlleva elaborar un programa de este tipo y los objetivos que tienen, como menciona el autor Luis Joyanes; “Los expertos consideran que el Stuxnet es el primer virus capaz de penetrar en los sistemas automáticos de control de infraestructuras públicas como centrales eléctricas y nucleares, presas e industrias químicas. La complejidad del programa es tal que los especialistas en seguridad informática que lo han examinado están convencidos de que no puede ser obra de un mero pirata

[78]Theiler O. *Nuevas amenazas: El ciberespacio*. Junio 7,2017, de OTAN Sitio web: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm.

[79] Díez C, Perojo J, Penide J, Arias M. (mayo 19, 2011). *Ciber-terrorismo. Definición de políticas de seguridad para proteger infraestructuras críticas frente a ciber- ataques terroristas*. (p. 21). enero 16,2018, de Universidad Europea de Madrid Sitio web: http://mendillo.info/seguridad/tesis/Penide-Diez-Arias-Perojo.pdf.

[80]BBC MUNDO. (octubre 18, 2010). *La guerra cibernética "debe preocuparnos"*. agosto 7, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2010/10/101018_1451_guerra_cibernetica_stuxnet_virus_dc.shtml.

informático. La mayoría opina que hay un Estado detrás y que es el primer ejemplo de guerra cibernética."[81]

Kaperky Lab (compañía de seguridad informática) en su análisis del caso Stuxnet confirmo la participación de gobiernos, dadas sus particularidades. "Los expertos en seguridad de Kaspersky Lab, que han analizado el código del gusano, insisten en que el objetivo principal de Stuxnet no ha sido sólo el de espiar sistemas infectados, sino también el de llevar a cabo acciones de sabotaje. Todos estos hechos apuntan al hecho de que es muy probable que algún estado-nación, con acceso a grandes volúmenes de información de inteligencia, haya dado cobertura al desarrollo de Stuxnet."[82]

Stuxnet perseguía un número especifico de centrifugadoras, número que conforman la estructura de la planta nuclear de Natanz. "Langner sabía que el gusano perseguía un controlador industrial muy concreto, manufacturado por Siemens y configurado para ejecutar una serie de centrifugadoras nucleares, pero no unas centrifugadoras cualesquiera, sino una serie de un cierto número de centrifugadoras unidas (984 para ser exactos) y de un tamaño determinado. Casualmente, 984 era el número exacto de centrifugadoras que tenía la planta nuclear de Natanz, una central iraní en la que se sospechaba que podían estar siendo desarrolladas ilegalmente armas nucleares." [83]

Además, el programa se diseñó para atacar específicamente los sistemas SCADA, sistemas encargados de controlar equipos industriales como plantas nucleares, por lo que Irán no resultó ser el único afectado. "Tras el atentado en Irán, Stuxnet ya ha infectado a más de 100 mil sistemas computacionales alrededor del mundo. Al principio, el gusano parecía ser uno más del montón, creado con la finalidad de robar información. Sin embargo, los expertos pronto determinaron que contenía código diseñado específicamente para atacar los sistemas de Siemens Simatic WinCC SCADA. ¿Qué tienen de especial estos sistemas? Bueno, son los encargados de controlar el manejo de tuberías, plantas nucleares y otros equipos industriales."[84]

La central nuclear de Bushehr es otro sistema afectado por Stuxnet como lo describe el autor Héctor Flores; "El caso del virus stuxnet, que en septiembre del 2010 infectó alguno de los

[81] Joyanes L. (febrero 2011). *Introducción. Estado del arte de la ciberseguridad*. En Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio (pp. 16-17). España: Ministerio de Defensa.
[82] Díaz J. (febrero 2011). *La ciberseguridad en el ámbito militar*. En Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio (p. 234). España: Ministerio de Defensa.
[83] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p. 197). España: Deusto S.A. Ediciones.
[84] Ecured. *Stuxnet*. octubre 27, 2017, de Ecured Sitio web: https://www.ecured.cu/Stuxnet.

sistemas de control de la central nuclear iraní de Bushehr, especialmente el Sistema de Control de las centrifugadoras (de aluminio), provocando que comenzaron a girar un 40% más rápido durante un breve período de tiempo (aproximadamente 15 minutos) y causando grietas en ellas."[85] Con el caso de Brushehr y Natanz se observa que las armas digitales además, de objetivos específicos también cumplen una función específica, en este caso la de detener la actividad normal de las plantas nucleares, lo que tendría como consecuencia una explosión de estas.

Existen diversas teorías sobre como Stuxnet logro acceder a la información y sistemas sensibles, una de ellas plantea el uso de otros malwares que ayudaron a descifrar las claves necesarias para poder acceder al sistema de las plantas nucleares. "Cómo los atacantes obtuvieron la clave privada de dichas compañías para la firma de los drivers es otro de los enigmas. Por un lado, hay quien cree que fue un robo físico debido a la proximidad de ambas compañías. Por otro, también hay quien cree que el robo se produjo utilizando otro tipo de malware, como, por ejemplo, Zeus que tiene la característica de robo de claves privadas."[86]

Otra teoría apuntó al uso de las propias fallas del sistema que controlaban Nataz, sin embargo, para ello el malware debió descifrar cuatro fallas, también conocidas como "días cero". "Stuxnet aprovechó cuatro errores de software desconocidos o "días cero", para romper a través de la seguridad una variedad de sistemas informáticos. Los analistas creen que cientos de centrifugadoras fueron dañadas, aunque nadie fuera de la operación lo sabe con seguridad."[87] Teoría en la cual Kaspersky complemento y descartando el uso de otro malware.

Kaspersky en su investigación concluyo que Stuxnet si aprovecho los "días cero" para acceder al sistema que controlaba la planta, sin embargo, descarta el uso de otro malware y plantea la colaboración del fabricante del sistema con los responsables del ataque. Con lo anterior la teoría apunta hacia un ataque elaborado por un gobierno. Debido a que descifrar todos los códigos necesarios habría requerido demasiado tiempo, sin tener acceso al código fuente de Windows, y que habría resultado demasiado complejo para un outsider. Al darse cuenta de esto, Kaspersky llegó a afirmar: "«Estamos entrando en una zona muy peligrosa. El siguiente paso, si queremos seguir por este camino, es pensar que hubo una llamada de Washington a

[85]Flores H. (mayo 2012). *Los ámbitos no terrestres en la guerra futura: Ciberespacio*. En Los ámbitos no terrestres de la guerra futura: Espacio (p. 34). España: Ministerio de Defensa.

[86]Díez C, Perojo J, Penide J, Arias M. (mayo 19, 2011). *Ciber-terrorismo. Definición de políticas de seguridad para proteger infraestructuras críticas frente a ciber- ataques terroristas*. (p. 23). enero 16,2018, de Universidad Europea de Madrid Sitio web: http://mendillo.info/seguridad/tesis/Penide-Diez-Arias-Perojo.pdf.

[87] Benedicto M. (abril 23, 2013). *EEUU ante el reto de los ciberataques*. (p. 6) diciembre 26, 2017, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO37-2013_Ciberataques_BenedictoSolsona.pdf.

Seattle para ayudar con el código fuente». Efectivamente, se hace dificilillo pensar que un Gobierno que no fuera el estadounidense pudiera haber llamado a Bill Gates para que solucionara los detallitos de un acceso rápido al código fuente de Windows."[88]

La teoría de Kaspersky tiene sentido al plantearse la relación que mantiene el gobierno de Estados Unidos y las empresas nacionales ante temas de Seguridad Nacional, donde las empresas tienen la obligación de apoyar al gobierno en situaciones que atenten contra la estabilidad del país. En resumen, Stuxnet resalta la colaboración entre sector público y priado con el fin de alcanzar sus objetivos, donde existe un flujo de información estratégica sobre adversarios y tecnología. Situación que se ajusta a las necesidades de ciberseguridad.

Finalmente, este caso refleja dos escenarios el primero desde la perspectiva de un acto ciberterrorista hacia Irán donde se pudo haber provocado la muerte de cientos de personas. El otro se plantea desde la necesidad de Estados Unidos por defender su nación, donde se justifica por el peligro que representan los proyectos nucleares de Irán para Estados Unidos.

3.1.2. FLAME; EL CÓDIGO QUE RECONCEPTUALIZA LOS RETOS EN CIBERSEGURIDAD.

Posterior al descubrimiento de Stuxnet surgieron otros casos de ciberarmas con objetivos distintos. Estas nuevas armas informáticas son el reflejo de la carrera armamentista que surge en el ciberespacio y cada una de ellas es desarrollada para fines distintos. "En mayo de 2012 la empresa rusa Kaspersky informó de la aparición de un nuevo conjunto de herramientas de ataque conocido como Flame. Flame es un gusano de ciberespionaje altamente sofisticado que ha afectado a ordenadores de muchos países de Oriente Próximo y Europa del Este."[89]

Flame es un programa de ciberespionaje, que no altera el funcionamiento del sistema infectado, solo se encarga de captar información y enviarla a su base de control. "Flame es uno de los programas "más sofisticados y subversivos" realizados hasta el momento, diseñado según los expertos para replicar información de redes, incluso de alta seguridad, y controlar las funciones cotidianas de un ordenador enviando la información a sus creadores."[90]

---

[88] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p. 195). España: Deusto S.A. Ediciones.

[89] Caro M. (junio 13, 2012). *Flame una nueva amenaza del ciberespionaje*. (p.2). junio 29, 2018, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI34-2012_Flame_Ciberespionaje_MJCB.pdf.

[90] ElMUNDO.es. (junio 20, 2012). *EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán*. junio 29, 2018, de ELMUNDO.es Sitio web: http://www.elmundo.es/elmundo/2012/06/20/navegante/1340173299.html.

Entre las características de los programas maliciosos se encuentra que no siempre se fabrican desde cero, es decir, toman propiedades de otros como en el caso de Flame. “Flame comparte muchas características con otros códigos dañinos como Stuxnet y Duqu. Sin embargo, Flame es uno de los códigos más complejos detectados hasta ahora. Es grande y sofisticado. Hace replantearse las nociones de ciberguerra, ciberterrorismo y ciberespionaje.”[91]

Las distintivas de Flame se camuflajean con características del cibercrimen, sin embargo, al analizar el programa se observó que su blanco era específico, por ello se clasifico como ciberarma. “El propósito principal de Flame parece ser el ciberespionaje y el robo de información de los equipos infectados. Dicha información es enviada a una red de servidores C&C ubicados en diferentes partes del mundo. La variada naturaleza de la información robada, que puede incluir documentos, imágenes, grabaciones de audio y una intercepción del tráfico de red, lo convierte en uno de las más avanzadas y completas herramientas de ataque que se haya descubierto.”[92]

Uno de los elementos que permitió clasificar a Flame como ciberarma, es el reporte de Kaspersky. Además, el programa se distinguió por ser sumamente silencioso, pese a haberse encontrado en el año 2012, se cree operaba desde 2010. “Flame es el arma cibernética más grande descubierta hasta la fecha, y fue diseñado de una manera que hizo que sea casi imposible rastrearlo. Mientras que el malware convencional está diseñado para ser pequeño y oculto, el tamaño total de Flame le permitió permanecer sin descubrir. Flame infecta las computadoras mediante el uso de técnicas sofisticadas que anteriormente solo utilizaban un arma cibernética: Stuxnet. Aunque parece que Flame ha estado en funcionamiento desde marzo de 2010, ningún software de seguridad lo había descubierto.”[93]

Respecto a sus funciones, María José Caro detalla; “Una vez infectada una máquina, Flame inicia un conjunto de operaciones complejas: recopilar archivos de datos, cambiar la configuración de forma remota en los equipos, encender los micrófonos de los equipos para grabar conversaciones cercanas, así como interceptar el teclado, tomar capturas de pantalla y registrar los chats de mensajería instantánea y las comunicaciones telefónicas por VoIP.” [94]

---

[91]Caro M. (junio 13, 2012). *Flame una nueva amenaza del ciberespionaje*. (p.3). junio 29, 2018, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI34-2012_Flame_Ciberespionaje_MJCB.pdf.

[92]CIO. (mayo 28, 2012). *Flame, nueva arma para el ciberespionaje*. marzo 13, 2018, de CIO Sitio web: http://cio.com.mx/flame-nueva-arma-para-el-ciberespionaje/.

[93] KASPERSKYLAB. *FLAME*. junio 29,2018, de Kaspersky Lab Sitio web: https://www.kaspersky.com/flame.

[94]Caro M. (junio 13, 2012). *Flame una nueva amenaza del ciberespionaje*. (p.3). junio 29, 2018, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI34-2012_Flame_Ciberespionaje_MJCB.pdf.

Las intenciones de Flame no eran tener repercusiones en estructuras físicas, sin embargo, el peligro del programa radica en las victimas a las que se dirigió el ataque, es decir, funcionarios iraníes a quienes se mantenían vigilados y razón por la cual Flame se denominó como ciberarma. “El virus Flame, de cuya existencia advirtió hace semanas la compañía de seguridad Kaspersky, fue diseñado para rastrear de forma secreta redes informáticas de Irán y controlar los ordenadores de los funcionarios iraníes, enviando un flujo constante de información utilizada en la campaña de guerra cibernética en marcha, según los funcionarios consultados por el diario. Esta campaña, en la que han participado la Agencia de Seguridad Nacional (NSA) estadounidense, la CIA y representantes militares de Israel, ha incluido el uso de un 'software' similar al destructivo virus Stuxnet que causó fallos en las centrifugadoras de la planta secreta de enriquecimiento de uranio de Natanz (Irán) en 2010.”[95]

Finalmente, el impacto de Flame es incierto dado que su objetivo no era el causar daños físicos, sino monitorear la actividad de funcionarios iraníes, donde se desconoce el uso de la información recolectada. Además, por los objetivos del malware se determinó existieron fines políticos.

3.1.3. GAUSS: UNA AMENAZA AL SECTOR BANCARIO, ¿UN MALWARE MÁS O UNA OBRA DE LOS ESTADOS?

Gauss es otra arma informática dedicada al ciberespionaje, la cual comparte similitudes con programas como Flame. “El malware parece ser un arma de espionaje cibernético diseñada por un país con el objetivo de atacar y rastrear a personas específicas.”[96]

El objetivo de Gauss eran los bancos libaneses, al igual que Flame también se caracterizó por no causar daños físicos, como ya se mencionó causar daños físicos no es la prioridad del ciberterrorismo, la mayoría de las ocasiones se persigue únicamente información estratégica. “Un programa fabricado para el espionaje ha sido hallado en miles de ordenadores en Oriente Próximo, según detalla un informe de la firma rusa Kaspersky Lab, dedicada a la seguridad informática. El virus, llamado Gauss (en honor del físico y matemático alemán Johann Carl Friedrich Gauss), ha sido hallado en al menos 2.500 ordenadores, la mayoría de ellos —unos 1.660— en bancos libaneses. No se activa en cualquier sistema: solamente en los que está

[95] ElMUNDO.es. (junio 20, 2012). *EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán*. junio 29, 2018, de ELMUNDO.es Sitio web: http://www.elmundo.es/elmundo/2012/06/20/navegante/1340173299.html.

[96] CNN en español. (agosto 10, 2012). *"Gauss", el virus que se autodestruye después de robar tu información*. julio 3, 2018, de CNN Sitio web: https://cnnespanol.cnn.com/2012/08/10/gauss-el-virus-que-se-autodestruye-despues-de-robar-tu-informacion/.

programado para atacar. Una vez instalado, guarda todas las actividades online de cada usuario, roba sus contraseñas y es capaz de ejecutar órdenes sin que el usuario se percate."[97]

Los programas que atacan cuentas bancarias son comunes en cibercrimen y se caracterizan por robar dinero de manera masiva, sin embargo, el objetivo de Gauss era distinto, por ello se le clasificó como ciberarma. Su intención era monitorear la actividad bancaria de personas específicas. "El sofisticado malware, descubierto por los laboratorios de seguridad de la compañía Kaspersky, ha capturado información de cuentas bancarias en línea desde septiembre de 2011. No hay evidencia de que se usaran para robar dinero. En lugar de ser un espía interesado en el rastreo de fondos, el virus reúne la información bancaria desde el inicio de la sesión, la envía de regreso a un servidor y se autodestruye rápidamente."[98]

Dicho ataque no provoco una infección masiva, se detectaron más de 500 casos afectados de acuerdo a los reportes de Kaspersky, número que comparado con la cantidad de usuarios existentes hoy en día en Internet, es un grupo pequeño. "Kaspersky también encontró 483 casos de Gauss en Israel y 261 en territorios palestinos. Sólo 43 casos se encontraron en Estados Unidos, y un puñado fueron descubiertos en otras partes del mundo."[99]

En resumen, Gauss es la muestra de que la guerra digital va más allá de un enfrentamiento físico, misma que resalta el valor de la información puesto que los programas en ciberespionaje van en aumento.

3.2. LA INFORMACIÓN, EL PETRÓLEO DE LA ERA DIGITAL.

A lo largo de la investigación se observó, como la información es un elemento clave para el ciberterrorismo, por ello actualmente es el principal objetivo de los criminales. En este sentido James Adams menciona; "La información es la clave de la guerra moderna, en lo estratégico, operativo, táctico y técnico. Por el momento bastaba saber que un nuevo tipo de guerra, que

[97]Calderón V. (agosto 10, 2012). *Hallado un nuevo virus utilizado para espiar en Líbano*. julio 3, 2018, de El País Sitio web: https://elpais.com/internacional/2012/08/10/actualidad/1344599271_563202.html.

[98]CNN en español. (agosto 10, 2012). *"Gauss", el virus que se autodestruye después de robar tu información*. julio 3, 2018, de CNN Sitio web: https://cnnespanol.cnn.com/2012/08/10/gauss-el-virus-que-se-autodestruye-despues-de-robar-tu-informacion/.

[99]CNN en español. (agosto 10, 2012). *"Gauss", el virus que se autodestruye después de robar tu información*. julio 3, 2018, de CNN Sitio web: https://cnnespanol.cnn.com/2012/08/10/gauss-el-virus-que-se-autodestruye-despues-de-robar-tu-informacion/.

exigía un nuevo tipo de guerrero con nueva clase de armas (no sólo laptops), esperaba el momento de ser librada."[100]

Sin embargo, el valor de la información es algo que ha existido a lo largo de la historia de las relaciones interpersonales, dado que la información previa permite tener ventaja y poder sobre el otros, como menciona Adolfo Arreola; "A lo largo de los siglos, la información precisa, veraz y oportuna se ha considerado como un medio de poder, por ello, quienes buscan preservar u obtener predominancia sobre el resto del grupo, no escatima esfuerzos para recopilar la mayor cantidad de información sobre los gustos, intereses, fortalezas, debilidades, hábitos, vicios y todo aquello que permita un conocimiento anticipado y profundo de las contrapartes."[101]

Para las Relaciones Internacionales los datos previos es una necesidad al tomar decisiones, necesidad que se satisface a través de las agencias de inteligencia de los Estados como lo plantea Adolfo Arreola; "En las relaciones internacionales existe la necesidad de contar con información con valor agregado, la cual debe ser recopilada a través de medios disponibles que, en esencia, es una tarea que corresponde a los servicios de inteligencia de los estados, pero que también es realizada por las empresas y los individuos para doblegar al oponente en turno."[102]

Derivado de la importancia de la información y la necesidad por obtenerla de los gobiernos, las agencias de inteligencia se basan en prácticas de espionaje o ciberespionaje, prácticas justificadas como una medida de seguridad. Derivado de ello surge con la exigencia por protegerla, "Los estados han buscado siempre la manera de acceder a informaciones de carácter secreto, interviniendo las comunicaciones realizadas a través de mensajeros y, más modernamente, los sistemas basados en tecnologías de la información y las comunicaciones. Del mismo modo, y conscientes de esa actividad, y las ventajas que puede aportar conocer las intenciones, estrategias, y organización interna, los estados han tratado también de proteger esas comunicaciones, securizándolas ante una intrusión o encriptándolas de modo que sean ilegibles e inútiles en caso de que resulten interceptadas."[103]

---

[100] Adams J. (1999). *Un mito del desierto*. La próxima guerra mundial (p.79). Buenos Aires: Granica S.A.

[101] Arreola A. (2015). *Ciberespionaje: La puerta al mundo virtual de los Estados e individuos. Una revisión de los programas de espionaje digital de los Estados Unidos* (p.7). México: Siglo XXI editores.

[102] Arreola A. (2015). *Ciberespionaje: La puerta al mundo virtual de los Estados e individuos. Una revisión de los programas de espionaje digital de los Estados Unidos* (p.211). México: Siglo XXI editores.

[103] Alfonso J. (septiembre 2015). *Espionaje, Espionaje electrónico, Ciberespionaje.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema nacional de seguridad. (p.11) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.

Además, de los gobiernos los criminales también han entendido el valor de la información como herramienta y una forma de ejercer presión hacia los Estados. “Se ha indicado la importancia de la información para los estados o para una organización, no es menos para los atacantes en una primera fase el atacante investigará y documentará toda la información posible relevante sobre la víctima.”[104]

Asimismo, para el ciberterrorismo no solo es atractiva la información de otros gobiernos sino, también la información económica se considera estratégica, razón por la cual las empresas también se vuelven objetivo para criminales. “La cuestión de atacar objetivos económicos es particularmente delicada, pues la mayoría de las operaciones están apoyadas por ordenadores y, por ello, resultan muy atractivas como objetivos de la guerra de la información.”[105] Además, en el caso de países como el de Estados Unidos la economía representa uno de los pilares de la Seguridad Nacional.

Martha Aranda plantea algunas de las consecuencias que el robo de información tiene para las empresas; “El robo de información se mantiene, desde 2015, como el primer motivo de los ciberataques. Además, durante estos últimos 3 años, el coste por su recuperación ha seguido en aumento, y ha llegado a suponer el componente más caro con un 43% respecto al resto de consecuencias como la disrupción del negocio, pérdida de ganancias y daños en el equipo.”[106] Lo anterior, dado que mediante el robo de información se pierden planos, proyectos o secretos industriales, que se traduce en pérdidas económicas.

El derecho al acceso a la información se ha convertido en una vulnerabilidad para las empresas, quienes se ven comprometidas a depositar información sobre ellas en sus sitios web, el error de estas es depositar información detallada, la cual puede ser utilizada por criminales. “Las grandes firmas de telecomunicaciones y las compañías de comunicaciones locales publican una gran cantidad de información delicada en sitios web sobre redes nacionales críticas … Además de los mapas de redes, el autor encontró información detallada de las localizaciones de centros de datos de Internet actuales y planeados, situaciones de routers y nodos principales de redes de área metropolitana. También estaban disponibles virtuales por centros que mostraban las situaciones de sistemas específicos, mapas

[104] Alfonso J. (septiembre 2015). *Web.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema nacional de seguridad. (p.115) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.

[105] Jeison. (noviembre 1, 2012). *Ciberterrorismo*. octubre 31, 2017, de E-GOV Sitio web: http://www.egov.ufsc.br/portal/conteudo/ciberterrorismo.

[106] Aranda M. (octubre 24, 2017). *¿Cuánto cuesta un ciberataque a las empresas?*. enero 16, 2018, de ODS Sitio web: https://opendatasecurity.io/es/cuanto-cuesta-un-ciberataque-a-las-empresas/.

representando puntos de terminación en la costa Este de todos los cables de comunicaciones submarinos de larga distancia, y mapas a nivel de la calle de redes de fibra óptica.”[107]

Sin embargo, pese a que el depositar información detallada en sitios web tanto de empresas como gobiernos, estos deben adaptarse y encontrar un equilibro para saber que si publicar y que no, y evitar que se violen derechos humanos. “Pero mientras la Web parece una mina de oro para los terroristas, es importante no permitir que los gobiernos utilicen el terrorismo como un pretexto para ocultar información al público que tiene el derecho y la necesidad de conocer. Éste es un acto de equilibrio que verdaderamente tiene consecuencias de vida y muerte.”[108]

Puntos como los mencionados en este apartado permiten comprender la importancia de la información, primero para los propietarios de esta, para quienes extraviarla representa pérdidas en diversos sentidos, y finalmente se tiene el valor para los grupos criminales por los beneficios que obtienen a través de ella.

3.3. EL PRECIO PARA ESTADOS UNIDOS DE UN CIBERESPACIO INSEGURO.

En este apartado se plantearán las pérdidas que la falta de seguridad en el ciberespacio representa para los gobiernos y la sociedad, en ocasiones las cifras están por debajo de las cifras reales debido a la falta de denuncias por parte de las víctimas. “En el último reporte que manejan Scotland Yard, la Oficina Federal de Investigación y el Servicio Secreto de los Estados Unidos, se pudo conocer que solamente el 3% de los ataques son reportados a través de los estamentos que tienen que administrar justicia. De ese 3%, indicó que se reportaron pérdidas, entre 8 mil y 10 mil millones de dólares, tan solo en el pasado mes de diciembre.”[109]

La falta de denuncias de casos de ciberataques se debe a que los afectados, sobre todo en casos de cibercrimen, prefieren realizar los pagos que los delincuentes solicitan para devolverles su información, sin embargo, estos pagos no son garantía de recuperar sus datos, lo que representa también económica. Por otra parte, en casos como el de los gobiernos o empresas prefieren no declarar cuando son víctimas de un ciberataque para no mostrarse débiles ante el fenómeno digital.

---

[107] Verton D. (2004). *La red del terror: Lo que sabe Al Qaeda de EE.UU*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.133). Madrid: McGraw-Hill.

[108] Verton D. (2004). *La red del terror: Lo que sabe Al Qaeda de EE.UU*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.145). Madrid: McGraw-Hill.

[109] Díaz D. (marzo 2, 2012). *Ciberterrorismo: amenaza que genera enormes pérdidas*. abril 23,2018, de Panamá América Sitio web: http://www.panamaamerica.com.pa/content/ciberterrorismo-amenaza-que-genera-enormes-p%C3%A9rdidas.

Las pérdidas económicas por ciberataques se dividen en dos vertientes; la primera considera la pérdida provocada por la actividad realizada para detener el ataque, la segunda más que un gasto representa una inversión ya que va en el sentido de prevenir futuros ataques. "Los expertos de B2B Internacional han calculado los daños derivados de los ciberataques incluyendo sólo los incidentes ocurridos en los últimos 12 meses y evaluando la información de las pérdidas sufridas como resultado directo de los incidentes de seguridad. El dato incluye dos componentes principales:

1. Daños causados por el incidente en sí – es decir, pérdidas derivadas de la fuga de datos críticos, continuidad de negocio y los costes asociados con la participación de especialistas para solventar el incidente. Suponen la mayor parte de las pérdidas, alrededor de 431.000 euros.
2. Costos no planificados, originados para prevenir futuros ataques similares, incluyendo el personal de contratación/formación, el hardware, el software y otros cambios de infraestructura. Suponen unos 69.000 euros."[110]

El sector comercial es uno de los sectores donde anualmente se registran daños importantes, tanto económica como intelectualmente, es decir, proyectos, secretos industriales y propiedad intelectual, esto derivado del papel que tienen actualmente las empresas dentro de la estabilidad nacional. "El comité de Asuntos de Espionaje de la Cámara de Representantes de EEUU ha calculado que los robos en Internet de secretos comerciales y propiedades intelectuales, en su gran mayoría dirigidos por China, le han costado a EEUU más de 300.000 millones de dólares en 2012."[111]

China destaca como uno de los principales actores que roba información a empresas y gobiernos, ello por su interés de alcanzar un mayor crecimiento y desarrollo económico, que a través de esta acción pretende favorecer sus empresas nacionales y tener efectos en su economía.

Los distintos delitos informáticos causan diferentes pérdidas, por ejemplo, en el cibercrimen, además, de información puede llegar a existir una pérdida económica sobre todo cuando las victimas intentan recuperar sus datos. En este sentido el Centro de Quejas de Delitos en Internet (IC3) hace un estimado de las pérdidas por ciberataques en 2016, donde debe considerarse la falta de denuncias. "El Internet Crime Complaint Center (IC3), publicó hace poco su reporte 2016 reuniendo estadísticas de los casos ingresados el año pasado en Estados Unidos. Según el informe, las víctimas de ciberataques perdieron 1,3 mil millones de dólares y se registraron 800 reclamos por día. En 2016, el IC3 recibió 2.673 reclamos

[110] Seguridad Informática. (julio 3, 2013). *¿Cuánto cuesta a una empresa un incidente grave de seguridad?*. enero 4, 2018, de Seguridad Informática Sitio web: https://seguinfo.wordpress.com/category/estadisticas/.

[111] Benedicto M. (abril 23, 2013). *EEUU ante el reto de los ciberataques*. diciembre 26, 2017, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO37-2013_Ciberataques_BenedictoSolsona.pdf.

identificados como infecciones de ransomware, que causaron pérdidas por más de 2,4 millones."[112]

Como ya se planteó los daños económicos ocasionados por ciberataques son acorde al tipo de ataque, en el caso de un ataque ciberterrorista las mermas pueden superar los gastos que un desastre natural representa. "Los ciberataques pueden salir más caros que los desastres naturales. Así lo indica un informe publicado por la aseguradora londinense Lloyd's. La firma, que es especialista, asegura que las pérdidas económicas vinculadas a las amenazas cibernéticas en Estados Unidos pueden llegar a los 121.000 millones de dólares."[113]

Además, el impacto económico de un ciberataque también se relaciona al nivel de dependencia que se tenga con el sistema afectado y la sensibilidad de este, es decir, existe una diferencia entre atacar el sistema de control de agua que el sistema eléctrico o una planta nuclear, tal como menciona Dan Verton; "Los impactos económicos de estos fallos probablemente también serían consecuencia de la dependencia general del sector de la banca y las finanzas en EE.UU. de las redes de telecomunicaciones y de la energía para mantener el normal funcionamiento de las operaciones."[114]

En síntesis, las consecuencias de cualquier ataque informático pueden ser tanto económicas como intelectuales y cualquiera que sea el tipo resalta la necesidad de desarrollar medidas para garantizar un ciberespacio seguro.

3.4. EL CIBERTERRORISMO, UN ENEMIGO DE LAS GRANDES EMPRESAS.

Como se ya se mencionó las empresas son uno de los principales blancos del ciberterrorismo, al ser un elemento clave en la estabilidad de los países, por ello el sabotaje empresarial ha adquirido cierta importancia para empresas y gobiernos, quienes buscan favorecerse ante sus

[112] Pagnotta S. (junio 28, 2017). *Las víctimas de ciberataques perdieron 1,33 mil millones de dólares en 2016*. diciembre 26, 2017, de welivesecurity Sitio web: https://www.welivesecurity.com/la-es/2017/06/28/victimas-ciberataques-millones-dolares/.

[113] Valencia I. (octubre 17, 2017). *Los ciberataques pueden salir más caros que los huracanes*. septiembre 22, 2017, de CISECE Sitio web: https://seguridad.cicese.mx/alerta/167/Los-ciberataques-pueden-salir-m%C3%A1s-caros-que-los-huracanes.

[114] Verton D. (2004). *Terror en la red: Internet como arma*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.52). Madrid: McGraw-Hill.

rivales. “Los virus, que hoy en día son la forma más común de sabotaje empresarial, ocasionan todos los días perdidas.” [115]

La autora Martha Arana plantea algunos factores que ayudan a calcular el daño económico de un ciberataque. “Hacer una valoración aproximada del impacto económico que supone para una empresa recuperarse de un ciberataque no es fácil. Hay que tener en cuenta múltiples factores que varían dependiendo del país, tipo de ataque, tipo de empresa, número de empresas encuestadas y los respectivos países en los que operan, etc. Por esta razón, los distintos medios de comunicación o estudios dedicados a investigar acerca del tema proporcionan diferentes resultados, ya que cada uno de ellos se valdrá de sus propias fuentes y encuestados, lo que suele desembocar en datos variables.” [116]

El sistema eléctrico se considera una Infraestructura Crítica dada su importancia para la sociedad, por la cantidad de sistemas alternos que depende de el, para su funcionamiento. “Un estudio reciente patrocinado por Electric Power Reserch Institute y el Consortium for Electric Infraestructure to Support a Digital Society descubrió que los apagones de energía, por ejemplo, cuestan a millones de firmas industriales y a otras compañías que dependen del almacenamiento y la recuperación de datos para sus operaciones diarias aproximadamente 13,4 mil millones de dólares al año en pérdidas de productividad y mano de obra. Un ciberataque que propiciara un apagón generalizado tendría consecuencias incalculables, tanto en términos de desórdenes sociales (los saqueos comienzan, de media, dos horas después de que se produzca un gran apagón) como por sus costes económicos.”[117]

Dan Verton complementa respecto a las consecuencias de los apagones eléctricos; “Además, el coste de los apagones e interrupciones de energía es directamente proporcional a la duración del fallo. Por ejemplo, el coste medio por segundo de un apagón entre las industrias y las firmas llamadas <<de la economía digital>> es de aproximadamente 1.477 dólares y de 7.795 dólares para un apagón de una hora. Dadas estas cifras, los apagones de energía del orden de los descritos en los ejercicios Black Ice y Blue Cascade (apagones que duran un mes

[115] Salellas L. (s/f). *Seguridad informática - Ciberterrorismo*. octubre 23, 2017, de Ilustrados Sitio web: http://www.ilustrados.com/tema/9670/Delitos-Informaticos-Ciberterrorismo.html.

[116] Arana M. (octubre 24, 2017). *¿Cuánto cuesta un ciberataque a las empresas?*. enero 16, 2018, de ODS Sitio web: https://opendatasecurity.io/es/cuanto-cuesta-un-ciberataque-a-las-empresas/.

[117] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p.209). España: Deusto S.A. Ediciones.

o más) provocarían daños financieros de más de 5 millones de dólares por compañía al mes."[118]

Algunos análisis mencionan, que el impacto de los ciberataques también varea según la zona geográfica que afecte, dado que no todos los países han alcanzado el mismo grado de interconectividad. "Los daños varían dependiendo de la región geográfica en la que opera la empresa en cuestión. Por ejemplo, los daños mayores se asocian con incidentes sufridos en empresas que operan en América del Norte, con un promedio de 624.000 euros, seguido de América del Sur, con 620.000 euros. Europa Occidental registró una media más baja, pero aún considerable, de las pérdidas derivadas de ciberataques, llegando a 478.000 euros."[119]

La industria china y estadounidense, son de las más afectadas por ataques informáticos, debido a la guerra comercial que actualmente enfrentan ambos países, donde existe un interés de China por impulsar su economía y por su parte Estados Unidos busca proteger el poder que ha adquirido. "Las mayores pérdidas generadas por ciberataques entre pequeñas y medianas empresas se registraron en compañías de Asia-Pacífico (73.000 euros). En segundo lugar, fue en empresas de América del Norte, con unas pérdidas de 62.000 y las más bajas se detectaron en Rusia, con 16.000 euros de media."[120]

La industria estadounidense es un modelo a seguir mundialmente, gracias al desarrollo e innovación alcanzado. Por esta razón la mayoría de las empresas del país se ven afectadas por ataques informáticos. "En otro estudio realizado en esta ocasión por el FBI, se ponía de manifiesto que casi un 90% de las empresas de Estados Unidos habían sido infectadas por virus o sufrieron ataques a través de Internet en los años 2004 y 2005, pese al uso generalizado de programas de seguridad. Estos ataques habían provocado unos daños por un importe medio de unos 24.000 dólares en las empresas e instituciones afectadas. Además, según los propios datos del FBI, cerca de un 44% de los ataques provenían del interior de las organizaciones."[121]

---

[118] Verton D. (2004). *Terror en la red: Internet como arma*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.55). Madrid: McGraw-Hill.

[119] Seguridad Informática. (agosto 22, 2013). *Solo el 35% de las organizaciones detectan filtraciones en los primeros minutos*. enero 4, 2018, de Seguridad Informática Sitio web: https://seguinfo.wordpress.com/category/estadisticas/.

[120] Seguridad Informática. (agosto 22, 2013). *Solo el 35% de las organizaciones detectan filtraciones en los primeros minutos*. enero 4, 2018, de Seguridad Informática Sitio web: https://seguinfo.wordpress.com/category/estadisticas/.

[121] Gómez A. *La lucha contra el ciberterrorismo y los ataques informáticos*. (p.3). noviembre 13, 2017, de EDISA Sitio web: https://www.edisa.com/wp-content/uploads/2019/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf.

El sector automotriz es otro de los afectados por el fenómeno digital donde las mermas económicas registradas superan los cien mil millones de dólares. La autora María Sánchez destaca algunas de las empresas afectadas; “Autoridades estadounidenses estiman que este espionaje les cuesta a las empresas de EE.UU. entre US$100 y US$250 mil millones de dólares. General Motors, Ford, General Electric and Boeing presuntamente están entre las compañías perjudicadas.”[122]

El ciberterrorismo es un fenómeno que año con año va en aumento, esto se observa en las cifras arrojadas por estudios realizados en el periodo que va de 2013 a 2017, donde las pérdidas han aumentado más del 50%. “Lógicamente para hacernos una idea del impacto económico global de los ciberataques, lo más fácil es hacer un repaso a los datos de años anteriores. El estudio elaborado por Accenture determina que de 2013 a 2017 el coste medio de los ciberataques ha aumentado un 62%. De hecho, sólo en el 2017 se ha incrementado un 27.4% respecto a 2016. Y es que en lo que llevamos de año, el coste medio se establece en 11.7 millones de dólares.”[123]

Las cifras de daños por ciberataques también deben considerar factores como la cantidad de capital que se invierte en programas de ciberseguridad en consecuencia de un ciberataque, ya que esto representa millones de dólares, como menciona la autora Martha Arana; “Las compañías gastaron de media 2 millones de dólares en combatir el malware (software malicioso) y 2.4 en los ataques de tipo web el año pasado.”[124]

En síntesis, las empresas son un sector importante de donde se sustrae información de manera ilícita, situación que tiene consecuencias económicas que van en aumento al igual que el número de ataques, esto refleja la necesidad de desarrollar mayores y mejores programas en ciberseguridad.

---

[122] Sánchez M. (marzo 5, 2011). *El espionaje industrial chino en aumento*. diciembre 7, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2011/03/110224_china_espionaje_economico_mes.shtml.

[123] Arana M. (octubre 24, 2017). ¿Cuánto cuestan un ciberataque a las empresas?. enero 16, 2018, de ODS Sitio web: https://opendatasecurity.io/es/cuanto-cuesta-un-ciberataque-a-las-empresas/.

[124] Arana M. (octubre 24, 2017). ¿Cuánto cuestan un ciberataque a las empresas?. enero 16, 2018, de ODS Sitio web: https://opendatasecurity.io/es/cuanto-cuesta-un-ciberataque-a-las-empresas/.

3.5. LAS INFRAESTRUCTURAS CRÍTICAS; EL SISTEMA NERVIOSO DE UNA NACIÓN.

En este apartado se plantearán las denominadas Infraestructuras Críticas (IC) y su importancia para la estabilidad nacional, considerado el sistema nervioso de un país y estos sistemas abarcan más allá del sector militar. “Las ciberamenazas a la seguridad nacional de EE.UU. no se limitan a blancos militares. Los hackers y los gobiernos extranjeros pueden lanzar cada vez más intrusiones a las redes que controlan la infraestructura civil crítica. Fallas inducidas por computadora a las redes de energía de EE.UU., a las redes de transporte o a los sistemas financieros podrían causar daños físicos masivos y trastornos económicos.”[125]

El presidente Clinton estableció la Comisión del Presidente sobre la Protección de Infraestructuras Críticas, donde por primera vez se habló del valor de dichos sistemas y necesidad de estudiarlos y cuidarlos, responsabilidad que se otorgó tanto al sector público como privado. “En respuesta a estas crecientes vulnerabilidades de la infraestructura crítica, el presidente Clinton estableció en 1996 la Comisión del Presidente sobre la Protección de la Infraestructura Crítica (PCCIP), con objeto de estudiar las infraestructuras críticas que constituyen los sistemas de apoyo vitales de Estados Unidos, determinar vulnerabilidades y proponer una estrategia para protegerlas. La comisión, en su informe de 1997 "Basamentos Críticos: Protección de las Infraestructuras de Norteamérica", destacó que la seguridad de la infraestructura crítica es una responsabilidad que comparten los sectores público y privado.”[126]

Respecto al objetivo de la Comisión Presidencial de Protección de Infraestructuras Críticas el autor Dan Verton complementa con lo siguiente; “La Comisión Presidencial de Protección de Infraestructuras Críticas se había formado un año antes de Eligible Receiver. Su propósito era simple: estudiar las implicaciones en la seguridad nacional del vertiginoso ritmo de desarrollo de las tecnologías de la información y, específicamente, la velocidad suicida a la que las infraestructuras críticas en la sociedad de EE.UU. estaban siendo migradas a Internet.”[127]

Las IC hoy en día sirven a criminales como un medio de presión en contra de los gobiernos, debido a la sensibilidad e interconectividad existente entre ellas, además, estas controlan

---

[125]Lynn W. *Defendiendo un nuevo ámbito, la ciberestrategia del Pentágono*. (p.6). abril 10, 2018, de air&space power journal Sitio web: http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/1524/Defendiendo%20un%20nuevo%20%C3%A1mbito.%20La%20ciberestrategia%20del%20Pent%C3%A1gono.pdf?sequence=1&isAllowed=y.

[126]Muñoz M. (julio 24, 2003). *Infraestructuras*. julio 2, 2019, de Belt.es Sitio web: http://www.belt.es/noticias/2003/julio/24/infraestructuras.htm.

[127] Verton D. (2004). *Ciberterrorismo: Realidad o ficción*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.38). Madrid: McGraw-Hill.

ciertos sistemas que afectarlos tendría severas repercusiones en el país. “Las infraestructuras críticas son aquellos sistemas físicos y cibernéticos esenciales para las operaciones mínimas de la economía y el gobierno. Incluyen, entre otros, telecomunicaciones, energía, banca y finanzas, transporte, sistemas de agua y servicios de emergencia, tanto gubernamentales como privados. Muchas de las infraestructuras críticas de la nación han sido históricamente sistemas separados física y lógicamente que tenían poca interdependencia. Sin embargo, como resultado de los avances en la tecnología de la información y la necesidad de mejorar la eficiencia, estas infraestructuras se han vuelto cada vez más automatizadas e interconectadas. Estos mismos avances han creado nuevas vulnerabilidades ante fallas de equipos, errores humanos, clima y otras causas naturales, y ataques físicos y cibernéticos. Abordar estas vulnerabilidades necesariamente requerirá flexibilidad.”[128]

Como resultado de la dependencia tecnológica en la actualidad el funcionamiento de las Infraestructuras Críticas depende de medios informáticos, por esta razón son vulnerables a ciberataques, además, de los daños que pueden ocasionarse a través de ellas. “Las infraestructuras críticas, compuestas de instituciones públicas y privadas, constituyen el sistema nervioso de las naciones desarrolladas. El ciberespacio es fundamental para su funcionamiento y, por ello, para la seguridad de la nación. La globalización de Internet hace que los centros de gravedad de un Estado sean más vulnerables a un ataque, al ser las fronteras de la red permeables. Un ataque contra el sistema informático de una infraestructura crítica puede generar muchos daños con un riesgo mínimo para el atacante.”[129]

Asimismo, los países desarrollados son sociedades con un alto nivel de interconectividad y dependencia tecnológica en su estructura, por esta razón son vulnerables a sufrir ciberataques.

El autor A. Gomez Vieites expone algunas de las consecuencias de dañar Infraestructuras Críticas. “Entre las posibles consecuencias del ciberterrorismo y de los ataques informáticos, podríamos citar las siguientes:

- Corte del suministro eléctrico y posible descontrol de centrales nucleares, centrales hidroeléctricas y térmicas.
- Colapso total de las redes telefónicas y los sistemas de comunicaciones.

[128] Directiva de Decisión Presidencial. (mayo 22, 1998). *Protección de infraestructura crítica*. octubre 4, 2018, de La Casa Blanca Washington Sitio web: https://fas.org/irp/offdocs/pdd/pdd-63.htm.

[129] Puime J. (2009). *El ciberespionaje y la ciberseguridad*. En La violencia del siglo XXI. Nuevas dimensiones de la guerra (p.48). España: Ministerio de Defensa.

- Desarrollo de ataques específicos contra los sistemas de comunicaciones militares."[130]

Dentro de las IC existen sistemas esenciales en la estructura de los países, tal como el eléctrico de quien depende el funcionamiento de otros sistemas alternos, al respecto Dan Verton menciona: "Si el sector de la energía experimentase un fallo o interrupción importante, sufriría todo lo que depende de la energía. Y hay pocas cosas en este mundo moderno nuestro que no funcionen con alguna clase de energía: petróleo, gas natural o electricidad. Y las interdependencias han aumentado incluso dentro de esas tres categorías energía, como, por ejemplo, la creciente dependencia del gas natural de las estaciones generadoras de electricidad (la alternativa <<ecológica>>) para alimentar las turbinas."[131]

Proteger los sistemas sensibles de un país en la actualidad es una responsabilidad de Seguridad Nacional para evitar acontecimientos incluso como la explosión en Hiroshima, escenarios posibles de provocar hoy en día desde un monitor, como la explosión del gasoducto soviético, planteado por Alejandro. "En 1982, hace la friolera de 33 años, un gasoducto soviético en Siberia explotó como consecuencia de algún tipo de sabotaje cibernético, dando lugar a la mayor explosión no nuclear jamás registrada. Se habla de una potencia de tres kilotones, que lo destruyó completamente. La explosión fue de tal magnitud, que fue el primer fuego visto desde el espacio. No fue Hiroshima, pero no estuvo nada mal, vaya. Se supone que alguna agencia norteamericana estaba detrás de este sabotaje."[132]

Otro de los primeros casos de ciberataques registrados, es el ataque al sistema ferroviario nipón, donde se muestra el peligro de la dependencia tecnológica en Infraestructuras Críticas. "El primer ataque digital a infraestructuras críticas tuvo lugar en 1985, y no nos debe extrañar que se produjera en Japón, una de las mecas mundiales del desarrollo tecnológico. En aquella ocasión, el grupo terrorista Middle Core Faction, una banda armada de ideología izquierdista radical, que nació tras la fragmentación del Partido Comunista de Japón, en 1957, atacó el sistema que controlaba los trenes de alta velocidad nipones. Para ello, cortaron el suministro eléctrico y los cables de control informatizados del ferrocarril, y después interceptaron y perturbaron las radiocomunicaciones de la policía para anticiparse a la respuesta de los agentes y ralentizarla. Afortunadamente, nadie resultó herido, pero 6,5 millones de viajeros se

[130] Gómez A. *La lucha contra el ciberterrorismo y los ataques informáticos*. (p.1). noviembre 13, 2017, de EDISA Sitio web: https://www.edisa.com/wp-content/uploads/2019/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf.

[131] Verton D. (2004). *Terror en la red: Internet como arma*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.43). Madrid: McGraw-Hill.

[132] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p.174). España: Deusto S.A. Ediciones.

vieron afectados por el atentado, y la empresa atacada perdió alrededor de seis millones de dólares de la época."[133]

Estados Unidos resalta ocho Infraestructuras Críticas plasmadas en la Orden Ejecutiva Presidencial 13010, al respecto el autor Dan Verton resalta; "Esas infraestructuras habían sido identificadas por la Orden Ejecutiva presidencial 13010 como <<críticas>> debido al potencial impacto debilitador que su destrucción o interrupción podría tener a escala regional o nacional. Se identificaron ocho sectores de infraestructuras, en este orden: telecomunicaciones, energía eléctrica, almacenamiento y transporte de petróleo y gas, bancos y finanzas, transportes, suministros de agua, servicios de emergencia (incluyendo los servicios médicos de emergencia, policía, bomberos y rescate), y servicios gubernamentales."[134]

Los avances tecnológicos se han vuelto indispensables en el funcionamiento de un sinfín de servicios básicos para los individuos, mismos que son controlados por las mencionadas IC, donde un fallo en su funcionamiento puede tener repercusiones, en la estabilidad tanto económica como nacional de un país. "Orden Ejecutiva 13010, firmada por el presidente, Clinton en 1996, defendía ocho infraestructuras críticas cuyos servicios eran tan vitales que su incapacidad o destrucción tendría un impacto debilitador en la defensa o en la seguridad económica de Estados Unidos. Todas esas infraestructuras dependen de computadoras o/y redes informáticas, incluyendo la Internet pública, para su funcionamiento continuo y su gestión diaria. Además, muchas infraestructuras no pueden funcionar bajo condiciones de apagones prolongados o fallos en otras infraestructuras."[135]

Juan Puime destaca otros sectores de importancia en la estructura nacional, como universidades quienes son parte de proyectos del gobierno, relacionados al ámbito digital como el desarrollar tecnología e investigaciones con el fin de crear un ciberejército. "Entre las infraestructuras vitales de un país se encuentran los medios de telecomunicaciones, las redes de distribución (agua, electricidad, gas o petróleo), los servicios de emergencia, los medios de transporte, los servicios gubernamentales y las Fuerzas Armadas. Organizaciones de gran entidad como bancos y universidades también son blancos para ciberataques, ya que muchas forman parte de estas infraestructuras críticas. Estas redes también controlan instalaciones físicas, como estaciones transformadoras de electricidad, centrales hidroeléctricas, bombas de

[133] Suárez A. (2015). *Ciberterrorismo*. En El Quinto Elemento (p.147). España: Deusto S.A. Ediciones.
[134] Verton D. (2004). *Terror en la red: Internet como arma*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.21). Madrid: McGraw-Hill.
[135] Verton D. (2004). *Infraestructuras Críticas*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.259). Madrid: McGraw-Hill.

oleoductos y gasoductos, mercados de valores, etc. De modo que la economía y seguridad nacionales dependen en gran medida de las tecnologías de la información y de la infraestructura de comunicaciones."[136]

Meschulam complementa al respecto de cómo la interdependencia se convierte en una vulnerabilidad para los gobiernos y su estabilidad, al plantear otros sistemas dependientes de la tecnología. "El problema principal radica en la dependencia en infraestructura tecnológica que todas las naciones han venido desarrollando en los últimos tiempos. La economía, las transacciones financieras, comerciales, la información, la comunicación, y una gran cantidad de actividades humanas, descansan en el buen y ágil funcionamiento de la red y de los sistemas cibernéticos. Esa dependencia se traduce en una enorme vulnerabilidad: quien quiere ejercer daños a veces incuantificables e irreparables, solo tiene que encontrar la manera de penetrar o golpear esos sistemas, ya sea de manera física o virtual."[137]

La dependencia tecnológica es un fenómeno en aumento, como resultado de las ventajas que la automatización de procesos y la tecnología en general proporcionan a la sociedad. "Servicios críticos para una sociedad moderna, como podrían ser los servicios financieros o la propia administración pública están soportados en su práctica totalidad por sistemas y redes informáticas, hasta el punto de que en muchos de ellos se han eliminado o reducido de forma drástica los papeles y los procesos manuales."[138] En respuesta a la crisis ambiental que hoy en día se experimenta, algunas empresas se apoyan de la tecnología e implementan prácticas como la digitalización de documentos, medida que ayuda a reducir el uso de papel.

Estados Unidos al entender la relevancia de las Infraestructuras Críticas realizó, a través del Departamento de Energía y el Mando Olímpico de Seguridad Pública, una de las primeras pruebas para medir el impacto de un ciberataque. "El primer ejercicio importante de interdependencia de las infraestructuras tuvo lugar en noviembre de 2000 en la preparación de los Juegos Olímpicos de Invierno de 2002 en Utha. Conocidas por su nombre en código, Black Ice, la simulación fue propuesta por el Departamento de Energía de EE. UU. y el Mando Olímpico de Seguridad Pública de Utha. Black Ice demostró con aterrador detalle cómo los

---

[136] Puime J. (2009). *El ciberespionaje y la ciberseguridad*. En La violencia del siglo XXI. Nuevas dimensiones de la guerra (p.49). España: Ministerio de Defensa.

[137] Meschoulam M. (octubre 30, 2015). *Ciberguerra y ciberterrorismo: ¿Futuro o presente?*. noviembre 13, 2017, de El Universal Sitio web: http://www.eluniversal.com.mx/entrada-de-opinion/articulo/mauricio-meschoulam/mundo/2015/10/30/ciberguerra-y-ciberterrorismo

[138] Gómez A. La lucha contra el ciberterrorismo y los ataques informáticos. (p.1). noviembre 13, 2017, de EDISA Sitio web: https://www.edisa.com/wp-content/uploads/2019/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf.

efectos de un ataque terrorista o desastre natural pueden significativamente ser peores debidos a un ciberataque simultaneo contra las computadoras que gestionan las infraestructuras críticas de la región."[139]

Una de las empresas encargadas del suministro de agua en Estados Unidos también realizó pruebas a sus sistemas informáticos. Dichas pruebas ayudan a saber si es o no seguro. "Sólo entre 2011 y 2013, las intrusiones en sistemas informáticos de infraestructuras críticas aumentaron un 1.700 por ciento. La preocupación por este tipo de ataques es tal que, en 2011, una empresa de suministro de agua de California contrató a un equipo de hackers para poner a prueba la seguridad de su red de ordenadores. Los responsables de la compañía quedaron bastante preocupados cuando comprobaron que los hackers a sueldo habían logrado romper la seguridad de los sistemas en menos de una semana."[140]

El sistema bancario es otro sector sensible dentro de la estructura de un país y su buen funcionamiento es indispensable para la estabilidad nacional, un fallo en el podría ocasionar grandes pérdidas. "La banca se sitúa como el sector más perjudicado por las ciberamenazas, ya que el coste medio anual se establece en 18.28 millones de dólares."[141]

El 11 de septiembre de 2001 mostró la vulnerabilidad y sensibilidad del sector aeroportuario ante las ciberamenazas, aunque no se considera un ciberataque en las pruebas forenses se detecto el uso de herramientas informáticas durante el ataque para dañar la señal de las bases aéreas. "Las vulnerabilidades en la seguridad inalámbrica en aeropuertos y aerolíneas son ciertamente un serio problema de seguridad pública."[142]

Los efectos del ciberterrorismo dependen del sector afectado, es decir, un daño en cada una de las infraestructuras críticas representa diferentes consecuencias para el país. Alejandro Suárez plantea algunas de dichas consecuencias; "Borg asegura que; los ataques informáticos podrían destruir generadores eléctricos, incendiar refinerías de petróleo, hacer explotar oleoductos, contaminar el agua potable, provocar fugas de gases tóxicos, dar lugar a accidentes de trenes y aviones, paralizar los servicios de emergencia o reducir al caos el sistema bancario. Y todo sin necesidad de una participación humana directa."[143]

---

[139] Verton D. (2004). *Black Ice: Los peligros ocultos del ciberterrorismo*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.20). Madrid: McGraw-Hill.

[140] Suárez A. (2015). *Ciberterrorismo*. En El Quinto Elemento (p.147). España: Deusto S.A. Ediciones.

[141] Arana M. (octubre 24, 2017). *¿Cuánto cuestan un ciberataque a las empresas?*. enero 16, 2018, de ODS Sitio web: https://opendatasecurity.io/es/cuanto-cuesta-un-ciberataque-a-las-empresas/.

[142] Verton D. (2004). *Terror en el aire: La amenaza inalámbrica*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.77). Madrid: McGraw-Hill.

[143] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (pp. 208-209). España: Deusto S.A. Ediciones.

Las IC demandan cierta atención porque dañarlas puede tener efectos como paralizar servicios indispensables para la población, consecuencias económicas para el país y las instituciones, además, en algunas ocasiones las consecuencias pueden ser mortales, como menciona Néstor Ganuza: "La amenaza cibernética no sólo puede afectar al normal desenvolvimiento de la vida de los ciudadanos de un país, sino que puede afectar a la infraestructura crítica nacional conllevando riesgos de daños físicos para la población."[144]

Asimismo, dichas infraestructuras se consideran el sistema nervioso de un país por toda la estructura que tienen bajo su control y la utilidad de estos servicios para el funcionamiento de la sociedad, ya que algunos de ellos se consideran pilares de Seguridad Nacional y estabilidad económica como resalta la Oficina del Secretario de Prensa de los Estados Unidos; "La seguridad nacional y económica de los Estados Unidos depende del funcionamiento confiable de la infraestructura crítica de la Nación." [145] Por esta razón es que son elementos claves para mantener la seguridad y es necesario desarrollar medidas de protección adecuadas.

3.6. CHINA VS ESTADOS UNIDOS, UNA LUCHA POR EL PODERÍO MUNDIAL.

En este apartado se planteará la relación que surge entre Estados Unidos y China a consecuencia de la era digital, donde sobresale el interés de China por información estratégica no solo de Estados Unidos sino también de otros gobiernos y empresas. "China ha sido centro permanente de atención y protagonista de muchos titulares, como origen de permanentes oleadas de ciberataques y continuas acusaciones de ciberespionaje por parte de EE.UU. y otros países occidentales. Estas acusaciones han sido siempre rechazadas por el gobierno chino."[146]

La actividad informática de China es motivada por diversos factores entre los que sobresale el interés comercial, donde el país busca alcanzar desarrollo económico y convertirse en potencia mundial. Entre los afectados por la oleada de ciberataques chinos se encuentra Estados Unidos, sin embargo, Julián Alfonso destaca a países como; "Corea del Sur, Japón, EE.UU., India y varios países europeos, entre ellos Francia, Alemania y Reino Unido, que denunciaban

---

[144] Ganuza N. (febrero 2011). *La situación de la ciberseguridad en el ámbito internacional y en la OTAN*. En Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio (p. 195). España: Ministerio de Defensa.

[145] Oficina del Secretario de Prensa. (febrero 9, 2016). *Plan de acción de ciberseguridad*. enero 10, 2018, de La Casa Blanca Sitio web: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[146] Alfonso J. (septiembre 2015). *Ciberguerra y ciberarmamento.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema Nacional de Seguridad. (p.101) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.

los constantes ataques chinos contra sus empresas y las constantes violaciones de los derechos de propiedad intelectual e industrial."[147]

Uno de los sectores afectados, por la oleada de ciberataques que experimenta hoy en día la sociedad mundial, es el sector empresarial por ello algunos autores plantean la existencia de una guerra comercial en el ciberespacio. "La tensión por el espionaje industrial y la vulneración de la propiedad intelectual ha marcado durante años la relación entre EE UU y China … La batalla en Internet no la libran sólo los militares y los espías. El robo de propiedad intelectual y de secretos empresariales es el último foco de tensión entre Estados Unidos y China. La ciberguerra también es comercial."[148] Además, la relación China – Estados Unidos se ha visto afectada como consecuencia de la guerra comercial.

Del sector empresarial, China persigue específicamente información sobre tecnología porque la falta de producción de esta por parte del país se ha convertido en el obstáculo para alcanzar el desarrollo. "Noviembre de 2011. EE UU acusa a China del robo "persistente" de su tecnología. Washington denuncia el espionaje económico e informático por agentes de Pekín y compañías privadas."[149]

Los ataques informáticos preocupan a Estados Unidos porque dicho fenómeno atenta contra su estabilidad económica y ponen en peligro su seguridad nacional, en este sentido Eva Saiz menciona; "Para EE UU este es un asunto de importancia estratégica decisiva porque, no solo se enfrenta al riesgo tradicional de que sus secretos de seguridad caigan en mano de una potencia extranjera, sino al peligro nuevo de que, con la intrusión en la red de Internet, China pueda sabotear la actividad económica del país o inhabilitar servicios públicos básicos, como los de agua potable o energía eléctrica. Sin contar con el robo de tecnología que, además de costarle miles de millones de dólares a este país, aumenta extraordinariamente las capacidades de China y su competencia de cara al futuro."[150]

---

[147] Alfonso J. (septiembre 2015). *Ciberguerra y ciberarmamento.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema Nacional de Seguridad. (pp.90-91) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.

[148] Bassets M. (mayo 19, 2014). *Washigton acusa a cinco militares chinos de ciberespionaje industrial*. noviembre 11, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html.

[149] El País. (mayo 19, 2014). *Las acusaciones de EEUU a China por espionaje*. diciembre 5, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400515474_703728.html.

[150] Saiz E. (marzo 13, 2013). *Los ciberataques sustituyen al terrorismo como primera amenaza para EEUU*. enero 30, 2018, de El País Sitio web: https://elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html.

Google es una de las empresas afectadas por los ataques cibernéticos de origen chino, derivado de la cantidad de información que concentra, dichos agravios originaron la "Operación Aurora" misma que se planteará en otro apartado. "Enero de 2010. Google hace público que una serie de ciberataques han sustraído información confidencial de diversas empresas estadounidenses, algo que le lleva a cerrar sus operaciones en China, principal sospechosa. El Gobierno de Estados Unidos pide a Pekín que haga cumplir la ley en la Red."[151]

Además, de las empresas, la información militar estadounidense también es afectada por los ataques digitales y ha registrado pérdidas por dicho fenómeno. "04 de mayo de 2013. Ciberespías chinos logran sortear a EE UU y robar secretos militares vitales. La Casa Blanca se dispone a pedir cuentas al país asiático por la tecnología robada gracias a la piratería informática."[152]

En los últimos años China ha lanzado productos comerciales y artefactos militares con los que busca dar el salto al desarrollo, sin embargo, EE.UU. ha realizado acusaciones al respecto donde señala el robar dichos proyectos. "Entre las muchas denuncias por ciberespionaje a China, el Departamento de Defensa de EE.UU. afirma que la tecnología del caza furtivo de 5° generación Shenyang J-31, fue obtenida de forma ilegítima de los desarrollos del Lockheed Martin F-35 Lightning, a través de la Oficina China de Información Técnica con sede en la provincia de Chengdu, y de allí fueron suministrados a la corporación estatal aeronáutica china, encargada de filtrar la información y suministrarla a empresas de los sectores aeroespacial y tecnológico, lo que facilitó a los chinos un salto tecnológico de dos generaciones y varias décadas de desarrollos."[153]

El gobierno de Estados Unidos señala la pérdida de 300 millones de dólares con el robo del proyecto de caza furtivo, además, menciona la pérdida de información confidencial de otros sectores del país. "Un grupo de hackers ha lanzado un ataque cibernético con objetivo el Pentágono del cual han podido sustraer terabytes de información entre los que destaca el proyecto Joint Strike Fighter valorado en 300.000 millones de dólares, el más caro de la historia

[151] El País. (mayo 19, 2014). *Las acusaciones de EEUU a China por espionaje*. diciembre 5, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400515474_703728.html.

[152] El País. (mayo 19, 2014). *Las acusaciones de EEUU a China por espionaje*. diciembre 5, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400515474_703728.html.

[153] Alfonso J. (septiembre 2015). *Ciberguerra y ciberarmamento.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema Nacional de Seguridad. (p.95) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.

del Pentágono. Está relacionado con el nuevo avión caza F-35. Los datos se sustrajeron gracias al uso de vulnerabilidades de webs de algunos contratistas."[154]

María Sánchez complementa planteando que, además, de la pérdida de planos del caza furtivo F-35, también se extraviaron proyectos de otros vehículos como submarinos y armamento militar. "Según Rachwald, se estima que fue por medio de ciberataques que los chinos se apropiaron de los planes de construcción de un modelo de submarino desarrollado por EE.UU., algo que China niega con vehemencia. "El gobierno de EE.UU. cree que el diseño para la construcción de submarinos y otras armas fueron tomados de sus computadores", señala."[155]

Los ciberataques chinos se caracterizan por ser estratégicos, al robar información que favorece al gobierno y empresas nacionales de diferentes sectores, como el sector energético. "Los militares están acusados de usurpar secretos de algunas de las mayores empresas de EE UU en sectores clave como el acero, el aluminio y la energía nuclear."[156]

Además del sector energético, la industria metalúrgica también es uno de los sectores afectados por el ciberespionaje chino, principalmente las empresas dedicadas a la producción de metales como el acero y aluminio, quienes son claves en la economía del país. En este sentido Marc Bassets destaca algunas de las empresas afectadas por la actividad informática china; "China ha lanzado ataques informáticos contra sectores que van desde la energía hasta las finanzas. Pero el caso anunciado no se centra en Wall Street o en sectores que quizá prefieran que su nombre no figure en una disputa de este calibre, sino en cinco empresas que tienen en común su vínculo con sectores industriales que se sienten amenazados por la competencia china y las deslocalizaciones en ese país. Las empresas son Westinghouse Electric, Alcoa, Allegheny Technologies, US Steel y Solar World, además del sindicato del acero United Steelworkers. El fiscal de Pensilvania David Hickton vinculó en la rueda de prensa con Holder las acciones del Ejército chino con la pérdida de empleos en regiones golpeadas por la desindustrialización."[157]

---

[154] Maturana J. (abril 21, 2019). *Hackers atacan el Pentágono*. mayo 21, 2020, de MC Sitio web: muycomputer.com/2009/04/21/actualidadnoticiashackers-atacan-el-pentagono_we9erk2xxdbnybiqxkd6elyiyrjdbw1059gc84jtpr_-wqrbldxlc5ynzmdyqrbn/.

[155] Sánchez M. (marzo 5, 2011). *El espionaje industrial chino en aumento*. diciembre 7, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2011/03/110224_china_espionaje_economico_mes.shtml.

[156] Bassets M. (mayo 19, 2014). *Washigton acusa a cinco militares chinos de ciberespionaje industrial*. noviembre 11, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html.

[157] Bassets M. (mayo 19, 2014). *Washigton acusa a cinco militares chinos de ciberespionaje industrial*. noviembre 11, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html.

La siguiente imagen muestra como en 2017 China contralaba aproximadamente la mitad del mercado del acero a nivel mundial, por ello su interés de obtener información de otras empresas que comenzaron a figurar en el mercado y ponen en peligro el comercio del país.

(https://circulodeempresarios.org/publicaciones/asi-esta-la-empresa-marzo-2018/, 24/06/19)

La red eléctrica también es blanco de los criminales, al considerarse parte de las Infraestructuras Críticas de los Estados por la cantidad de sistemas que controla, además, dañarlo tendría consecuencias severas para el país. “Abril de 2009. EE UU revela que espías localizados en Rusia, China y otros países se han infiltrado en su red eléctrica. Su intención podría haber sido tomar control de esa red en caso de guerra, según oficiales cercanos al Gobierno.”[158]

La administración de Barack Obama, en materia de ciberterrorismo se caracterizó por responsabilizar al gobierno chino de la actividad informática que afectaba al país, principalmente a las empresas nacionales. “El asesor de Seguridad Nacional del presidente de EE UU, Thomas E. Donilon, exigió a las autoridades chinas que dejaran de sustraer información comercial de los ordenadores de las empresas estadounidenses. Las declaraciones de Donilon son las primeras en las que un miembro de la Administración Obama responsabiliza directamente a China de lo que muchos funcionarios del Gobierno de EE UU han calificado como una campaña sistemática de ciberespionaje comercial a las empresas estadounidenses.”[159]

---

[158] El País. (mayo 19, 2014). *Las acusaciones de EEUU a China por espionaje*. diciembre 5, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400515474_703728.html.

[159] Saiz E. (marzo 13, 2013). *Los ciberataques sustituyen al terrorismo como primera amenaza para EEUU*. enero 30, 2018, de El País Sitio web: https://elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html.

Estados Unidos también acuso al ejército chino de participar en las agresiones informática implementada en su contra, fenómeno que cuesta al gobierno estadounidense millones de dólares anualmente. “La acusación formal contra militares chinos, anunciada en Washington en mayo de 2014 por el fiscal general Eric Holder, titular del Departamento de Justicia de EE.UU., representa la primera vez que se presentan imputaciones criminales contra funcionarios gubernamentales de otro país por ciberespionaje. Según una estimación citada por The Washington Post, el ciberespionaje comercial cuesta a EE UU entre 24.000 y 120.000 millones de dólares al año (entre 17.500 y 88.000 millones de euros).”[160]

Pese a la negación del gobierno chino de su relación con los ciberataques en contra de Estados Unidos, este realiza dicha afirmación por los patrones seguidos en cada ataque, sin embargo, China manifiesta también ser víctima de actividad informática originada en Estados Unidos. “La sombra de los ciberataques procedentes de China parece siempre seguir unos parámetros que difícilmente podrían apuntar a hackers individuales. Así los sucesivos ataques a empresas, prensa y organismo gubernamentales como la NASA, no dejan de apuntar, aunque sin pruebas concluyentes, hacia miembros apoyados por el propio gobierno. La contraparte es aún más oscura. China, apenas reporta casos en los que su seguridad haya sido comprometida, a pesar de la constancia de que no dejan de sucederse casos en ambas direcciones. Así, el ministerio de Defensa chino y otros sitios militares han llegado a contabilizar mensualmente un promedio de 144.000 a lo largo de 2012, de cuyo origen parece que un 62,9% partía de EEUU según una de las pocas informaciones suministradas.”[161]

Edward Snowden, exagente de la Agencia de Seguridad Nacional, confirmo en 2013 la actividad cibernética que Estados Unidos mantenía en contra de China, ataques a través de los cuales se obtenía información sobre tecnología como, la fibra óptica. “En el año 2013, Snowden demostró que la NSA había hackeado los sistemas de la prestigiosa Universidad de Tsinghua, en Pekín. El suceso es de especial relevancia, porque esta universidad es una de las seis columnas vertebrales que conducen el tráfico de internet por todo el país. Estados Unidos también pirateó la sede de Pacnet en Hong Kong, una de las mayores compañías de fibra óptica de la región Asia-Pacífico.”[162]

---

[160] Alfonso J. (septiembre 2015). *Ciberguerra y ciberarmamento.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema Nacional de Seguridad. (pp. 101-104) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.

[161] Andrades F. (mayo 7, 2013). *Cinco escenarios de ciberguerra en el nuevo orden mundial*. abril 23, 2018, de eldiario.es Sitio web: https://www.eldiario.es/turing/escenarios-ciberguerra-nuevo-orden-mundial_0_129837338.html.

[162] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p.180). España: Deusto S.A. Ediciones.

De acuerdo al informe de la empresa Taia Global (empresa especializada en ciberseguridad), los efectos del ciberterrorismo en China, se deben a la falta de regulación en el ciberespacio. “Según Jeffrey Carr, fundador de la empresa de ciberseguridad Taia Global, está claro que en China se originan un gran número de ataques porque no hay leyes ni una cultura de protección de la propiedad intelectual, pero los chinos no son los únicos.”[163]Asimismo, el ciberterrorismo en dicho país se ve favorecido por la falta de licencias originales en los equipos, derivado de los altos índices de piratería que lo caracterizan. “Lo cierto es que China es el país que sufre el mayor número de ciberataques del mundo. El 95 por ciento del software que usan los ordenadores chinos es pirata. Esto significa que no cuentan con las últimas actualizaciones de seguridad ni los parches que tienen quienes usan una licencia legal.”[164]

En resumen, la relación Estados Unidos - China en la era digital se ha caracteriza por los múltiples ciberataques de ambas partes, ataques motivados por diversos factores que, además, han originado una guerra comercial entre estos.

3.6.1. OPERACIÓN AURORA, LOS INTERESES POLÍTICOS DETRÁS DEL CIBERESPIONAJE ECONÓMICO.

A continuación, se planteará el caso del ciberataque que afecto a distintas multinacionales estadounidenses entre ellas la firma de Google, quien tomo medidas definitivas en su relación con China. Dicho acontecimiento denominado “Operación Aurora” demostró que los ciberataques son motivados por diversos factores entre los que destaca el económico y político. “El caso de espionaje económico quizá más importante protagonizado por el gobierno de China es el que recibió el nombre de «Operación Aurora». En esta ocasión, los objetivos del ataque fueron varias decenas de multinacionales, entre las que destacaba Google; pero el robo de la información empresarial no sería destinado únicamente a usos comerciales, sino también políticos.”[165]

La Operación Aurora también mostró la necesidad de las empresas de capacitar a su personal en materia de ciberseguridad, ello sin importar la función del empleado porque todos son una pieza clave para prevenir a tiempo cualquier irregularidad en la red informática, pero, también

[163] Benedicto M. (abril 23, 2013). *EEUU ante el reto de los ciberataques*. (p.5) diciembre 26, 2017, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO37-2013_Ciberataques_BenedictoSolsona.pdf.
[164] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p.180). España: Deusto S.A. Ediciones.
[165] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (pp.60-61). España: Deusto S.A. Ediciones.

son la parte clave para permitir la propagación de programas maliciosos. “En diciembre de 2009, diversos empleados de Google localizados en China y varios países más recibieron un extraño correo electrónico en el que se les pedía que clicaran en un enlace. Un troyano se descargó de forma secreta en los ordenadores infectados, instalando un programa que permitía el acceso remoto de un usuario no autorizado para robar la información almacenada. El malware era tan sofisticado (utilizaba hasta ocho zero days, algo nunca visto antes) que resultaba casi imposible determinar quién era el responsable de la operación, pero una serie de indicios llevaron a sospechar que el Gobierno de China estaba detrás de lo sucedido. Después de un rastreo exhaustivo, la NSA llegó a la conclusión de que los ataques provenían de dos universidades chinas que mantenían estrechos vínculos con el Ejército Popular de Liberación, rama militar del Partido Comunista Chino.”[166]

Además de Google, alrededor de 34 empresas multinacionales resultaron afectadas por el malware que culminó con la Operación Aurora. “Varios empleados de Google asentados en China y otros países, recibieron correos electrónicos “extraños”: los invitaba a acceder a una página de internet, a través de un link. Lo que siguió después ya se ha etiquetado como “Uno de los ciberataques más sofisticados hasta ahora registrados”. Bautizada con el nombre de “Operación Aurora”, en el que además de Google, otras 34 empresas multinacionales (hasta ahora es el número detectado) sufrieron robo de información a través de un “malware” (software malicioso”).”[167]

Empresas de distintos sectores resultaron afectadas por el malware Agent.btz, causante de la Operación Aurora, entre dichos sectores destaca la industria de softwares y servicios informáticos, en este sentido Alejandro Suárez plantea algunas de las empresas afectadas: “Google no fue la única víctima de este ciberataque, que golpeó a cerca de cuarenta multinacionales, entre ellas Adobe, Juniper, Rackspace, Symantec, Northrop Grumman, Morgan Stanley y Yahoo!.”[168]

Entre las empresas perjudicadas también se encuentran las dedicadas a servicios de seguridad informática, lo cual confirmo el interés de China de robar tecnología y producirla a través de sus empresas.

---

[166] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (pp.61-62). España: Deusto S.A. Ediciones.

[167] Díez C, Perojo J, Penide J, Arias M. (mayo 19, 2011). *Ciber-terrorismo. Definición de políticas de seguridad para proteger infraestructuras críticas frente a ciber-ataques terroristas*. (p.18). enero 16, 2018, de Universidad Europea de Madrid Sitio web: http://mendillo.info/seguridad/tesis/Penide-Diez-Arias-Perojo.pdf.

[168] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (p.61). España: Deusto S.A. Ediciones.

Al ser Google una empresa que concentra un alto número de información de todo tipo se ha convertido en objetivo de constantes ciberataques, como ocurrió en 2009 ataques donde, además, de intereses económicos China perseguía intereses políticos que le permitieran mantener controlada la situación interna del país. "El objetivo de los ataques no era únicamente el de robar información a las grandes multinacionales para que las empresas chinas pudieran copiar y desarrollar su tecnología, sino que tenía también la intención de obtener los datos personales de millones de ciudadanos chinos para poder identificar y perseguir a opositores al régimen. Google confirmó el robo de propiedad intelectual de la empresa, así como la violación del acceso a algunas cuentas de correo electrónico de activistas de derechos humanos de China, motivo por el que decidió dejar de censurar los resultados de sus búsquedas en aquel país y trasladarse a Hong Kong, que no está sujeta a las leyes anticensura de China."[169]

En conclusión, la Operación Aurora evidencio como los gobiernos utilizan los medios informáticos para perseguir sus objetivos, tanto políticos como económicos, además, en el caso particular de China las declaraciones de Google muestran como el país utiliza dichas herramientas para mantener controlada a la población mediante la censura.

3.6.2. GRUPO SHAGHÁI; UNA BASE MILITAR PARA EL DOMINIO DE LA INFORMACIÓN.

En este apartado se expondrá la Unidad 61398 también conocida como Grupo Shanghái, base militar por la cual Estados Unidos relaciona los ataques recibidos en su contra con el gobierno chino. "La presentación a finales de 2013 del informe de la consultora de seguridad Mandiant, se exponía la actividad de la unidad 61398 del Ejército Popular de Liberación chino, se identificaba a algunos de sus integrantes, y se mostraban pruebas que permitían atribuirles la autoría de numerosos actos de ciberespionaje llevados a cabo desde 2006. El informe popularizó el concepto APT, Advanced Persistent Threat, como el conjunto de actividades y técnicas que permiten mantener una campaña de ciberespionaje de manera sigilosa y persistente. Además, revelaba la existencia de una estrategia militar global centrada en el concepto de guerra asimétrica, por el que China se planteaba en el escenario de un futuro enfrentamiento armado con EE.UU. impidiéndole utilizar su fuerza militar y provocándole un daño inhabilitante atacando sus infraestructuras críticas. El desarrollo de esta estrategia se

[169] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (p.62). España: Deusto S.A. Ediciones.

basa en zhinxinxiquan, el “dominio de la información”, y la Unidad 61398 sería la encargada de asumir esta función.”[170]

La estrategia china para el dominio de la información se basa en obtener información de otros gobiernos y empresas, además, busca restringir que entra y sale del país para tener el control sobre lo que los ciudadanos leen o saben, tal como lo muestra la Operación Aurora donde Google expreso las condiciones bajo cuales brindaba el servicio al gobierno chino. “Todo el tráfico que circula desde y hacia China es filtrado, y en su caso censurado, por el llamado Great FireWall (en referencia a la Gran Muralla, Great Wall en inglés y los dispositivos firewall de seguridad perimetral de redes). China puede de este modo dominar la información, siguiendo su política del zhixinxiquan, pero también se ha dotado de una poderosa arma de ciberdefensa, ya que es el único país del mundo que podría aislar completamente sus redes nacionales protegiéndolas ante un eventual estado de ciberguerra, manteniendo total o parcialmente su capacidad de respuesta.”[171]

La política zhixinxiquan, además, de ser una estrategia para obtener información de otras empresas y gobiernos sirve como un medio de control social para evitar movilizaciones en contra del régimen chino, en una crisis informática podría servir como una herramienta para evitar propagaciones de programas maliciosos.

De acuerdo a los reportes de Mandiant (empresa estadounidense de ciberseguridad) se detectó que los ciberataques contra Estados Unidos provenían de un edificio propiedad del Ejercito Popular chino, en dichos reportes también se dio a conocer los nombres de los militares a cargo de tal unidad, a quienes el gobierno estadounidense responsabilizó de la actividad informática que afectó al país. “Un informe de la empresa privada norteamericana Mandiant, publicado en febrero de 2013, identificó un edificio de las Fuerzas Armadas chinas en Shanghái de donde supuestamente partían decenas de ciberataques contra empresas de todo el mundo. A una unidad del inmueble se adscriben, según la acusación presentada por

[170] Alfonso J. (septiembre 2015). *Ciberguerra y ciberarmamento.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema Nacional de Seguridad. (p.102) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.

[171] Alfonso J. (septiembre 2015). *Ciberguerra y ciberarmamento.* En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema Nacional de Seguridad. (p.104) noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1

un tribunal federal de Pensilvania, Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu y Gu Chunhui, los cinco responsables del pirateo informático."[172]

"El gobierno de EE.UU. puso en la lista de los "más buscados" cinco oficiales del ejército chino, acusados de robo de secretos comerciales y el espionaje. Beijing responde con furia, convoca embajador de EE.UU. y se retirara de la mesa conjunta chino-estadounidense para la seguridad cibernética. Detrás del enfrentamiento, la batalla por la supremacía en Asia-Pacífico y el deseo de "redimensionar" las ambiciones chinas." [173]

Estados Unidos con las acusaciones en contra de los militares chinos también responsabilizo al gobierno de la actividad informática que perturbó al país en los últimos años, lo cual generó tensiones entre ambos países, similares a las de la guerra fría. "La Casa Blanca describió este martes los reiterados ataques cibernéticos, que una investigación reciente vincula directamente con una unidad secreta del Ejército chino, como "un serio desafío para la seguridad y la economía de Estados Unidos", lo que es la señal de que una nueva guerra fría, en el desconocido e incontrolable espacio de Internet, ha comenzado entre las dos grandes potencias que se disputan la supremacía en el siglo XXI."[174]

La idea de una nueva guerra fría surge a raíz de la actividad informática existente entre ambos países, además, de la carrera armamentista que ambos desarrollan en el ciberespacio, aunque no ha existido un enfrentamiento declarado.

En las investigaciones realizadas a los ciberataques en contra de Estados Unidos también se detectó la participación de universidades, que son financiadas por el gobierno como parte de su proyecto para formar un ciberejército, desarrollar tecnología e investigaciones sobre el ámbito digital. "La prensa estadounidense informa que, aunque la mayoría de los grupos investigados, como la unidad 61398, pertenecen al Ejército Popular de Liberación en China,

[172]Bassets M. (mayo 19, 2014). *Washington acusa a cinco militares chinos de ciberespionaje industrial*. noviembre 28, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html.

[173] Asianews.it. (mayo 20, 2014). *Bejin, tira y afloja con los Estados Unidos sobre el espionaje industrial y electrónico*. julio 2, 2019, de Asianews.it Sitio web: http://www.asianews.it/noticias-es/Beijing,-tira-y-afloja-con-los-Estados-Unidos-sobre-el-espionaje-industrial-y-electr%C3%B3nico-31123.html.

[174] Caño A. (febrero 19, 2013). *Estados Unidos y China. ante la primera ciberguerra fría*. diciembre 5, 2017, de El País Sitio web: https://elpais.com/internacional/2013/02/19/actualidad/1361300185_954734.html.

muchos piratas informáticos en la mira de Washington trabajan también para compañías privadas chinas o se desempeñan en universidades estatales, y son contratados ocasionalmente por departamentos gubernamentales."[175]

Una de las formas de prepararse en el ámbito digital tanto de Estados Unidos como de China, es el reclutamiento de jóvenes universitarios interesados en formar parte del ciberejército que ambos países desarrollan. "China ha comenzado a equiparse para futuras ciberamenazas y conflictos, y el gasto en ciberguerra ha pasado a representar una de sus partidas prioritarias. Además, el país se ha dotado de nuevas unidades militares destinadas a preparar ciberataques contra el enemigo que dependen de la sección del Ejército Popular de Liberación equivalente a la NSA. Se estima que esta división cuenta con unos 130.000 hombres. Por otro lado, se sabe de la existencia de cibercomandos chinos asimilables a los USCYBERCOM, que cuentan con al menos diez subdivisiones implicadas en el «diseño y desarrollo de redes de ordenadores para la defensa, el ataque y los sistemas de explotación»."[176]

El gobierno chino además ve en las universidades una fuente de investigaciones y desarrollo de tecnología, aspectos que son base en la estrategia de ciberseguridad que el país desarrolla. "China sigue determinada a hacer de la ciberguerra una de sus prioridades presupuestarias. Pekín considera que la inversión en investigación, desarrollo e innovación (I+D+i) aplicados al espionaje digital y la guerra en internet constituyen una estrategia crucial, y así lo ha hecho constar en su Plan Quinquenal 2011-2015."[177]

El grupo Shanghái no es la única base detectada que realiza actividad de ciberespionaje, sin embargo, de acuerdo a los reportes de Mandiant si es una de las unidades más activas en el espionaje informático. "Mandiant, compañía que el año pasado emitió un informe sobre las actividades de la unidad 61398 a la que denominó A.P.T.1, por ser el más prolífico de los 20 grupos de espionaje cibernético que identificó en China."[178]

En los últimos años la mayoría de las empresas e instituciones en Estados Unidos han resultado afectadas por el ciberespionaje emitido por el Ejército de Liberación Popular chino.

---

[175] BBC MUNDO. (mayo 20, 2014). *La unidad china 61398, el nuevo enemigo número uno de EE.UU*. diciembre 1, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2014/05/140520_tecnologia_hackers_china_unidad_61398_mz.

[176] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p.181). España: Deusto S.A. Ediciones.

[177] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (pp.181-182). España: Deusto S.A. Ediciones.

[178] BBC MUNDO. (mayo 20, 2014). *La unidad china 61398, el nuevo enemigo número uno de EE.UU*. diciembre 1, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2014/05/140520_tecnologia_hackers_china_unidad_61398_mz.

“La compañía de seguridad Mandiant, situada en las afueras de Washington, que asegura que en los últimos seis años más de 140 empresas y organizaciones, casi todas de EE UU, han sido invadidas desde Internet por la Unidad 61398 del Ejército de Liberación Popular chino.”[179]

La pérdida de información confidencial y estratégica es consecuencia de la oleada de ciberataques que reciben las empresas e instituciones estadounidenses, información a través de la cual China favorece su gobierno y empresas. “Según los investigadores del Departamento de Estado, los oficiales robaron secretos comerciales y documentos internacionales de cinco compañías y un sindicato. "Nosotros afirmamos que miembros de la unidad 61398 conspiraron para ingresar ilegalmente en computadoras de seis víctimas en Estados Unidos para robar información beneficiosa para los competidores de esas víctimas, incluyendo empresas públicas chinas", dijo John Carling, asistente del fiscal general para la Seguridad Nacional.”[180]

En resumen, el Grupo Shanghái expone la relevancia del ámbito digital para el gobierno chino, quien utiliza la tecnología para distintos fines que van desde intereses económicos hasta políticos, además, la unidad 61398 también es ejemplo de la carrera armamentista digital en la que invierten los gobiernos actualmente.

[179] Caño A. (febrero 19, 2013). *Estados Unidos y China. ante la primera ciberguerra fría*. diciembre 5, 2017, de El País Sitio web: https://elpais.com/internacional/2013/02/19/actualidad/1361300185_954734.html.

[180] BBC MUNDO. (mayo 20, 2014). *La unidad china 61398, el nuevo enemigo número uno de EE.UU*. diciembre 1, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2014/05/140520_tecnologia_hackers_china_unidad_61398_mz.

4. LA RESPUESTA DE ESTADOS UNIDOS ANTE EL TERRORISMO DESPUÉS DEL 11S.

Como es sabido el terrorismo es uno de los fenómenos que ha marcado la historia de Estados Unidos y su dirección en materia de seguridad nacional, por ello en este apartado se plantearan algunas de las acciones implementadas por el país para mitigarlo y prevenirlo posterior a los atentados del 11 de septiembre de 2001. Dan Verton señala que; "Después de los ataques terroristas del 11 de septiembre de 2001 y desde que América comprendiera que la gente que intenta matarlos ha vivido en su país durante años, el Gobierno ha cambiado su centro de atención hacia la creación, como describió Barr, de "una estructura legal explícita y desarrollada" para mejorar la flexibilidad de las agencias de aplicación de la ley y de las agencias de inteligencia en su batalla diaria contra el terrorismo."[181]

La aprobación del Acta Patriota es una de las primeras acciones del gobierno estadounidense a consecuencia de los atentados de 2001, en dicho documento se plantea la necesidad de proteger el ciberespacio. "El gobierno de EEUU aprobó la ley "Patriot Act" en octubre 2001 y Reino Unido la ley "Anti-Terrorism Act" en diciembre de 2005 las cuales daban más poder a las fuerzas de seguridad para vigilar las comunicaciones electrónicas."[182]

El nacionalismo es considerado un elemento clave del gobierno para lograr la participación de las empresas en temas que representan una amenaza para el país. Además, la Acta Patriótica permitió al gobierno iniciar un proyecto de vigilancia masiva en el país, y se comprometía a las empresas a colaborar con el gobierno en materia de Seguridad Nacional. "Si el patriotismo y el dinero no son suficientes para promover la colaboración de las empresas estadounidenses, el Gobierno del país dispone de la Ley Patriótica, que fue aprobada tras los atentados del 11 de septiembre de 2001, y que amplió los poderes de vigilancia contra los delitos de terrorismo. Amparado en esta ley, el Gobierno de Estados Unidos ha ejercido un espionaje masivo, tanto sobre extranjeros como sobre sus propios ciudadanos."[183]

Como se ha mencionado la economía es un pilar de Seguridad Nacional por ello el valor de la participación de las empresas con el gobierno para mantener la estabilidad nacional. Además, estas cuentan con información y tecnología útil para el gobierno. "En Estados Unidos, el patriotismo se vive de forma distinta (y, a menudo, más intensa) que, en Europa, por lo que no

---

[181] Verton D. (2004). *Juego de patriotas: Seguridad, Terror, Libertad*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.235). Madrid: McGraw-Hill.

[182] Díez C, Perojo J, Penide J, Arias M. (mayo 19, 2011). *Ciber-terrorismo. Definición de políticas de seguridad para proteger infraestructuras críticas frente a ciber-ataques terroristas*. (p.35). enero 16, 2018, de Universidad Europea de Madrid Sitio web: http://mendillo.info/seguridad/tesis/Penide-Diez-Arias-Perojo.pdf.

[183] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (p.82). España: Deusto S.A. Ediciones.

es de extrañar que muchas empresas norteamericanas colaboren de buen grado con su Gobierno e identifiquen los intereses económicos de Estados Unidos con cuestiones de seguridad nacional. Esto hace que, frecuentemente, las compañías estadounidenses se comporten como verdaderos apéndices de la política de la Casa Blanca, hasta el punto de que los propios trabajadores de estas compañías son incapaces de discernir si están trabajando para su empresa o para el Gobierno."[184]

El Acta Patriótica establece los poderes necesarios que requieren las agencias de inteligencia para agilizar los procesos de investigación ante casos de posibles actos de terrorismo como señala el autor Dan Verton; "La USA Patriot Act proporcionó al FBI y a otros brazos del Departamento de Justicia la capacidad de obtener órdenes judiciales para interceptar comunicaciones referentes a actividades terroristas sospechosas, bien estén relacionadas con ataques planeados o con la financiación o apoyo de redes terroristas. El proyecto amplió de forma drástica la capacidad de realizar escuchas telefónicas del FBI permitiendo a los investigadores escuchar múltiples teléfonos fijos y móviles de los posibles terroristas. Antes del proyecto de ley, el FBI necesitaba conseguir una orden judicial para cada teléfono que deseaba intervenir, lo que provocaba importantes problemas a los investigadores que intentaban vigilar a los terroristas cuyas comunicaciones giraban en torno a múltiples teléfonos móviles y un número altísimo de cuentas de Internet."[185]

La vigilancia masiva permite a las agencias monitorear llamadas telefónicas, conversaciones y búsquedas realizadas en internet, tanto de ciudadanos nacionales como extranjeros porque después de los acontecimientos del septiembre de 2001 todos los usuarios de Internet representan una posible amenaza para el país.

Además, del Acta Patriótica el gobierno de Estados Unidos implemento otras tres medidas en su lucha contra el terrorismo, las cuales se plantean a continuación; "EE.UU. ha desarrollado diversos planes y capacidades relacionadas con la ciberdefensa tanto en el ámbito civil, como en el ámbito militar. EE.UU. dispone de tres estrategias relacionadas con la seguridad nacional que son las siguientes:

- Estrategia de Seguridad Nacional ("National Security Strategy") del año 2002, actualizada en el 2006.
- Estrategia Nacional para Combatir el Terrorismo ("National Strategy for Combating Terrorism") del año 2006.

[184] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (p.80). España: Deusto S.A. Ediciones.

[185] Verton D. (2004). *Juego de patriotas: Seguridad, Terror, Libertad*. En Black Ice: Una amenaza invisible del ciberterrorismo (pp.235-236). Madrid: McGraw-Hill.

- Estrategia para la Seguridad del Territorio Nacional ("National Strategy for Homeland Security") del año 2002 y actualizada en el 2007. Del conjunto de estrategias, destaca por sus referencias a la Ciberdefensa la "Estrategia

para la Seguridad del Territorio Nacional", que es complementaria a las otras dos, y cuyo propósito es movilizar y organizar a la nación para asegurarla frente a los ataques terroristas."[186]

Parte de la respuesta del gobierno estadounidense contra el terrorismo es invertir en programas de criptografía con el fin de proteger sus comunicaciones e información. "El uso cotidiano de herramientas tan diversas para espiar orilló a los EUA a desarrollar sistemas de criptología sofisticados, a fin de garantizar la seguridad de sus comunicaciones. Como muestra de la importancia que para los estadounidenses significaba contar con un sistema criptográfico fuerte que resista los ataques de los criptoanalistas del enemigo, se muestra la siguiente gráfica (p.107), con el presupuesto asignado por el gobierno de los EUA en el 2013 al programa de criptología." [187]

FIGURA 5.1. PORCENTAJE DE FONDOS EMPLEADOS POR LA NSA PARA EL PROGRAMA DE CRIPTOLOGÍA

FUENTE: <http://goo.gl/eDzKep>, consultado el 21 de enero de 2014.

La criptografía también se utiliza como un medio de espionaje en contra de otros actores para obtener información estratégica. "Es claro que la criptología es un instrumento importante para

[186] Pastor O, Pérez J, Arnáiz D, Taboso P. (octubre 2009). *Seguridad Nacional y Ciberdefensa*. (p. 58) noviembre 3, 2017, de ISDEFE Sitio web: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

[187] Arreola A. (2015). *La edificación del sistema de inteligencia de los Estados Unidos de América*. En Ciberespionaje: La puerta al mundo virtual de los Estados e individuos. Una revisión de los programas de espionaje digital de los Estados Unidos (p.106). México: Siglo XXI editores.

la seguridad, así como un arma que utiliza el gobierno estadounidense para descifrar los secretos más importantes del mundo."[188]

En conclusión, la respuesta de Estados Unidos contra el terrorismo se basó en invertir en programas para proteger su información, además, del otorgamiento de mayores poderes a sus agencias de inteligencia con el fin de detectar cualquier actividad anormal que pusiera en peligro al país.

4.1. ¿CÓMO MITIGA EL CIBERTERRORISMO EL GOBIERNO ESTADOUNIDENSE?

De igual manera como ocurrió con el terrorismo, con el ciberterrorismo también se comenzaron a tomar medidas para prevenir y mitigar sus efectos, debido a que posterior a los acontecimientos del 11S se observó el peligro del ciberespacio, sin embargo, existen acontecimientos decisivos en el tema de la ciberseguridad como la Operación Buckshot Yankee.

El peligro y relevancia del ciberespacio en la sociedad comenzó a contemplarse incluso antes de lo acontecido en 2001, sin embargo, no se tenía un conocimiento profundo sobre el tema y el reto que representaría para la seguridad del país. "En enero de 2000, la administración Clinton público el primer "Plan Nacional" para defender el ciberespacio. En realidad, sin embargo, el plan era un típico "mapa de ruta" gubernamental que describía un mundo perfecto en el futuro, pero no indicaba nada que ayudara a hacerlo realidad."[189]

Como se mencionó en otro apartado en 2008 Estados Unidos se vio involucrado en el acontecimiento que culminó con la operación Buckshot Yankee, la cual se considera un acto decisivo en el tema de ciberseguridad del país, con ello surgieron iniciativas como la siguiente; "La Casa Blanca a crear en 2008 la Iniciativa Integral de Ciberseguridad Nacional (CNCI). 4 entre sus atribuciones se encuentran:

- La gestión de las redes del gobierno de manera unificada mediante el programa "Trusted Internet Connections".
- La puesta en marcha de sistemas de detección y prevención de intrusiones en todo el gobierno.
- La coordinación de los esfuerzos en I+D.
- La conexión de los centros federales de operaciones cibernéticas.
- El desarrollo y la aplicación de un plan de contrainteligencia cibernética que abarque a todo el gobierno.

[188] Arreola A. (2015). *La edificación del sistema de inteligencia de los Estados Unidos de América*. En Ciberespionaje: La puerta al mundo virtual de los Estados e individuos. Una revisión de los programas de espionaje digital de los Estados Unidos (p.106). México: Siglo XXI editores.

[189] Verton D. (2004). *Terror en la red: Internet como arma*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.40). Madrid: McGraw-Hill.

• El aumento de la seguridad de las redes confidenciales.
• La expansión de la educación cibernética.
• El desarrollo de estrategias y programas de disuasión.
• La gestión de riesgos de la cadena de suministro.
• La definición del papel del Gobierno federal en materia de ciberseguridad de las infraestructuras críticas."[190]

La iniciativa en ciberseguridad propuesta en 2008, se retomó por el presidente Barack Obama quien realizó nuevas recomendaciones con el fin de poner en práctica dicho Plan de Acción y tener un ciberespacio seguro. "Poco después de asumir el cargo en 2009, el presidente Obama ordenó una revisión de las iniciativas federales, como la CNCI, y pidió al Consejo de Seguridad Nacional que desarrollara un enfoque global sobre ciberseguridad. La Revisión de la Política Cibernética resultante recomendó la adopción de varias medidas:

• Crear un puesto de coordinador de ciberseguridad.
• Trabajar con las administraciones estatales y locales y con el sector privado para ofrecer una respuesta unificada a futuros incidentes cibernéticos.
• Fortalecer las alianzas público-privadas.
• Invertir en una I+D de punta.
• Iniciar una campaña para promover la sensibilización sobre la ciberseguridad y la formación de mano de obra digital." [191]

Además, las recomendaciones propuestas por Obama se caracterizaron por plantear la creación de puestos especializados en la materia, dando como resultado la creación del puesto de Coordinador de Ciberseguridad de la Casa Blanca. "El Coordinador de Ciberseguridad de la Casa Blanca —un puesto creado tras la Revisión de la Política Cibernética de 2009— dirige el desarrollo interinstitucional de la estrategia y la política nacional de ciberseguridad, y supervisa a los organismos en la aplicación de dichas políticas." [192]

---

[190] Andrew J. (julio 2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. (p.48). marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.

[191] Andrew J. (julio 2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. (pp.48-49). marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.

[192] Andrew J. (julio 2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. (p.54). marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.

Como se mencionó la participación de las empresas es un elemento clave en el tema de seguridad nacional desde lo acontecido en 2001, por esa razón desde entonces el gobierno considera importante la colaboración de las empresas en sus iniciativas de leyes, como en el caso de la Ley de Protección y Uso Compartido de Ciberinteligencia (CISPA por sus siglas en inglés), donde se plantea la colaboración de las empresas con el gobierno para vigilar las comunicaciones a través de Internet. "La Cyber Intelligence Sharing and Protection Act (CISPA), algo así como una Ley de Protección y Uso Compartido de Ciberinteligencia. La nueva norma permitirá extender la capacidad del Gobierno para vigilar las comunicaciones en internet, tanto a través de sus agencias como gracias a la colaboración activa con las empresas nacionales. La medida ha sido justificada por la necesidad de reforzar la seguridad nacional frente a ciberamenazas."[193]

En 2015 se aprobó el Plan de Acción Nacional de Ciberseguridad en cual se establecen las necesidades del país para el ámbito digital, donde se destaca la necesidad por proteger ciertos sectores fundamentales para la estabilidad del país. "Como se establece en el Plan de Acción Nacional de Ciberseguridad, la política de ciberseguridad en EE.UU. se basa en tres pilares estratégicos: elevar el nivel de ciberseguridad en los sectores público, privado y consumidores; adoptar medidas para prevenir, disuadir, desarticular e interferir con la actividad maliciosa en el ciberespacio contra los Estados Unidos o sus aliados y responder con eficacia y recuperarse de los ciberincidentes. El Plan de Acción Nacional de Ciberseguridad, aprobado por el presidente estadounidense y anunciado en Febrero de este año, el cual contiene una serie de acciones dirigidas a aumentar la protección y la concienciación en ciberseguridad, proteger la privacidad, mantener la seguridad pública, económica y nacional, así como capacitar a los estadounidenses a tener un mejor control de su seguridad digital."[194]

Dentro del Plan de Acción Nacional de Ciberseguridad también se contemplaron acciones como la inversión en tecnología y el aumento de presupuesto con la finalidad de garantizar la seguridad informática, además, se creó el puesto de Director de Seguridad de la Información entre otros puntos que a continuación se mencionaran; "Los puntos destacados del CNAP incluyen acciones para:

- Establecer la "Comisión para mejorar la seguridad cibernética nacional" … La Comisión hará recomendaciones sobre las medidas que se pueden tomar durante la próxima década para fortalecer la

[193] Suárez A. (2015). *Ciberterrorismo*. En El Quinto Elemento (p.138). España: Deusto S.A. Ediciones.

[194] Departamento de Seguridad Nacional. (agosto 12, 2019). *Directiva de los Estados Unidos para la coordinación de ciberincidentes*. septiembre 10, 2019, de DSN Sitio web: http://www.dsn.gob.es/es/actualidad/sala-prensa/directiva-estados-unidos-para-coordinacion-ciberincidentes.

ciberseguridad tanto en el sector público como en el privado al tiempo que se protege la privacidad; mantener la seguridad pública y la seguridad económica y nacional; fomentar el descubrimiento y el desarrollo de nuevas soluciones técnicas; y reforzar las asociaciones entre el gobierno federal, estatal y local y el sector privado en el desarrollo, promoción y uso de tecnologías, políticas y mejores prácticas de ciberseguridad.

- Modernice la TI gubernamental y transforme la forma en que el gobierno gestiona la ciberseguridad mediante la propuesta de un fondo de modernización de la tecnología de la información de $ 3,100 millones …así como la formación de un nuevo puesto, el Director de Seguridad de la Información del Director Federal.
- Permita a los estadounidenses asegurar sus cuentas en línea yendo más allá de las contraseñas y agregando una capa adicional de seguridad.
- Invierte más de $ 19 mil millones en seguridad cibernética como parte del Presupuesto del año fiscal del presidente (FY) 2017."[195]

Las estrategias de Estados Unidos desde el 11 de septiembre de 2001 se caracterizaron por designar importantes sumas al presupuesto destinado a la seguridad nacional, y en el caso de la ciberseguridad no es una excepción. Dentro del presupuesto se contempló invertir en la educación y capacitación de la población en la materia a fin de reducir el número de infecciones por malware. "El gobierno federal, a través de iniciativas tales como la Iniciativa Nacional para la Educación Cibernética, mejorará la educación y capacitación en seguridad cibernética en todo el país y contratará a más expertos en ciberseguridad para asegurar las agencias federales. Como parte del CNAP, el Presupuesto del presidente invierte $ 62 millones en personal de ciberseguridad."[196]

El ciberterrorismo ha originado el potencial negocio de la ciberseguridad, dado que las instituciones de gobierno no son las únicas preocupadas y ocupadas en proteger el ciberespacio, actualmente las empresas también brindan servicios de seguridad informática. "Estados Unidos cuenta con un gran mercado en crecimiento en términos de tecnología de la seguridad cibernética. Los seguros cibernéticos también están ganando popularidad para poder proteger financieramente a las compañías estadounidenses en caso de incidentes." [197]

---

[195] Oficina del Secretario de Prensa. (febrero 9, 2016). *Plan de Acción Nacional de Ciberseguridad*. septiembre 10, 2019, de La Casa Blanca Sitio web: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[196] Oficina del Secretario de Prensa. (febrero 9, 2016). *Plan de Acción Nacional de Ciberseguridad*. septiembre 10, 2019, de La Casa Blanca Sitio web: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

[197] Andrew J. (julio 2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. (p.57). marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.

El crecimiento del negocio de la ciberseguridad, ha originado el interés del gobierno y empresarios de invertir en la creación de nuevas empresas especializadas en el tema, lo que contribuye en el posicionamiento de Estados Unidos como líder en el desarrollo de tecnología en ciberseguridad. “Estados Unidos es un país líder en tecnología y ciberseguridad de la información. La ciberseguridad se ha convertido en una prioridad de inversión tanto para el gobierno como para el sector privado. El pasado año, empresas de capital de riesgo invirtieron más de US$1.000 millones en startups de ciberseguridad. Diecisiete empresas de capital de riesgo de Silicon Valley se centran en el desarrollo de tecnologías innovadoras de ciberseguridad, y el año pasado invirtieron en más de 230 startups de ciberseguridad.” [198]

El gobierno de Estados Unidos invierte en la creación del ejercito informático como parte de los proyectos que forman la estrategia para contrarrestar los efectos del ciberterrorismo. “Los USCYBERCOM han experimentado un crecimiento muy rápido dentro del ejército de Estados Unidos, tanto en lo que se refiere a su tamaño como por lo que respecta a su peso específico. Basta señalar que, en 2014, el Gobierno estadounidense dobló el presupuesto destinado a estos cibercomandos, mientras recortaba todas las demás partidas del gasto militar.”[199]

En resumen, el gobierno estadounidense ha basado su estrategia de ciberseguridad en la inversión de tecnología y el desarrollo de proyectos especializados en el tema para atender las necesidades del fenómeno digital, la estrategia del gobierno también se basa en establecer alianzas con el sector privado, quien es fundamental en sus estrategias. Además, de las empresas algunas agencias de inteligencia también participan en la estrategia del gobierno contra el ciberterrorismo.

4.2. PLANES, PROYECTOS Y ACCIONES DE LA INTELIGENCIA ESTADOUNIDENSE CONTRA EL CIBERTERRORISMO.

Como se mencionó algunas agencias de inteligencia también forman parte de las estrategias del gobierno de los Estados Unidos para disuadir los efectos del ciberterrorismo y en este apartado se expondrán algunos de los planes, proyectos y acciones que dichas agencias han tenido.

[198] Andrew J. (julio 2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. (p.55). marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.

[199] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p.117). España: Deusto S.A. Ediciones.

En este apartado se plantearán las agencias que actualmente colaboran en materia de ciberseguridad, algunas de ellas ya establecidas incluso antes de los acontecimientos del 11S y otras que surgen como consecuencia del ciberterrorismo. El autor James Andrew destaca las siguientes; “La responsabilidad de la ciberseguridad la comparten diversos organismos, cada uno con su propio conjunto de responsabilidades y atribuciones. Los más importantes son el Departamento de Seguridad Nacional (DHS), el Departamento de Justicia y la Oficina Federal de Investigación (FBI), y los Departamentos de Estado y Defensa.”[200]

En una crisis informática las agencias de inteligencia deben seguir un protocolo de acción para evitar se afecten otros sistemas para lograr esto, además, de las líneas de acción las agencias deben actuar de manera conjunta y no independiente como se actuaba con el terrorismo o crímenes tradicionales. “Las agencias federales deben emprender tres líneas simultáneas de esfuerzo: respuesta a la amenaza; respuesta de activos; y apoyo de inteligencia y actividades relacionadas. Además, cuando una agencia federal es una entidad afectada, debe emprender una cuarta línea simultánea de esfuerzo para administrar los efectos del incidente cibernético en sus operaciones, clientes y fuerza de trabajo.”[201]

En resumen, la inteligencia de Estados Unidos es el medio a través del cual el gobierno efectúa las acciones para prevenir acontecimientos informáticos y las cuales han tenido que adaptarse a las necesidades del ciberespacio, situación que ha provocado el surgimiento de nuevas agencias y puestos especializados en el tema.

4.2.1. LA NSA Y SU LÍNEA DE ACCIÓN CONTRA EL CIBERTERRORISMO.

Dentro de la lista de agencias que colaboran con el gobierno actualmente en los proyectos contra el ciberterrorismo se encuentra la Agencia de Seguridad Nacional (NSA por sus siglas en inglés).

Como ya se planteó el sector privado, tiene una participación relevante con el gobierno y por lo tanto la inteligencia del país, donde su colaboración se caracteriza por aportar información

[200]Andrew J. (julio 2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. (p.55). marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.

[201]Oficina del Secretario de Prensa. (julio 26, 2016). *Directiva de política presidencial - Coordinación de incidentes cibernéticos de Estados Unidos*. enero 10, 2018, de La Casa Blanca Sitio web: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

confidencial de otras empresas, gobiernos y en general de los usuarios de Internet. “En la mayoría de los casos, las multinacionales colaboran de buen grado con la NSA, facilitándole un acceso permanente y sin autorización previa a toda la información privada almacenada en sus servidores. Además, según desveló el diario The Guardian, la NSA paga millones de dólares a las multinacionales tecnológicas para asegurarse su complicidad en el proceso de vigilancia.”[202]

La Agencia de Seguridad Nacional ha desarrollado un programa de vigilancia masiva como parte de sus proyectos para prevenir incidentes tanto en el terreno físico como en el digital, en dicho proyecto colaboran empresas como Microsoft, quien brinda acceso a las cuentas de correo de sus usuarios a través de las cuales el gobierno obtiene información. “La realidad es que desde que Microsoft adquirió Skype, la compañía de Bill Gates ha estado ayudando a la NSA para que las comunicaciones de los usuarios sean interceptadas por el sistema de vigilancia PRIMS ... Microsoft colaboró con la agencia de seguridad estadounidense para que el Gobierno pudiera eludir el sistema de encriptado que protege las conversaciones entre usuarios de su mensajería electrónica Outlook.” [203]

Microsoft, además de proporcionar a la NSA acceso a cuentas de correo de Outlook, también se le ha relacionado con casos como el de Stuxnet donde se plantea, la empresa proporciono al gobierno las claves de los días cero del sistema que controlaba la planta nuclear de Natanz para que este pudiera acceder.

Estados Unidos al igual que China mantiene sus proyectos de dominio de la información como es el caso de PRIMS de la Agencia de Seguridad Nacional, donde participan principalmente empresas de servicios de comunicación a través de Internet. “PRIMS Es un programa clandestino que busca apoderarse de toda la información guardada y enviada a través de dispositivos digitales, lo que se llama en argot informático data mining (minado de datos). Fue lanzado en 2007 por la National Security Agency de los EUA y los Goverment Communications HeadQuarters (GCHQ) de la Gran Bretaña. De hecho, el nombre código Prims hace referencia al esfuerzo gubernamental de recolección de información denominado SIGAD (SIGINT Activity Designator) US-984XN que se refiere a la recolección de comunicaciones a través de Internet por medio de las peticiones de información que se realizan a compañías como Google, Yahoo, Apple, Microsoft, Skype, YouTube, AOL, etcétera. Estas peticiones son con base en los lineamientos establecidos en la sección 702 de la Ley de Vigilancia de la Internet Extranjera

[202] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (p.81). España: Deusto S.A. Ediciones.
[203] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (pp.80-81). España: Deusto S.A. Ediciones.

(FISA, por sus siglas en inglés) y acuerdos secretos con dichas compañías, a las que se le ofrece inmunidad a cambio de su cooperación." [204]

La campaña de vigilancia masiva tanto del gobierno como de las agencias se ha favorecido debido al flujo de información que percibe el país, y por sus leyes que permiten inspeccionar dicha información mientras se encuentre en territorio estadounidense. "El programa Prims (The Guardian, 2013) toma ventaja de que gran parte del flujo de comunicaciones globales pasa por territorio estadounidense y que, al encontrarse temporalmente bajo la jurisdicción del gobierno de los EUA, este simple hecho le permite interceptar la información con un supuesto apego a la ley."[205]

Dentro de las funciones de la inteligencia del país se encuentra el analizar la información que fluye en la red, con el fin de detectar irregularidades o posibles amenazas que pongan en riesgo a la nación, para ello la NSA ha implementado el siguiente programa;

"PINWALE (GREENWALD, 2013; RISEN Y LICHTBLAU,2009)
Es la principal base de datos utilizada para analizar las actividades de Internet. Es un nombre clave asignado por la NSA a un sistema de colección y obtención de inteligencia digital de la red (Digital Network Intelligence). En el presente, el programa Pinwale ha incorporado información de diversos medios de comunicación digital. Y requiere de una orden judicial para realizar la búsqueda y recolección. También ofrece a las compañías con las cuales trabaja inmunidad en caso de verse inmiscuidas en reclamos legales."[206]

El gobierno ofrece a las empresas inmunidad a cambio de proporcionar información a la inteligencia del país, sin embargo, también facilita a las agencias las ordenes necesarias para solicitar información a las empresas y estas estén obligadas a brindárselas, a través de un tribunal especial. "En realidad, conseguir una orden judicial no es muy complicado para la NSA, que puede obtenerla rápidamente a través de un tribunal secreto llamado Foreign Intelligence Surveillance Court (FISC), algo así como Tribunal de Vigilancia de Inteligencia Extranjera … De las 1.800 órdenes de investigación que el FBI y la NSA solicitaron en 2012, el 98,9 por ciento fueron aprobadas por ese tribunal. ¡Qué efectividad, chicos! Y, una vez se han hecho

[204] Arreola A. (2015). *La edificación del sistema de inteligencia de los Estados Unidos de América*. En Ciberespionaje: La puerta al mundo virtual de los Estados e individuos. Una revisión de los programas de espionaje digital de los Estados Unidos (p.116). México: Siglo XXI editores.
[205] Arreola A. (2015). *Programas de los EUA para el espionaje cibernético*. En Ciberespionaje: La puerta al mundo virtual de los Estados e individuos. Una revisión de los programas de espionaje digital (p.117). México: Siglo XXI editores.
[206] Arreola A. (2015). *Programas de los EUA para el espionaje cibernético*. En Ciberespionaje: La puerta al mundo virtual de los Estados e individuos. Una revisión de los programas de espionaje digital (p.131). México: Siglo XXI editores.

con la orden judicial, las empresas están obligadas por ley a suministrar al Gobierno la información que solicite."[207]

El ciberterrorismo demanda una respuesta uniforme del gobierno, para ello las agencias se han tenido que adaptar y trabajar de manera conjunta, sin importar la autonomía con la que cuentan, en ese sentido la NSA desarrolló "El Programa de transferencia de tecnología (TTP) de la NSA transfiere la tecnología desarrollada por la NSA a la industria, la academia y otras organizaciones de investigación, lo que beneficia a la economía y la misión de la Agencia. El programa cuenta con una amplia cartera de tecnologías patentadas en múltiples áreas tecnológicas." [208]

La educación y el desarrollo de tecnología en materia digital son fundamentales para, entender el fenómeno y contar con las herramientas necesarias para dar una respuesta acorde a las necesidades de este. Es por eso que los gobiernos establecen alianzas con universidades para capacitar a los jóvenes y tener acceso a capital humano especializado en la materia, dicho lo anterior: "La Dirección de Investigación de la Agencia de Seguridad Nacional patrocina la Iniciativa de la Ciencia de la Seguridad para promover la ciencia fundacional de la seguridad cibernética que se necesita para madurar la disciplina de la seguridad cibernética y para apuntalar los avances en defensa cibernética. La iniciativa SoS funciona de varias maneras. 1. Involucrar a la comunidad académica para la investigación fundacional, 2. Promover principios científicos rigurosos, y 3. hacer crecer la comunidad SoS."[209]

Los programas de reclutamiento para universitarios proporcionar mano de obra en ciberseguridad y es el paso que el gobierno e instituciones dan para la formación del ciberejército, en el que actualmente varios países invierten. "La Agencia Nacional de Seguridad (NSA) y el DHS han construido una red de Centros Nacionales de Excelencia Académica en las áreas de defensa cibernética y de operaciones cibernéticas, con universidades de todo el país. Bajo los auspicios de la Iniciativa Nacional para la Educación sobre Ciberseguridad (NICE), estos programas buscan solventar la escasez de personal con conocimientos de

[207] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (p.85). España: Deusto S.A. Ediciones.
[208] NSA|CSS. (s/a). *Oficina de investigación y aplicaciones tecnológicas de la NSA*. julio 19, 2019, de NSA Sitio web: https://www.nsa.gov/what-we-do/research/technology-transfer/.
[209] SOS. *Objetivos de la organización virtual de ciencias de la seguridad*. julio 19, 2019, de SOS Sitio web: https://cps-vo.org/group/SoS/about.

ciberseguridad. La NICE se ocupa de la educación y el desarrollo de mano de obra para la ciberseguridad."[210]

En síntesis, la Agencia de Seguridad Nacional ha mostrado conciencia en las necesidades del ciberterrorismo con los programas que hasta ahora ha desarrollado para dar respuesta a dicha amenaza, al colaborar con otras agencias y empresas con quienes comparten información y tecnología.

4.2.2. EL FBI; UN ORGANISMO LÍDER EN LA INVESTIGACIÓN DE LOS CIBERDELITOS.

El Buró Federal de Investigaciones (FBI) se caracteriza por ser una de las principales agencias en investigación criminal del Departamento de Defensa de los Estados Unidos, asimismo, figura entre las agencias que hoy en día trabajan para dar una respuesta a las amenazas informáticas. "El FBI es el organismo líder en la investigación de los delitos informáticos (el Servicio Secreto, vinculado al DHS, investiga también los delitos informáticos financieros). Tanto el FBI como la Agencia Nacional de Seguridad (que forma parte del Departamento de Defensa) apoyan al DHS en su misión de cuidar de la ciberseguridad nacional."[211]

El Buró Federal de Investigación basa sus estrategias en el desarrollo de programas de vigilancia de comunicaciones, con la finalidad de identificar o rastrear a aquellos individuos o grupos que representen un peligro para el país. "El FBI anunció a finales de la década pasada que había desarrollado un programa especial de vigilancia informática llamado 'Carnivore' que le permitía leer mensajes electrónicos y otras comunicaciones entre presuntos criminales, espías y terroristas, y que según aseguraba era mucho mejor que los productos comerciales."[212]

---

[210] Andrew J. (julio 2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. (pp.50-51). marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.

[211] Andrew J. (julio 2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. (p.55). marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.

[212] El País. (enero 19, 2005). *El FBI retira "Carnivore", su programa para espiar en internet*. enero 5, 2018, de El País Sitio web: https://elpais.com/tecnologia/2005/01/19/actualidad/1106126878_850215.html.

“Carnivore” es uno de los programas desarrollado por el FBI para analizar la información que fluye en la red y detectar aquellas palabras, frases o búsquedas que pudieran tener relación con grupos criminales o planes de ataques terroristas. “El programa informático “Carnívoro” es en realidad un paquete de programas muy sofisticados desarrollados por expertos del FBI como continuación de un proyecto anterior llamado “Omnívoro” que se implementó a me8diados de la década de los noventa. Actualmente se denomina “SCD1000” o “Sistema de Colección Digital 1000”, siendo uno de los primeros programas de vigilancia en ser usados por agencias de seguridad para rastrear actividad sospechosa en Internet y aunque no necesita una orden judicial sí selecciona lo que considera sospechoso en base a criterios judiciales.”[213]

Por ejemplo; buscar como elaborar una bomba en Internet, puede provocar que agencias como el FBI pongan atención a las conversaciones y búsquedas de la dirección IP de donde se emitió esa señal. “Carnívoro es un programa especializado que se instala en la; red de un proveedor de acceso a Internet. Luego, el FBI lleva; una computadora a la oficina de ese servidor, la conecta a la; PC del proveedor, y hace un "download" (una copia) de todo lo; que se encuentra allí guardado. Al entrar en funcionamiento, "Carnívoro" revisa todos los; correos que entran y salen de la dirección del blanco que; investiga, además de rastrear las visitas que hace a sitios de; la Red y las sesiones de chat en las que participa. El sistema actúa en tiempo real y no deja señal ni rastro que; permita delatar su uso. Con la existencia del software ningún; usuario puede darse cuenta de que está siendo vigilado.”[214]

Como se mencionó el programa Carnivore no requiere de una orden judicial para interferir comunicaciones, es decir, el Buró Federal de Investigaciones puede revisar la información de los usuarios de la red sin su consentimiento, situación que representa una violación a los Derechos Humanos de dichos usuarios.

Además, el Buró Federal de Investigación (FBI) invierte en sistemas para ampliar sus capacidades de rastreo, incluso en niveles de la red donde existen mayores candados que protegen la identidad de los usuarios, situación que es aprovechada por criminales para realizar actos ilícitos de manera segura y con menores riesgos de ser identificados. “El FBI utilizaba el software de los italianos para desenmascarar a usuarios que usan la red TOR.

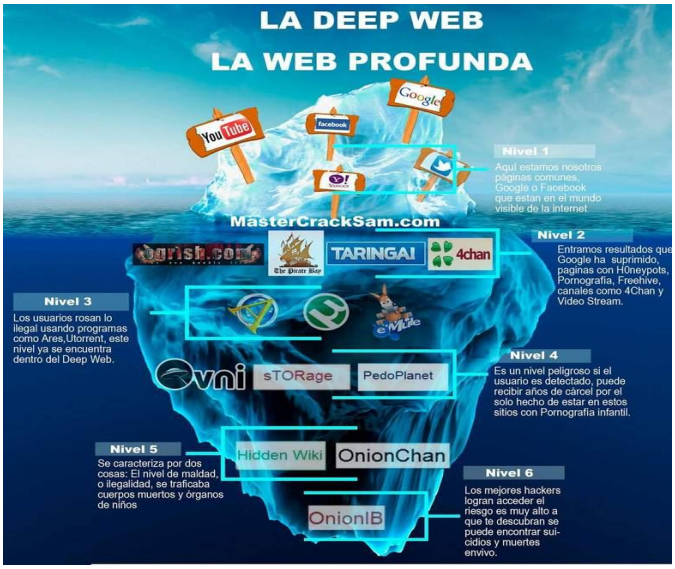
---

[213] Red Safe World. (marzo 22, 2011). *La lucha contra el ciberterrorismo*. enero 5, 2018, de Red Safe World Sitio web: https://redsafeworld.wordpress.com/2011/03/22/la-lucha-contra-el-ciberterrorismo/.

[214] Gómez O. (julio 14, 2003). *Estudian respaldo a "Plan Carnivóro"*. enero 9, 2018, de El Nuevo Diario Sitio web: http://archivo.elnuevodiario.com.ni/nacional/114569-estudian-respaldo-plan-carnivoro/.

Primero los infectaba, y luego revelaba su IP real cuando estuvieran usando TOR. El FBI gastó hasta 775.000 dólares en el uso de herramientas de Hacking Team."[215]

La siguiente imagen muestra los diferentes niveles que componen la estructura del ciberespacio y donde interactúan los diferentes actores de la sociedad.



(https://www.diariodeleon.es/noticias/innova/buscadores-lado-oscuro-internet_1071448.html , 25/07/19).

El Centro Nacional Protección de Infraestructuras (NIPC por sus siglas en inglés) también formó parte de los proyectos que el Buró Federal de Investigación desarrolló para evaluar el riesgo en Infraestructuras Criticas principalmente informáticas, aunque, actualmente dicho organismo ya no forma parte del FBI. "Anteriormente una unidad de la Buro Federal de Investigación (FBI), el Centro Nacional de Protección de Infraestructura (NIPC) se mudó al Departamento de Seguridad Nacional (DHS) cuando este último comenzó a funcionar en marzo de 2003. NIPC está encargado de evaluar las amenazas a la infraestructura crítica - particularmente los sistemas informáticos - y proporcionar advertencias sobre amenazas y vulnerabilidades. También lleva a cabo investigaciones y proporciona una respuesta a los ataques informáticos."[216]

[215] Suárez A. (2015). *Espionaje económico e industrial*. En El Quinto Elemento (p.77). España: Deusto S.A. Ediciones.

[216] Encyclopedia.com. (abril 8, 2020). *Centro de Protección de Infraestructura, Nacional de los Estados Unidos*. mayo 22, 2020, de Encyclopedia.com Sitio web: https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/infrastructure-protection-center-nipc-united-states-national.

Finalmente, aunque la función del FBI está dirigida a atender los casos de cibercrimen, existe una aportación de dicha institución en el tema del ciberterrorismo como se planteó en este apartado.

4.2.3. EL DHS; ACCIONES PARA DETECTAR Y PREVENIR LAS AMENAZAS DEL CIBERESPACIO.

El Departamento de Seguridad Nacional actualmente se distingue por ser uno de los principales organismos que trabajan en materia de ciberseguridad. En este apartado se plantearán los proyectos de dicha institución en la materia. "El DHS es el principal organismo en materia de ciberseguridad nacional, y su Dirección de Programas y Protección Nacional (NPPD) tiene la responsabilidad operativa. La NPPD se ve obstaculizada tanto por la falta de recursos como de competencia legislativa."[217]

Departamento de Seguridad Nacional tiene la función de unir instituciones con el propósito de elaborar medidas en ciberseguridad y dar una respuesta uniforme al fenómeno digital. "Los esfuerzos realizados en Ciberdefensa dentro de EE.UU. son llevados a cabo principalmente por el DHS, entre cuyas responsabilidades están las siguientes:

1. Desarrollar un plan integral para asegurar los recursos clave y las infraestructuras críticas de los Estados Unidos, incluyendo las TIC y los bienes tecnológicos y físicos en los que se apoyan;
2. Proporcionar gestión de las crisis, en respuesta a los ataques que puedan sufrir los sistemas críticos de información;
3. Proporcionar asistencia técnica al sector privado y otras entidades gubernamentales, con respecto a los planes de recuperación de emergencia para fallos en los sistemas de información críticos.
4. Coordinarse con otras agencias del gobierno federal para:
5. Proveer información específica de alarma y consejo sobre las medidas de protección adecuadas y las contramedidas a adoptar por las organizaciones estatales, locales y no gubernamentales incluyendo al sector privado, académico, etc.
6. Llevar a cabo y financiar la investigación y desarrollo, junto con otras agencias, lo que llevará a nuevos conocimientos científicos y tecnologías en apoyo a la seguridad nacional.

[217] Andrew J. (julio 2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad*. (p.55). marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.

Dentro del DHS las responsabilidades en Ciberdefensa han sido asignadas más concretamente a la "División de Ciberseguridad Nacional" de la "Junta Directiva para la Seguridad Nacional y Programas"."[218]

El Departamento de Seguridad Nacional además de encargarse de crear alianzas entre los organismos del gobierno, también se encarga de generar las alianzas necesarias con el sector privado, quien desempeña un papel fundamental en el tema de ciberseguridad. "El DHS fomenta, dentro del sector privado, el desarrollo de la capacidad de compartir una visión resumida de la salud del ciberespacio. Motivado por ello, el DHS creará un punto de contacto para la interacción del gobierno federal y otros socios, para todo lo referente a funciones que se presten constantemente, como el análisis, la alerta, el compartir la información, la respuesta a incidentes graves y los esfuerzos de recuperación a nivel nacional."[219]

Como resultado de la necesidad por unir esfuerzos entre las agencias para dar una respuesta uniforme en ciberseguridad el Departamento de Seguridad Nacional desarrollo el Plan Nacional de Protección de Infraestructuras (NIPP por sus siglas en inglés), donde se destaca el valor y vulnerabilidades que el ámbito digital representa en la sociedad actual. "El DHS y sus socios desarrollaron el Plan Nacional de Protección de Infraestructuras ("National Infrastructure Protection Plan", NIPP), que junto a los Planes complementarios Específicos por Sector, proporcionan una estructura consistente y unificada para integrar los esfuerzos de protección actuales y futuros relativos a las infraestructuras nacionales… se identifica que en este plan se reconoce que la economía y la seguridad nacional de los EE.UU. son altamente dependientes de las TIC porque estas posibilitan el funcionamiento de servicios esenciales de la nación. Por otro lado, la proliferación de las TIC aunque mejora la productividad y la eficiencia también incrementa el riesgo de ciberataques contra la nación, si la ciberseguridad no es abordada e integrada de forma apropiada."[220]

Asimismo, el Departamento de Seguridad Nacional establece en 2017 la estrategia de seguridad cibernética, la cual se conforma por cinco pilares fundamentales para alcanzar sus objetivos. "En medio de la preocupación por la seguridad de las elecciones intermedias y los ataques de alto perfil contra empresas privadas, el Departamento de Seguridad Nacional emitió el 16 de mayo su Estrategia de Seguridad Cibernética, según lo dispuesto en la Sección 1912

[218] Pastor O, Pérez J, Arnáiz D, Taboso P. (octubre 2009). *Seguridad Nacional y Ciberdefensa*. (p.55-54) noviembre 3, 2017, de ISDEFE Sitio web: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.
[219] Pastor O, Pérez J, Arnáiz D, Taboso P. (octubre 2009). *Seguridad Nacional y Ciberdefensa*. (p.64-65) noviembre 3, 2017, de ISDEFE Sitio web: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.
[220] Pastor O, Pérez J, Arnáiz D, Taboso P. (octubre 2009). *Seguridad Nacional y Ciberdefensa*. (p.59-60) noviembre 3, 2017, de ISDEFE Sitio web: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

de la Ley de Autorización de Defensa Nacional 2017. La estrategia brinda al DHS un marco de cinco años para reducir las vulnerabilidades de seguridad cibernética, crear resiliencia y mejorar las capacidades de respuesta ... El documento de estrategia identifica cinco pilares de un enfoque de gestión de riesgos de ciberseguridad en todo el departamento. El primer pilar apunta a comprender mejor las amenazas que enfrentan los EE. UU. El segundo, tercer y cuarto pilares trabajan para reducir la frecuencia y el daño de las amenazas cibernéticas. Finalmente, el quinto pilar apunta a hacer que el ciberespacio sea más defendible." [221]

Finalmente, como parte de las aportaciones del DHS se desarrolló en conjunto con otras instituciones el Centro Nacional de Resistencia de Ciberseguridad, quien desarrollar sandbox que ponen a prueba futuros proyectos en ciberseguridad. "El Departamento de Seguridad Nacional, el Departamento de Comercio y el Departamento de Energía aportan recursos y capacidades para establecer un Centro Nacional de Resistencia de Ciberseguridad donde las empresas y organizaciones de todo el sector pueden probar la seguridad de los sistemas en un entorno contenido, como por ejemplo someter una réplica de una red eléctrica a un ciberataque."[222]

Finalmente, los proyectos del Departamento de Seguridad Nacional están dirigidos a desarrollar una relación de cooperación entre los diferentes órganos del país y el sector privado con el fin de acoplarse a las demandas del nuevo ámbito donde se desarrollan las amenazas actuales.

4.2.4. ALCANCES DEL PENTÁGONO PARA UN CIBERESPACIO SEGURO.

El Departamento de Defensa, también conocido como el Pentágono, es quien trabaja en la seguridad informática en el sentido militar. En este apartado se describirán algunas de sus aportaciones. "A medida que ha aparecido la escala de la amenaza de la ciberguerra a la seguridad nacional y a la economía de Estados Unidos, el Pentágono ha creado defensas en

[221] SecureWeek. (junio 28, 2018). *La estrategia de ciberseguridad del Departamento de Seguridad Nacional DHS*. agosto 6, 2019, de SecureWeek Sitio web: https://www.secureweek.com/2018/06/28/la-estrategia-de-ciberseguridad-del-departamento-de-seguridad-nacional/.

[222] Oficina del Secretario de prensa. (febrero 9, 2016). *Plan de Acción Nacional de Ciberseguridad*. enero 10, 2018, de La Casa Blanca Sitio web: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

etapas y robustas alrededor de las redes militares e inauguró el nuevo Comando Cibernético de Estados Unidos para integrar operaciones de ciberdefensa en la milicia."[223]

Como se mencionó el Departamento de Defensa desarrolla proyectos de ciberseguridad con sentido militar, en este sentido se crea el ejército informático, también conocido como USCYBERCOM. "La creación del USCYBERCOM, el cibercomando impulsado oficialmente desde el Pentágono desde principios de octubre, se configura como la unidad altamente especializada encargada de las operaciones de defensa de las redes de información sensibles de Estados Unidos. También incluye entre sus competencias operaciones de ataque cibernético, entre otras muchas, y su labor será crucial para defender al país de los continuos ataques de hackers relacionados con China, Rusia y otros países." [224]

El proyecto de Estados Unidos de crear un ejército cibernético surge en 2018, año en el cual se planeó iniciar el proyecto con al menos 133 equipos destinados para la fuerza de misión cibernética, quien tiene como objetivo apoyar al gobierno en misiones y crisis cibernéticas. "El Comando Cibernético de EE. UU. Está construyendo una Fuerza de Misión Cibernética de 133 equipos ensamblados a partir de 6,200 militares, civiles y personal de apoyo de contratistas de todos los departamentos militares y componentes de defensa. La Cyber Mission Force, que estará en pleno funcionamiento en 2018, ya está empleando capacidades en apoyo de los objetivos del Gobierno de los EE. UU. En todo el espectro de operaciones cibernéticas."[225]

Los comandos cibernéticos se crearon con el propósito de brindar al gobierno de los Estados Unidos la capacidad de respuesta en todos los dominios del ciberespacio, dicho esto el autor Alejandro Suárez describe su función; "La tarea de los USCYBERCOM es «planear, coordinar, integrar, sincronizar y conducir actividades para: dirigir operaciones y defender las redes de información específicas del Departamento de Defensa; prepararse para (y dirigir, cuando se indique) operaciones militares que barran todo el espectro del ciberespacio, con el objetivo de

[223]Lynn W. *Defendiendo un nuevo ámbito*. enero 23, 2018, de Sitio web: http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/1524/Defendiendo%20un%20nuevo%20%C3%A1mbito.%20La%20ciberestrategia%20del%20Pent%C3%A1gono.pdf?sequence=1&isAllowed=y.

[224] BBC NEW. (junio 25, 2019). *Que es el cibercomando de EU, la avanzada fuerza que Trump utiliza contra Irán y Rusia*. mayo 22, 2020, de El Universal Sitio web: https://www.eluniversal.com.mx/mundo/que-es-el-cibercomando-de-eu-la-avanzada-fuerza-que-trump-utiliza-contra-iran-y-rusia.

[225] Oficina del Secretario de prensa. (febrero 9, 2016). *Plan de Acción Nacional de Ciberseguridad*. enero 10, 2018, de La Casa Blanca Sitio web: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

permitir acciones en todos los dominios; asegurar la libertad de acción en el ciberespacio de Estados Unidos y sus aliados, y denegársela a todos los enemigos».” [226]

El comando cibernético tiene tres misiones, dirigidas a fomentar el cambio de paradigma que actualmente demanda el fenómeno digital que experimenta la sociedad, dicho cambio consiste en actuar de manera conjunta para dar una respuesta uniforme al ciberterrorismo. “El Comando Cibernético tiene tres misiones. Primero, está al frente de la protección diaria de todas las redes de defensa y apoya las misiones militares y contraterroristas con operaciones en el ciberespacio. Segundo, provee una manera clara y responsable de ordenar los recursos de la ciberguerra de toda la milicia. La tercera misión del Comando Cibernético es trabajar con una variedad de socios dentro y fuera del gobierno de Estados Unidos. Representantes del FBI, del Departamento de Seguridad Nacional, del Departamento de Justicia y de la Agencia de Sistemas de Informática de la Defensa trabajan en el cuartel general del Comando Cibernético, en el Fuerte Meade, al igual que oficiales de enlace de la comunidad de inteligencia y de gobiernos aliados.”[227]

Como se expresó en otros apartados, la creación de puestos especializados en el tema de ciberseguridad es parte de la respuesta del gobierno y la inteligencia del país ante el ciberterrorismo. “El Pentágono creó por primera vez el puesto de Chief Information Officer (jefe de información), que también servía como ayudante suplente del secretario de Defensa del Command, Control, Communications, and Inteligence (C3I). Art Money, la primera persona en ocupar ese puesto, se convirtió en la persona clave del Pentágono para mejorar la seguridad informática y asegurar que Internet no se iba a convertir en el talón de Aquiles del ejército más poderoso del mundo.”[228]

En síntesis, el Pentágono se encarga de dar el sentido militar a la estrategia de ciberseguridad de los Estados Unidos, adaptándose a las condiciones del ciberespacio, es decir, la forma militar de responder en el ciberespacio no es de la misma manera que en un ámbito físico.

---

[226] Suárez A. (2015). *Ciberguerra*. En El Quinto Elemento (p.176). España: Deusto S.A. ediciones.

[227] Lynn W. *Defendiendo un nuevo ámbito*. enero 23, 2018, de Sitio web: http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/1524/Defendiendo%20un%20nuevo%20%C3%A1mbito.%20La%20ciberestrategia%20del%20Pent%C3%A1gono.pdf?sequence=1&isAllowed=y.

[228] Verton D. (2004). *Terror en la red: Internet como arma*. En Black Ice: Una amenaza invisible del ciberterrorismo (p.38). Madrid: McGraw-Hill.

4.2.5. EL CENTRO DE INTEGRACIÓN DE INTELIGENCIA CONTRA LA AMENAZA CIBERNÉTICA, UN ORGANISMO PARA LA NUEVA ERA DEL TERRORISMO.

Así como desarrollar puestos especializados en el ámbito digital, es parte de la respuesta del gobierno y sus organismos hacia el ciberterrorismo, el desarrolló de instituciones especializadas en ciberseguridad como, el Centro de Integración de Inteligencia Contra la Amenaza Cibernética, también son parte de dicha estrategia.

Como ya se planteó la inteligencia de los Estados Unidos son entidades autónomas y cada una de estas agencias, anteriormente al fenómeno digital, tomaban decisiones de manera independiente con base a la información que estas mismas obtenían. Estas agencias no compartían información entre ellas, sin embargo, hoy en día las necesidades en seguridad son distintas, es necesario compartir información y trabajar en conjunto, para satisfacer esa necesidad se desarrolló: "La nueva agencia, denominada Centro de Integración de Inteligencia contra la Amenaza Cibernética (CTIIC, por sus siglas en inglés), recopilará información de inteligencia entre varios departamentos gubernamentales, que la obtienen por separado. "Tenemos que compartir información más ampliamente y coordinar acciones. Podemos hacer más en evaluar las amenazas que se mueven rápidamente", apuntó la asesora de la Casa Blanca. El CTIIC busca emular el modelo del Centro Nacional de Contraterrorismo, que se creó tras los atentados del 11 de septiembre de 2001 ante las críticas de que el Gobierno no compartió adecuadamente información de inteligencia que podría haber evitado los ataques terroristas. Mónaco admitió diferencias entre la lucha contra el terrorismo y la piratería informática, pero consideró que los cambios "estructurales, organizativos y culturales" aplicados en el primer ámbito pueden ser útiles en el segundo."[229]

La Oficina del Director de Inteligencia Nacional (ODNI por sus siglas en inglés) estableció cinco responsabilidades para el Centro de Integración de Inteligencia Contra la Amenaza Cibernética. "El Memorando Presidencial delineó cinco responsabilidades para el Centro:

1. Proporcionar un análisis integrado de todas las fuentes de inteligencia relacionada con ciberamenazas extranjeras o incidentes cibernéticos que afecten los intereses nacionales de los EE. UU.
2. Apoyar centros cibernéticos federales proporcionando acceso a la inteligencia necesaria para llevar a cabo sus respectivas misiones.
3. Supervisar el desarrollo y la implementación de capacidades de intercambio de inteligencia para mejorar el conocimiento situacional compartido de la inteligencia relacionada con amenazas e incidentes cibernéticos en el extranjero.

[229] Faus J. (febrero 10, 2015). *Estados Unidos aplica el modelo antiterrorista a la ciberseguridad*. mayo 7, 2018, de El País Sitio web: https://elpais.com/internacional/2015/02/11/actualidad/1423610572_212199.html.

4. Asegúrese de que los indicadores de actividad cibernética maliciosa y, según corresponda, los informes de amenazas relacionados incluidos en los canales de inteligencia se degraden a la clasificación más baja posible para su distribución a las entidades del sector privado de los Estados Unidos y el gobierno de Estados Unidos.
5. Facilitar y apoyar los esfuerzos interinstitucionales para desarrollar e implementar planes coordinados para contrarrestar las amenazas cibernéticas extranjeras a los intereses nacionales de los EE. UU. Utilizando todos los instrumentos de poder nacional, incluidas las actividades diplomáticas, económicas, militares, de inteligencia, de seguridad nacional y de aplicación de la ley." [230]

Entre las funciones del Centro de Integración de Inteligencia contra la Amenaza Cibernética destaca el análisis de información, con el fin de hacerla comprensible no solo para especialistas en la materia sino, también para quienes no lo son y de esta manera poder facilitar la toma de decisiones y elaboración de proyectos en ciberseguridad para los Estados Unidos. "CTIIC respalda y facilita las opciones de todo el gobierno en respuesta a amenazas cibernéticas para ayudar a garantizar que los responsables de la toma de decisiones reciban cursos de acción potenciales que reflejen todos los instrumentos del poder nacional. CTIIC ofrece análisis de oportunidad y ayuda a desarrollar medidas de efectividad para los esfuerzos de la campaña cibernética. El Centro identifica formas de facilitar los puntos críticos de decisión y crea marcos repetibles y de amenazas agnósticas para los actores que equilibran los riesgos, los beneficios y las acciones al principio del proceso de toma de decisiones."[231]

Finalmente, es importante mencionar que dicho centro es un proyecto joven por lo cual no cuenta con una gran lista de acciones. Por otra parte, el Centro de Integración de Inteligencia contra la Amenaza Cibernética funge como el punto de enlace de las agencias del país, asimismo, es el organismo encargado de establecer colaboraciones entre el sector público y privado.

[230] Oficina del Director de Inteligencia Nacional. *Quienes somos*. mayo 7, 2018, de Centro de Integración de Inteligencia de Amenazas Cibernéticas Sitio web: https://www.dni.gov/index.php/ctiic-who-we-are.
[231] Oficina del Director de Inteligencia Nacional. *Quienes somos*. mayo 7, 2018, de Centro de Integración de Inteligencia de Amenazas Cibernéticas Sitio web: https://www.dni.gov/index.php/ctiic-who-we-are.

CONCLUSIONES

A lo largo de esta investigación se revisaron conceptos y temas clave para comprender el fenómeno digital que actualmente experimenta la sociedad, empresas y gobiernos.

El primer capítulo se conformó por una serie de conceptos fundamentales para comprender y definir el ciberterrorismo, fenómeno que ha originado nuevos conceptos y diluido la línea existente entre el mundo físico y el digital. De igual manera se definió como la continuación del terrorismo a través del uso de otros medios y recursos como, la tecnología que ha permitido ampliar sus efectos a bajos costos y con un menor riesgo para los criminales.

También se demostró el valor de la información en la sociedad actual y su función para la estabilidad nacional. Por ello el ciberespacio se suma a los ámbitos donde se puede materializar la guerra y poner en peligro a las naciones y se definió como; el ámbito que sirve de herramienta a los criminales, debido a sus cualidades y la falta de regulación. Razón por la que se considera un arma de doble filo, porque aporta beneficios a la sociedad, optimizando tiempo y costos mediante la automatización de procesos, pero, también genera vulnerabilidades que ponen en peligro a las naciones.

El ámbito digital tiene cualidades como, la velocidad a la que interactúa, simultaneidad y anonimato, elementos que han incrementado anualmente el uso de ciberataques, cifras donde figura la participación de gobiernos, quienes justifican dichos actos como un acto de seguridad nacional e incluso invierten en desarrollar una carrera armamentística. Dicha carrera avanza a gran velocidad debido a las cualidades ya mencionadas y expone la conciencia de los gobiernos sobre el peligro que representa la tecnología.

Asimismo, la militarización del ciberespacio ha originado un ambiente de guerra cibernética, protagonizada por Estados Unidos y China. Lucha que originó términos como el de ciberguerra (continuación de la guerra en el ámbito digital) dicho termino representa un cambio de paradigma porque en la guerra informática no siempre cumple con los elementos de la guerra tradicional, como ocurre con el uso de la fuerza, los daños físicos pueden o no estar presentes. La participación de los Estados, es otro elemento que contribuye a este cambio ya que no siempre se tiene certeza de su participación, debido al anonimato.

La ciberguerra se considera la guerra fría del siglo XXI porque no ha existido un ataque declarado, sin embargo, se es consciente de la actividad cibernética existente entre ambos países y el desarrollo de armas informáticas, situación que ha generado tensiones en la relación China - Estados Unidos, la cual se ha caracterizado en los últimos años por un constante robo de información de ambas partes, a través de prácticas como el ciberespionaje,

El espionaje se considera un instrumento de la guerra fría y su uso ha trascendido a lo largo de la historia de las Relaciones Internacionales, porque sirve para obtener información previa y estratégica de otros, además, actualmente se apoya de la tecnología para amplificar sus efectos, originando el espionaje digital. Ambos fenómenos son de utilidad para los gobiernos,

quienes han hecho parecer su uso legal, implementando dichas prácticas en agencias de inteligencia, como el caso de Estados Unidos. Asimismo, estas prácticas se justifican como una forma de seguridad para el país y su información, sin embargo, se sabe que son utilizadas con el fin de obtener información estratégica de otros gobiernos, empresas e individuos para favorecerse tanto económica como políticamente. En síntesis, el ciberespionaje es decisivo en la toma de decisiones en la diplomacia.

Por otra parte, las empresas son afectadas por el ciberespionaje por ser uno de los principales desarrolladores de tecnología, y un potencial usuario de los medios informáticos, mismos que utilizan con el fin de hacer crecer sus ganancias mediante procesos de e-commerce, que ha permitido globalizar el comercio a través de Internet, como en el caso de China, quien se caracteriza por impulsar su economía a través de tales prácticas.

Con esta investigación se observaron las vulnerabilidades que el ciberterrorismo ha generado en la sociedad, las cuales es necesario implementar medidas de seguridad. Por ello la ciberseguridad es fundamental para prevenir, evitar y mitigar acontecimientos informáticos que atenten contra la información y la estabilidad de los Estados e instituciones públicas y privadas.

También se planteó la importancia de definir y entender el concepto, ciberseguridad, porque, para plantear estrategias en este sentido, se debe considerar que las características del ámbito digital son distintas a las del ámbito físico, por lo tanto, el ciberespacio requiere de estrategias en función de sus características y necesidades.

En resumen, la seguridad informática también implica un cambio de paradigma, puesto que el contrataque no es una opción viable en el ciberespacio, debido a la velocidad que este interactúa y al anonimato existente, por ello se vuelve un reto para gobiernos y empresas, quienes deben elaborar estrategias de prevención, pues pocas veces se es consciente de estar infectado por un programa malicioso o se conoce al responsable de los ataques.

El primer capítulo de esta investigación tuvo la finalidad de familiarizar al lector con los conceptos utilizados a lo largo de esta. También se plantearon algunos acontecimientos que marcaron el inicio del ciberterrorismo, ante esto cabe destacar que los ataques informáticos han existido incluso antes de los sucesos expuestos, sin embargo, pero con el tiempo estas prácticas evolucionaron al igual que la tecnología, y comenzaron a representar un peligro mayor para la seguridad nacional, al dirigirse a objetivos sensibles de las naciones.

El 11 de septiembre de 2001 mostró el valor de mantener en funcionamiento estructuras controladas por sistemas informáticos, como el sistema de emergencias el cual se vio afectado con el derrumbe de las torres gemelas. Además, con el estudio de dicho atentado también se obtuvo información de los daños sufridos en la red de algunos aeropuertos, provocados a través de programas maliciosos. En el 11S vislumbró que la próxima guerra sería a través del ámbito digital y era necesario protegerlo. Sin embargo, no se tomaron medidas al respecto y

como resultado se tuvieron escenarios como los ocurridos en Estonia en 2007 o en Estados Unidos en 2008.

Los ciberataques a Estonia en 2007 permitieron entender que la dependencia tecnológica en sistemas sensibles puede tener consecuencias graves para toda una nación, sobre todo en aquellas que han alcanzado un alto nivel de interconectividad. Además, se resaltó la falta de experiencia ante una crisis informática tanto de gobiernos como de las empresas que brindan servicios en ciberseguridad.

La Operación Buckshot Yankee marcó un momento decisivo para Estados Unidos en materia de ciberseguridad, así como en su momento lo hizo el 11 de septiembre de 2001 en el tema de Seguridad Nacional. Dichos casos son muestra del escepticismo de los gobiernos ante las capacidades de las amenazas, porque en ambos casos existieron análisis previos que planteaban la necesidad de elaborar estrategias para prevenir crisis en materia de seguridad, sin embargo, en ambos casos las medidas se tomaron posterior a los ataques.

Los acontecimientos desarrollados en el segundo capítulo, mostraron que tanto el terrorismo como el ciberterrorismo tiene diversos intereses entre los que se encuentran interés políticos, militares, comerciales e incluso sociales y culturales. Además, se pudo observar que no existe una estrategia de ciberseguridad y que la respuesta dada por los gobiernos es momentánea, la cual no sirve para evitar futuros acontecimientos, es decir, no se han elaborado estrategias que realmente eliminen la proliferación de grupos terroristas y la realización de actos que atenten contra la estabilidad nacional.

En el tercer capítulo se planteó como el ciberterrorismo ha impactado en los costos para efectuar un ataque, reduciéndolos, al igual que el grado de riesgo que los criminales asumen en un ataque convencional, por ende, el grado de violencia que se experimenta en el terrorismo y la guerra. También en este apartado se observó que derivado de las características del ciberespacio se ha originado una carrera armamentista informática, en la cual invierten los gobiernos, aunque estos la justificado como parte de su estrategia de seguridad, sin embargo, se ha comprobado el uso de estas prácticas para obtener ventaja ante otros gobiernos y favorecer a sus empresas y economía.

De dicha carrera armamentista surgieron programas como Stuxnet quien se considera uno de los primeros programas en mostrar las capacidades y efectos en la sociedad de los programas maliciosos, asimismo, resalto el peligro de la dependencia tecnológica de infraestructuras críticas.

Stuxnet resalto que la frontera entre el ciberespacio y el mundo físico se ha disuelto y actualmente es posible causar daños físicos a través de un medio digital. Por otra parte, dicho malware también expuso la participación de las empresas en proyectos como este, derivado del compromiso que tienen de colaborar con el gobierno en temas que atenten contra la seguridad del país, esto particularmente en el caso de Estados Unidos.

Asimismo, el ciberterrorismo también mostró que no siempre se necesita recurrir a la violencia o a los daños físicos para representar un peligro, muestra de ello es “Flame” programa malicioso caracterizado por el robo de información de funcionarios iraníes, donde sobresale el valor de la información como instrumento para ejercer presión sobre los gobiernos.

Gauss, denotó el valor de la información en la era digital, al igual que Flame. Ambos programas son cruciales para definir el ciberterrorismo y ciberguerra, porque cumplen con características que los diferencian de los programas de cibercrimen, como el perseguir objetivos específicos tales como infraestructuras críticas.

La carrera armamentista crece a gran velocidad, debido a que las ciberarmas no siempre se desarrollan desde cero, es decir, toman elementos de programas ya existentes para la creación de nuevos. Además, al igual que la tecnología las armas informáticas han evolucionado y se han convertido en un fenómeno que puede tener consecuencias físicas e incluso mortales.

También se expuso la relevancia que la información ha adquirido en las Relaciones Internacionales a lo largo de la historia, derivado del uso estratégico que se la da, las amenazas informáticas van en aumento. Además, la información previa es un medio utilizado por los gobiernos y empresas para obtener proyectos principalmente tecnológicos, sin la necesidad de comenzar de cero, situación que optimiza tiempo a la hora de desarrollar proyectos.

Por su parte, el robo de información ha representado pérdidas de conocimiento y saldos negativos tanto para el sector privado como el público debido a la falta de medidas eficientes de ciberseguridad. En conclusión, la información es un elemento que otorga poder a quien la posea, por ello se ha clasificado como el petróleo de la actualidad ya que por obtenerla puede desencadenarse escenarios incluso de guerra.

Como se mencionó las empresas juegan un papel importante dentro del mundo de la tecnología, y se han apoyado de las herramientas tecnológicas para expandir sus capacidades e incrementar sus ganancias como ha ocurrido en la región Asia - Pacífico, la cual se ha caracterizado por impulsar su economía a través de Internet, volviéndose vulnerables a los peligros del ciberespacio. Dicho lo anterior anualmente las empresas registran pérdidas económicas e intelectuales, derivado de los constantes ciberataques entre empresas, lo que dio origen a la denominada guerra comercial. Sin embargo, no solo las empresas atacan a otras empresas, los gobiernos y criminales también han entendido el valor del sector empresarial dentro de la estructura de los Estados y han visto a este actor como un medio para desestabilizar, ejercer presión y causar daños a los gobiernos.

Las Infraestructuras Críticas, son otro de los sectores afectados por el ciberterrorismo al ser el sistema nervioso de un país ya que son los encargados de controlar servicios indispensables para la sociedad, como ocurre con el sistema eléctrico, del cual depende el funcionamiento de otros sistemas alterno, como la bolsa de valores o las plantas nucleares, derivado de la sensibilidad de dichas infraestructuras es que se han convertido en un medio a través del cual

se puede poner en peligro a los Estados. Al ser consideradas un pilar de la estructura en los países demandan una estrategia de ciberseguridad eficiente, porque de lo contrario las consecuencias de un ataque digital hacia estas pueden ser catastróficas, como advirtió Stuxnet.

El fenómeno digital ha desencadenado una guerra comercial donde destacan países como Estados Unidos y China, este último ha mostrado un interés por secretos industriales y comerciales de empresas e instituciones de Estados Unidos, situación que se relaciona a la necesidad de China por alcanzar el desarrollo económico y convertirse en una verdadera potencia mundial y para alcanzarlo debe comenzar a producir su propia tecnología.

En resumen, China con su actividad cibernética persigue intereses económicos y políticos muestra de ello la Operación Aurora, que es el resultado de la intrusión que expuso como el país emplea Internet como un medio de control social para favorecer al régimen chino al filtrar la información que llega a su población. Asimismo, los ataques hacia la firma de Google se utilizaron para identificar a la oposición del país.

Los ciberataques hacia Google expusieron la carrera militar que China desarrolla en el ciberespacio a través bases militares como el Grupo Shanghái, el cual es el reflejo del interés del gobierno por dominar la información y crear un ciberejército proyecto donde participan el gobierno, las empresas y universidades del país. Por otra parte, la creación de un ejército informático se considera parte de la estrategia de ciberseguridad del país basada en la investigación, desarrollo e innovación.

De igual manera Estados Unidos ha desarrollado su estrategia para dar respuesta al fenómeno digital, porque como se sabe el país se ha caracterizado por su interés en temas de Seguridad Nacional a consecuencia de los atentados del 11 de septiembre de 2001, con los cuales inicio oficialmente la guerra contra el terrorismo. Como resultado de la guerra contra el terrorismo se estableció la responsabilidad para las empresas de colaborar con el gobierno en temas que pusieran en riesgo la estabilidad del país, ello bajo el lema de “conmigo o contra mí”, el uso del sentimiento nacionalista y todo lo que estuviera en manos del gobierno para lograr dicha colaboración.

A la estrategia de ciberseguridad de Estados Unidos se han sumado algunas de las agencias de inteligencia del país, las cuales en la mayoría de las ocasiones han demostrado su falta de experiencia en el tema y han aplicado programas desarrollados para otras amenazas, las cuales no son suficientes ni acordes a las necesidades del fenómeno digital, como resultado el ciberterrorismo sigue representando un peligro para el país. También es importante reconocer como estas agencias han renunciado a la autonomía de la que gozan para adaptarse a las necesidades de la seguridad informática, la cual demanda un flujo de información para lograr una respuesta homogénea.

Además, como parte de la estrategia de ciberseguridad se ha creado nuevas instituciones especializadas en el tema informático, quienes se han encargado de concentrar la información y ser el enlace entre organismos públicos y establecer relaciones con el sector privado.

En conclusión, la respuesta del gobierno de los Estados Unidos no ha sido suficiente para detener la proliferación del fenómeno ciberterrorista y la ciberseguridad seguirá siendo un reto para los gobiernos quienes se enfrentan a cualidades como la velocidad a la que el ciberespacio interactúa.

Finalmente, se espera que esta investigación sirva para exponer el peligro que representan el ciberespacio para las naciones y la importancia de que los internacionalistas estudien dicho ámbito.

GLOSARIO

1. **Anonimato:** Estado de una persona cuyo nombre no es conocido. Condición de la persona que oculta su nombre o su personalidad.
2. **Antivirus:** El concepto de antivirus se utiliza en el terreno de la informática con referencia a un software que está en condiciones de buscar y eliminar virus en un sistema informático.
3. **APT advanced:** Tienen dos significados: Por una parte, esta amenaza es un tipo sofisticado de ciberataque. En cambio, también puede referirse a aquellos grupos, normalmente patrocinados por los estados, que son los responsables del lanzamiento de dichas campañas maliciosas.
4. **Argot informático:** Es el lenguaje específico utilizado por un grupo de personas que comparten unas características comunes por su categoría social, profesión, procedencia, aficiones, etc. Los grupos profesionales suelen crear tanto argots como jergas. Piénsese en policías, profesionales de la medicina y de la informática, deportistas o periodistas.
5. **Automatización:** Aplicación de máquinas o de procedimientos automáticos en la realización de un proceso o en una industria.
6. **B2B:** Significa de negocio a negocio, es un modelo de transmisión de información en la red relacionado con las transacciones comerciales que las empresas del mundo realizan.
7. **Bushehr:** La central nuclear de Bushehr (BNPP) es el primer reactor nuclear comercial de Irán. En 1994, Teherán y Moscú firmaron un acuerdo para construir el reactor de agua ligera VVER 1000MWe.
8. **Centrifugadoras:** Máquina que aprovecha la fuerza centrífuga para secar ciertas sustancias o para separar los componentes de una masa o mezcla.
9. **Ciberamenazas:** Aquellas actividades realizadas en el ciberespacio, que tienen por objeto la utilización de la información que circula por el mismo, para la comisión de distintos delitos mediante su utilización, manipulación, control o sustracción.
10. **Ciberarmas:** Es un elemento, script, código malicioso, X lo que sea para atacar y muy importante también nos puede servir para defendernos.
11. **Cibercrimen:** Se entiende que se trata de delitos cometidos a través de internet por medio del uso de un computador o mecanismo análogo (por ejemplo: smartphone, pendrive, tablet, etc.).
12. **Comunidad SoS:** La Unidad de Soporte de Operaciones y Sistemas (S.O.S.), asume la atención y resolución de consultas relacionadas con el uso de ordenadores y redes de voz y datos.
13. **Criptografía:** Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.
14. **Data mining:** La extracción no trivial de información implícita, previamente desconocida y potencialmente útil a partir de datos. La exploración y el análisis -por medios automáticos o semiautomáticos- de grandes cantidades de datos con el fin de descubrir patrones con significado.

15. **DDoS:** En el caso de los ataques DDoS, se realizan peticiones o conexiones empleando un gran número de ordenadores o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio objeto del ataque. Un ataque DDoS es más difícil de detectar, ya que el número de peticiones proviene desde diferentes IP´s y el administrador no puede bloquear la IP que está realizando las peticiones, como sí ocurre en el ataque DoS.
16. **Días cero:** Existen dos tipos de día cero. Una vulnerabilidad de día cero es una brecha en la seguridad del software y puede estar en un navegador o en una aplicación. Por otra parte, un exploit de día cero es un ataque digital que se aprovecha de una vulnerabilidad de día cero para instalar software malicioso en un dispositivo.
17. **Dirección IP:** La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo que utilice el protocolo o, que corresponde al nivel de red del modelo TCP/IP.
18. **Download:** En la informática se puede decir que se utiliza como sinónimo de “bajar”, y “download” es un término que proviene del inglés, compuesto por “down” que significa “abajo” y “load” indica que es “cargar”, esto alude a una copia de datos que es normalmente un archivo entero que pueden ser documentos.
19. **Drivers:** Controlador, rutina o programa que enlaza un dispositivo periférico al sistema operativo.
20. **Duqu:** Es un conjunto de malware para ordenador descubierta el 1 de septiembre de 2011, se cree que está relacionado con el gusano Stuxnet.
21. **E-business:** Consiste en introducir tecnologías de la comunicación para realizar las actividades de un negocio. Es un conjunto de nuevas tecnologías y nuevas estrategias de negocio para desarrollar estos negocios en línea.
22. **Efecto domino:** Es el efecto acumulativo producido cuando un acontecimiento origina una cadena de otros acontecimientos similares.
23. **Era digital:** La Era Digital es el nombre que recibe el período de la historia de la humanidad que va ligado a las tecnologías de la información y la comunicación.
24. **Fibra óptica:** Filamento de material dieléctrico, como el vidrio o los polímeros acrílicos, capaz de conducir y transmitir impulsos luminosos de uno a otro de sus extremos; permite la transmisión de comunicaciones telefónicas, de televisión, etc., a gran velocidad y distancia, sin necesidad de utilizar señales eléctricas.
25. **Firewall:** Es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años.
26. **Globalización:** Es un proceso económico, tecnológico, político, social y cultural a escala mundial que consiste en la creciente comunicación e interdependencia entre los distintos países del mundo uniendo sus mercados sociales, a través de una serie de transformaciones sociales y políticas que les brindan un carácter global. La globalización

es a menudo identificada como un proceso dinámico producido principalmente por la sociedad, y que ha abierto sus puertas a la revolución informática, llegando a un nivel considerable de liberalización y democratización en su cultura política, en su ordenamiento jurídico y económico nacional, y en sus relaciones nacionales e internacionales.

27. **Great Firewall:** El Gran Cortafuegos Chino (Great Firewall, un juego de palabras en referencia a la Gran Muralla China, o Great Wall) es el sistema establecido por el Ministerio de Seguridad Pública de la República Popular de China desde el año 2003 para censurar y vigilar el acceso a Internet de sus habitantes.
28. **Hackers:** Es alguien que descubre las vulnerabilidades de una computadora o un sistema de comunicación e información.
29. **Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático
30. **ICMP:** El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).
31. **innovación I+D+i:** Es un nuevo concepto adaptado a los estudios relacionados con el avance tecnológico e investigativo centrados en el avance de la sociedad, siendo una de las partes más importantes dentro de las tecnologías informativas.
32. **Interconectividad:** Es el nivel de conexión que ocurre entre dos o más elementos.
33. **Internet:** Es un neologismo del inglés que significa red informática descentralizada de alcance global. Se trata de un sistema de redes interconectadas mediante distintos protocolos que ofrece una gran diversidad de servicios y recursos, como, por ejemplo, el acceso a archivos de hipertexto a través de la web.
34. **Link:** Elemento de un documento electrónico que permite acceder automáticamente a otro documento o a otra parte del mismo.
35. **Lloydis:** Es un mercado de seguros británico. Sirve como lugar de encuentro para empresas financieras o aseguradoras.
36. **Malware:** Es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.
37. **Middle core faction:** Es un grupo revolucionario de extrema izquierda japonés, a menudo denominado Chūkaku-ha (中 核 派Facción del Núcleo Medio) en japonés. Sus objetivos principales es que Japón y el mundo entero adopten políticas comunistas.
38. **Nacionalismo:** Doctrina y movimiento políticos que reivindican el derecho de una nacionalidad a la reafirmación de su propia personalidad mediante la autodeterminación política. Apego especial a la propia nación y a cuanto le pertenece.
39. **Natanz:** Es una planta protegida de Enriquecimiento de Combustible, cubre 10 ha; el complejo está construido a 8 metros bajo la superficie y protegida por una coraza de 25 dm de cemento reforzado.
40. **Ordenador:** También denominado como computadora, es una máquina electrónica que recibe y procesa datos con la misión de transformarlos en información útil.

41. **Outsider:** Persona que accede al sistema desde el exterior del perímetro de seguridad.
42. **Overflows:** En seguridad informática y programación, un desbordamiento de búfer (del inglés buffer overflow o buffer overrun) es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada a tal efecto (buffer): Si dicha cantidad es superior a la capacidad preasignada, los bytes sobrantes se almacenan en zonas de memoria adyacentes, sobrescribiendo su contenido original, que probablemente pertenecían a datos o código almacenados en memoria. Esto constituye un fallo de programación.
43. **Página web:** Se conoce como página web al documento que forma parte de un sitio web y que suele contar con enlaces (también conocidos como hipervínculos o links) para facilitar la navegación entre los contenidos.
44. **Patriotismo:** Pensamiento que vincula a un individuo con su patria.
45. **PC:** Sigla de personal computer, computadora personal.
46. **Plan quinquenal:** Es un proyecto, plan, o idea, que se propone terminar o alcanzar su objetivo en un plazo de 5 años. La planificación económica es generalmente promovida por el gobierno de un Estado. Además, sirve para fortalecer a las industrias.
47. **Propiedad intelectual:** Es una rama del derecho que busca por una parte fomentar la innovación, la creación y la transferencia tecnológica y por la otra, ordenar los mercados facilitando la toma de decisiones por el público consumidor.
48. **Ransomware:** Es un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.
49. **Red de servidores C&C:** Es un computador que da órdenes a dispositivos infectados con malware y que recibe información de esos dispositivos. Algunos servidores controlan millones de dispositivos.
50. **Red inalámbrica:** Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.
51. **Routers:** Es un dispositivo de hardware que permite la interconexión de ordenadores en red. Es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet.
52. **Sabotaje:** Daño o destrucción que se hace intencionadamente en un servicio, una instalación, un proceso, etc., como forma de lucha o protesta contra el organismo que los dirige o bien como método para beneficiar a una persona o grupo que es contrario a dicho organismo.
53. **Sandbox:** Es un proceso de separación de entorno, es decir, se aísla un proceso informático cualquiera, con la finalidad de que dicha ejecución sea segura para probarla sin que pueda afectar al resto del sistema, en el caso de que estuviese infectado con cualquier software malicioso.

54. **Secretos comerciales:** Se puede considerar como secreto industrial o empresarial todo conocimiento sobre productos o procedimientos industriales, cuyo mantenimiento en reserva proporciona a su poseedor una mejora, avance o ventaja competitiva.
55. **Seguridad:** Es un conjunto de sistemas, medios organizativos, medios humanos y acciones dispuestas para eliminar, reducir o controlar los riesgos y amenazas que puedan afectar a una persona a una entidad a una instalación o a un objeto. La seguridad proporciona las condiciones para afrontar el peligro, en síntesis, seguridad es la minimización del riesgo.
56. **Seguridad nacional:** La seguridad nacional se refiere a la noción de relativa estabilidad, calma o predictibilidad que se supone beneficiosa para el desarrollo de un país; así como a los recursos y estrategias para conseguirla.
57. **Servidor:** El término servidor tiene dos significados en el ámbito informático. El primero hace referencia al ordenador que pone recursos a disposición a través de una red, y el segundo se refiere al programa que funciona en dicho ordenador.
58. **Siemens:** Es una empresa multinacional nacida en Berlín, Alemania en el año 1847 por Werner von Siemens y Johann Georg Halske que se dedica a las telecomunicaciones, al transporte, la iluminación, medicina, financiamiento, equipos eléctricos, motores, automatización, instrumentación industrial y energía entre otras.
59. **Simultaneidad:** La simultaneidad es la relación entre dos eventos que se supone que ocurren al mismo tiempo en un marco de referencia dado.
60. **SIPRNET:** Es un sistema de redes de computadoras interconectadas utilizado por el Departamento de Defensa de Estados Unidos y el Departamento de Estado norteamericano para trasmitir información secreta, en un entorno absolutamente seguro, que excede las prestaciones del protocolo TCP/IP. También provee servicios como acceso a documentos de hipertexto y correo electrónico, SIPRNet es el componente secreto de la red de sistemas de información de defensa de Estados Unidos.
61. **Software:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.
62. **Startup:** Es una empresa de nueva creación que comercializa productos y/o servicios a través del uso intensivo de las tecnologías de la información y la comunicación (TIC’s), con un modelo de negocio escalable el cual le permite un crecimiento rápido y sostenido en el tiempo.
63. **TCP:** Es un acuerdo estandarizado de transmisión de datos entre distintos participantes de una red informática.
64. **Terrorismo:** Sucesión de actos de violencia ejecutados para infundir terror. Actuación criminal de bandas organizadas, que, reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos.
65. **TI:** La tecnología de la información (TI) es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas.

66. **TOR:** Es una red que implementa una técnica llamada Onion Routing (enrutado cebolla en castellano), diseñada con vistas a proteger las comunicaciones en la Marina de los Estados Unidos. La idea es cambiar el modo de enrutado tradicional de Internet para garantizar el anonimato y la privacidad de los datos.
67. **Troyano:** Es un tipo de malware que a menudo se disfraza de software legítimo. Los cibercriminales y hackers pueden utilizar troyanos para tratar de acceder a los sistemas de los usuarios. Generalmente, los usuarios son engañados por alguna forma de ingeniería social para que carguen y ejecuten troyanos en sus sistemas. Una vez activados, los troyanos permiten a los cibercriminales espiarte, robar tu información confidencial y obtener acceso de puerta trasera a tu sistema.
68. **VoIP:** Es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP.
69. **Vulnerabilidades:** Es el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes, sean ellos desastres naturales, desigualdades económicas, políticas, sociales o culturales.
70. **Wincc SCADA:** Es un sistema de control de supervisión y adquisición de datos e interfaz hombre-máquina de Siemens. Los sistemas SCADA se utilizan para monitorear y controlar procesos físicos involucrados en la industria y la infraestructura a gran escala y a largas distancias.
71. **Zeus:** Es un paquete de malware troyano que se ejecuta en versiones de Microsoft Windows. Se puede utilizar para llevar a cabo muchas tareas maliciosas y delictivas, a menudo se utiliza para robar información bancaria mediante el registro de teclas del navegador y el acaparamiento de formularios.

BIBLIOGRAFÍA

1. Adams J. (1999). La próxima guerra mundial. Buenos Aires. Granica S.A.
2. Arreola A. (2015). En Ciberespionaje: La puerta al mundo virtual de los estados e individuos, una revisión de los programas de espionaje digital de los Estados Unidos. México. Siglo XXI editores.
3. Verton D. (2004) Black Ice: La Amenaza Invisible del Ciberterrorismo. Madrid. McGraw-Hill.
4. Díaz J, Ganuza N, Joyanes L, (febrero 2011). Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. España. Ministerio de Defensa.
5. Flores H. (mayo 2012). Los ámbitos no terrestres en la guerra futura: Espacio. España. Ministerio de Defensa.
6. Puime J. (2009). La violencia del siglo XXI. Nuevas dimensiones de la guerra. España. Ministerio de Defensa.
7. Suárez A. (2015). En El Quinto Elemento. España. Deusto S.A. Ediciones.

MESOGRAFÍA

1. Acero F. (mayo 30, 2007). Consecuencias de los ciberataques a Estonia. septiembre 28, 2017, de LIVEJOURNAL Sitio web: https://fernando-acero.livejournal.com/40250.html.
2. Alfonso J. (septiembre 2015). En Ataques entre Estados mediante Internet. Estudio de casos orientados por el esquema Nacional de Seguridad. noviembre 6, 2017, de Universitat Politécnica de Valéncia Sitio web: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1.
3. Andrades F. (mayo 7, 2013). Cinco escenarios de ciberguerra en el nuevo orden mundial. abril 23, 2018, de eldiario.es Sitio web: https://www.eldiario.es/turing/escenarios-ciberguerra-nuevo-orden-mundial_0_129837338.html.
4. Andrew J. (julio 2016). Experiencias avanzadas en políticas y prácticas de ciberseguridad. marzo 21, 2018, de Banco Interamericano de Desarrollo Sitio web: https://publications.iadb.org/bitstream/handle/11319/7759/Experiencias-avanzadas-en-politicas-y-practicas-de-ciberseguridad-Panorama-general-de-Estonia-Israel-Republica-de-Corea-y-Estados-Unidos.pdf?sequence=7.
5. Appel M. (agosto 2, 2017). La guerra silenciosa de Moscú. septiembre 28, 2017, de Europafocus Sitio web: http://www.europafocus.com/2017/08/02/la-guerra-silenciosa-de-moscu/.
6. Aranda M. (octubre 24, 2017). ¿Cuánto cuesta un ciberataque a las empresas?. enero 16, 2018, de ODS Sitio web: https://opendatasecurity.io/es/cuanto-cuesta-un-ciberataque-a-las-empresas/.

7. Asianews.it. (mayo 20, 2014). Bejin, tira y afloja con los Estados Unidos sobre el espionaje industrial y electrónico. julio 2, 2019, de Asianews.it Sitio web: http://www.asianews.it/noticias-es/Beijing,-tira-y-afloja-con-los-Estados-Unidos-sobre-el-espionaje-industrial-y-electr%C3%B3nico-31123.html.
8. Ballesteros A. Seguridad de Instalaciones. marzo 8, 2019, de Escuela Penitenciaria Nacional Sitio web: http://epn.gov.co/elearning/distinguidos/SEGURIDAD/index.html.
9. Bañuelos E. (marzo 10, 2016). La Próxima Guerra Mundial Será Cibernética. noviembre 11, 2017, de Código Nuevo Sitio web: https://www.codigonuevo.com/sociedad/proxima-guerra-mundial-cibernetica.
10. Bassets M. (mayo 19, 2014). Washington acusa a cinco militares chinos de ciberespionaje industrial. noviembre 28, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400511284_751167.html.
11. BBC MUNDO. (febrero 15, 2011). Revelan radiografía de Stuxnet, "el arma de la ciberguerra". agosto 3, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2011/02/110215_1448_stuxnet_virus_iran_symantec_dc.shtml
12. BBC MUNDO. (mayo 20, 2014). La unidad china 61398, el nuevo enemigo número uno de EE.UU. diciembre 1, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2014/05/140520_tecnologia_hackers_china_unidad_61398_mz.
13. BBC MUNDO. (octubre 18, 2010). La guerra cibernética "debe preocuparnos". agosto 7, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2010/10/101018_1451_guerra_cibernetica_stuxnet_virus_dc.shtml.
14. BBC NEW. (junio 25, 2019). Que es el cibercomando de EU, la avanzada fuerza que Trump utiliza contra Irán y Rusia. mayo 22, 2020, de El Universal Sitio web: https://www.eluniversal.com.mx/mundo/que-es-el-cibercomando-de-eu-la-avanzada-fuerza-que-trump-utiliza-contra-iran-y-rusia.
15. Benedicto M. (abril 23, 2013). EEUU ante el reto de los ciberataques. diciembre 26, 2017, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO37-2013_Ciberataques_BenedictoSolsona.pdf.
16. Calderón V. (agosto 10, 2012). Hallado un nuevo virus utilizado para espiar en Líbano. julio 3, 2018, de El País Sitio web: https://elpais.com/internacional/2012/08/10/actualidad/1344599271_563202.html.
17. Candau J. (febrero 2011). En Ciberseguridad. Retos y Amenazas a la Seguridad Nacional. España. Ministerio de Defensa.
18. Caño A. (febrero 19, 2013). Estados Unidos y China. ante la primera ciberguerra fría. diciembre 5, 2017, de El País Sitio web: https://elpais.com/internacional/2013/02/19/actualidad/1361300185_954734.html.

19. Caro M. (junio 13, 2012). Flame una nueva amenaza del ciberespionaje. junio 29, 2018, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI34-2012_Flame_Ciberespionaje_MJCB.pdf.
20. Caro M. Alcance y Ámbito de la Seguridad Nacional en el Ciberespacio. junio 14, 2017, Sitio web: http://www.ieee.es/Galerias/fichero/cuadernos /CE_149 _Ciberseguridad.pdf.
21. CiberDerecho. ¿Qué es el ciberespionaje Industrial?. marzo 11, 2019, de CiberDerecho Sitio web: http://www.ciberderecho.com/que-es-el-ciberespionaje-industrial/.
22. CIO. (mayo 28, 2012). Flame, nueva arma para el ciberespionaje. marzo 13, 2018, de CIO Sitio web: http://cio.com.mx/flame-nueva-arma-para-el-ciberespionaje/.
23. CNN en español. (agosto 10, 2012). "Gauss", el virus que se autodestruye después de robar tu información. julio 3, 2018, de CNN Sitio web: https://cnnespanol.cnn.com/2012/08/10/gauss-el-virus-que-se-autodestruye-despues-de-robar-tu-informacion/.
24. Departamento de Seguridad Nacional. (agosto 12, 2019). Directiva de los Estados Unidos para la coordinación de ciberincidentes. septiembre 10, 2019, de DSN Sitio web: http://www.dsn.gob.es/es/actualidad/sala-prensa/directiva-estados-unidos-para-coordinacion-ciberincidentes.
25. Díaz D. (marzo 2, 2012). Ciberterrorismo: amenaza que genera enormes pérdidas. abril 23,2018, de Panamá América Sitio web: http://www.panamaamerica.com.pa/content/ciberterrorismo-amenaza-que-genera-enormes-p%C3%A9rdidas.
26. Díez C, Perojo J, Penide J, Arias M. (mayo 19, 2011). Ciber-terrorismo. Definición de políticas de seguridad para proteger infraestructuras críticas frente a ciber- ataques terroristas. enero 16,2018, de Universidad Europea de Madrid Sitio web: http://mendillo.info/seguridad/tesis/Penide-Diez-Arias-Perojo.pdf.
27. Directiva de Decisión Presidencial. (mayo 22, 1998). Protección de infraestructura crítica. octubre 4, 2018, de La Casa Blanca Washington Sitio web: https://fas.org/irp/offdocs/pdd/pdd-63.htm.
28. EcuRed. Ciberespacio. marzo 6, 2019, de EcuRed Sitio web: https://www.ecured.cu/Ciberespacio
29. Ecured. Stuxnet. octubre 27, 2017, de Ecured Sitio web: https://www.ecured.cu/Stuxnet.
30. El País. (enero 19, 2005). El FBI retira "Carnivore", su programa para espiar en internet. enero 5, 2018, de El País Sitio web: https://elpais.com/tecnologia/2005/01/19/actualidad/1106126878_850215.html.
31. El País. (mayo 19, 2014). Las acusaciones de EEUU a China por espionaje. diciembre 5, 2017, de El País Sitio web: https://elpais.com/internacional/2014/05/19/actualidad/1400515474_703728.html.

32. ElMUNDO.es. (junio 20, 2012). EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán. junio 29, 2018, de ELMUNDO.es Sitio web: http://www.elmundo.es/elmundo/2012/06/20/navegante/1340173299.html.
33. Encyclopedia.com. (abril 8, 2020). Centro de Protección de Infraestructura, Nacional de los Estados Unidos. mayo 22, 2020, de Encyclopedia.com Sitio web: https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/infrastructure-protection-center-nipc-united-states-national.
34. Estévez A. (marzo 22, 2011). La Lucha Contra el Ciberterrorismo. enero 5, 2018, de Red Safe World Sitio web: https://redsafeworld.wordpress.com/2011/03/22/la-lucha-contra-el-ciberterrorismo/.
35. Faus J. (febrero 10, 2015). Estados Unidos aplica el modelo antiterrorista a la ciberseguridad. mayo 7, 2018, de El País Sitio web: https://elpais.com/internacional/2015/02/11/actualidad/1423610572_212199.html.
36. Gallagher M. (abril 30, 2012). Ciberguerra: Las víctimas reales que puede dejar un conflicto virtual. marzo 21, 2018, de BBC Sitio web: http://www.bbc.com/mundo/noticias/2012/04/120430_tecnologica_ciber_armas_aa
37. Gómez A. La lucha contra el ciberterrorismo y los ataques informáticos. noviembre 13, 2017, de EDISA Sitio web: https://www.edisa.com/wp-content/uploads/2019/08/la_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf.
38. Gómez O. (julio 14, 2003). Estudian respaldo a "Plan Carnivóro". enero 9, 2018, de El Nuevo Diario Sitio web: http://archivo.elnuevodiario.com.ni/nacional/114569-estudian-respaldo-plan-carnivoro/.
39. Guerras Posmodernas. (abril 28, 2017). Rumbo a Letonia. Y España entro en la nueva guerra fría. septiembre 20, 2017, de Guerra Posmodernas Sitio web: https://guerrasposmodernas.com/2017/04/28/rumbo-a-letonia-y-espana-entro-en-la-nueva-guerra-fria/.
40. INDEADIVERSITY. (diciembre 13, 2016). Introducción a la Ciberseguridad: ¿Qué es y porque es importante?. octubre 3, 2017, de INDEADIVERSITY Sitio web: http://indeadiversity.com/tag/ciberataques/
41. Jeison. (noviembre 1, 2012). Ciberterrorismo. octubre 31, 2017, de E-GOV Sitio web: http://www.egov.ufsc.br/portal/conteudo/ciberterrorismo.
42. KASPERSKYLAB. FLAME. junio 29,2018, de Kaspersky Lab Sitio web: https://www.kaspersky.com/flame.
43. La Razón. (mayo 15, 2017). El próximo 11-S empezará con un click. octubre 3, 2017, de La Razón Sitio web: https://www.larazon.es/blogs/cultura/todo-esta-en-los-libros/el-proximo-11-s-empezara-con-un-click-EB15147641/.
44. Lynn W. Defendiendo un nuevo ámbito, la ciberestrategia del Pentágono. abril 10, 2018, de air&space power journal Sitio web: http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/1524/Defendiendo%20

un%20nuevo%20%C3%A1mbito.%20La%20ciberestrategia%20del%20Pent%C3%A1gono.pdf?sequence=1&isAllowed=y.
45. Maturana J. (abril 21, 2019). Hackers atacan el Pentágono. mayo 21, 2020, de MC Sitio web: muycomputer.com/2009/04/21/actualidadnoticiashackers-atacan-el-pentagono_we9erk2xxdbnybiqxkd6elyiyrjdbw1059gc84jtpr_-wqrbldxlc5ynzmdyqrbn/.
46. Meschoulam M. (octubre 30, 2015). Ciberguerra y Ciberterrorismo: ¿Presente o Futuro?. Septiembre,19, 2017, de El Universal Sitio web: http://www.eluniversal.com.mx/entrada-de-opinion/articulo/mauricio-meschoulam/mundo/2015/10/30/ciberguerra-y-ciberterrorismo.
47. Muñoz M. (julio 24, 2003). Infraestructuras. julio 2, 2019, de Belt.es Sitio web: http://www.belt.es/noticias/2003/julio/24/infraestructuras.htm.
48. NSA|CSS. Oficina de investigación y aplicaciones tecnológicas de la NSA. julio 19, 2019, de NSA Sitio web: https://www.nsa.gov/what-we-do/research/technology-transfer/.
49. Oficina del Director de Inteligencia Nacional. Quienes somos. mayo 7, 2018, de Centro de Integración de Inteligencia de Amenazas Cibernéticas Sitio web: https://www.dni.gov/index.php/ctiic-who-we-are.
50. Oficina del Secretario de prensa. (febrero 9, 2016). Plan de Acción Nacional de Ciberseguridad. enero 10, 2018, de La Casa Blanca Sitio web: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.
51. Oficina del Secretario de Prensa. (julio 26, 2016). Directiva de política presidencial - Coordinación de incidentes cibernéticos de Estados Unidos. enero 10, 2018, de La Casa Blanca Sitio web: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
52. Olmos A, Seco F. Sistemas de gestión para minimizar ciberamenazas. Marzo 13, 2018 AENOR, Sitio web: http://www.aenor.es/revista/pdf/ene15/12ene15.pdf.
53. Ortigosa A, Hernández L. (2016). Las nuevas amenazas cibernéticas del S.XXI, ciberterrorismo: Nueva forma de subversión y desestabilización. octubre 10, 2018, de Cuaderno de la Guardia Civil Sitio web: https://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/local_repository/documents/18272.pdf.
54. Pagnotta S. (junio 28, 2017). Las víctimas de ciberataques perdieron 1,33 mil millones de dólares en 2016. diciembre 26, 2017, de welivesecurity Sitio web: https://www.welivesecurity.com/la-es/2017/06/28/victimas-ciberataques-millones-dolares/.
55. Pastor O, Pérez J, Arnáiz D, Taboso P. (octubre 2009). Seguridad Nacional y Ciberdefensa. noviembre 3, 2017, de ISDEFE Sitio web: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

56. PROFECO. (2016). El comercio electrónico. julio 30, 2018, de PROFECO Sitio web: https://www.profeco.gob.mx/internacionales/com_elec.asp.
57. Quintana Y. (junio 25, 2016). El espía que inauguró la ciberseguridad. septiembre 29, 2017, de eldiario.es Sitio web: http://www.eldiario.es/internacional/espia-inauguro-ciberguerra_0_529847934.html.
58. Red Safe World. (marzo 22, 2011). La lucha contra el ciberterrorismo. enero 5, 2018, de Red Safe World Sitio web: https://redsafeworld.wordpress.com/2011/03/22/la-lucha-contra-el-ciberterrorismo/.
59. Rodríguez C. (agosto 12, 2015). ¿Qué es e-commerce o comercio electrónico?. agosto 25, 2019, de Marketing Digital Sitio web: https://marketingdigital.bsm.upf.edu/e-commerce-comercio-electronico/
60. Romeo N. (agosto 8, 2016). La Amenaza Cibernética: Ciberguerra y Ciberdefensa. octubre 31, 2017, de CISDE Sitio web: https://observatorio.cisde.es/archivo/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa/.
61. Saiz E. (marzo 13, 2013). Los ciberataques sustituyen al terrorismo como primera amenaza para EEUU. enero 30, 2018, de El País Sitio web: https://elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html.
62. Salellas L. Seguridad informática - Ciberterrorismo. octubre 23, 2017, de Ilustrados Sitio web: http://www.ilustrados.com/tema/9670/Delitos-Informaticos-Ciberterrorismo.html.
63. Sánchez M. (marzo 5, 2011). El espionaje industrial chino en aumento. diciembre 7, 2017, de BBC MUNDO Sitio web: http://www.bbc.com/mundo/noticias/2011/03/110224_china_espionaje_economico_mes.shtml.
64. Schmitt M. (junio 30, 2002). La guerra de la información: Los ataques por vía informática y el just in bello. Octubre 31, 2017. de Comité Internacional de la Cruz Roja Sitio web: https://www.icrc.org/data/rx/es/resources/documents/misc/5tecg3.htm.
65. SecureWeek. (junio 28, 2018). La estrategia de ciberseguridad del Departamento de Seguridad Nacional DHS. agosto 6, 2019, de SecureWeek Sitio web: https://www.secureweek.com/2018/06/28/la-estrategia-de-ciberseguridad-del-departamento-de-seguridad-nacional/.
66. Seguridad Informática. (agosto 22, 2013). Solo el 35% de las organizaciones detectan filtraciones en los primeros minutos. enero 4, 2018, de Seguridad Informática Sitio web: https://seguinfo.wordpress.com/category/estadisticas/.
67. Seguridad Informática. (julio 3, 2013). ¿Cuánto cuesta a una empresa un incidente grave de seguridad?. enero 4, 2018, de Seguridad Informática Sitio web: https://seguinfo.wordpress.com/category/estadisticas/.
68. Sistemas. Definición de e-commerce. marzo 11, 2019, de Sistemas Sitio web: https://sistemas.com/e-commerce.php.

69. Soesanto S. (octubre 1, 2016). No todos los ataques son ciberataques. octubre 3, 2017, de EL País Sitio web: https://elpais.com/tecnologia/2016/09/28/actualidad/1475059265_198963.html.
70. SOS. Objetivos de la organización virtual de ciencias de la seguridad. julio 19, 2019, de SOS Sitio web: https://cps-vo.org/group/SoS/about.
71. Tecnologicon. (julio 6, 2015). Definición de Ciberespacio. marzo 3, 2019, de Tecnologicon Sitio web: https://tecnologicon.com/definicion-de-ciberespacio-informatica/.
72. The Physics Arxiv Blog. (septiembre 13, 2015). Los 20 ciberataques más perversos del S.XXI. junio 10,2017, de MIT Technology Review Sitio web: https://www.technologyreview.es/s/7413/los-20-ciberataques-mas-perversos-del-siglo-xxi.
73. Theiler O. Nuevas amenazas: El ciberespacio. junio 7,2017, de OTAN Sitio web: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm.
74. Ureña F. (enero 16, 2015). Ciberataques, la mayor amenaza actual. mayo 15, 2020, de ieee.es Sitio web: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf.
75. Valencia I. (octubre 17, 2017). Los ciberataques pueden salir más caros que los huracanes. septiembre 22, 2017, de CICESE Sitio web: https://seguridad.cicese.mx/alerta/167/Los-ciberataques-pueden-salir-m%C3%A1s-caros-que-los-huracanes.
76. Valencia I. (octubre 17, 2017). Los ciberataques pueden salir más caros que los huracanes. septiembre 22, 2017, de CISECE Sitio web: https://seguridad.cicese.mx/alerta/167/Los-ciberataques-pueden-salir-m%C3%A1s-caros-que-los-huracanes.
77. XL SEMANAL. Los cibersoldados de la OTAN. septiembre 28, 2017, de XL SEMANAL Sitio web: http://www.xlsemanal.com/actualidad/20141123/cibersoldados-otan-7850.html