



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

*La estrategia de ciberseguridad de Barack Obama: El
ataque (ciberguerra) al Programa Nuclear Iraní en 2010*

T E S I S

PARA OPTAR POR EL GRADO DE

Licenciado en Relaciones Internacionales

P R E S E N T A :

Fredy Alejandro Escárcega García

**DIRECTOR DE TESIS:
Dr. Jesús Gallegos Olvera**



Ciudad Universitaria, Enero 2017



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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

AGRADECIMIENTOS:

Agradezco a mi familia, por estar a mi lado en todo estos años. Por enseñarme a caer y levantar, por creer en mí y sobre todo por darme las herramientas necesarias para afrontarme a los retos.

A Teresita. Muchas gracias mami, por tu comprensión y amor, siempre has estado ahí en los buenos y malos momentos. Te amo.

A Claudia, mi hermana, eres un ejemplo a seguir y si a alguien le debo este éxito es a ti, tú siempre creíste en mí y me ayudaste a salir adelante en los momentos difíciles. Gracias por hacerme una persona fuerte y capaz de creer que todo lo que me proponga siempre lo lograré, te amo hermanita.

A mi tutor de tesis, Jesús Gallegos Olvera un pilar en mi formación como internacionalista, gran profesor, excelente persona y sobre todo un buen amigo, Gracias por los consejos, las enseñanzas y porque no, las llamadas de atención que me motivan a ser mejor día con día. Eres alguien a quien admiro, respeto y le tengo un gran cariño. Sabes que agradezco infinitamente la confianza que depositas en mí.

Al Dr. José Luis Orozco Alcántar, cuya calidad humana es incomparable, más que un profesor es un guía, siempre tiene las palabras correctas que se traducen en sabios consejos que transmite a diario. Gracias por brindarme la oportunidad de pertenecer a su equipo de trabajo y encontrar en “el cubo” a grandes amigos. Me hacen falta palabras para mostrarle mi cariño y respeto.

A mis sinodales, el Dr. Héctor Zamitiz Gamboa, por su atención, tiempo y quien acompañado de un café me hizo reflexionar y enriquecer este trabajo, por recordarme que aún falta mucho por aprender. A la Dra. Ismene Bras, que esta tesis me ha permitido conocerla aún más, por enseñarme que lo “ciber” siempre será un tema complejo, por brindarme su conocimiento y apoyo durante este proceso. Por último pero no menos importante al Dr. Moisés Garduño García, quien enriqueció con sus comentarios esta tesis, quien compartió conmigo sus conocimientos y experiencia en Medio Oriente y por hacerme ver que el camino es difícil, pero lleno de satisfacciones.

A María Ledesma, mi amiga incondicional, con quien siempre estaré agradecido por motivarme a arriesgarme y a salir adelante, eres un ejemplo de perseverancia esfuerzo y comprensión, gracias por todas esas aventuras que he vivido a tu lado, más que una amiga, eres una hermana. Te quiero.

A Daniela Águila, una amiga que siempre ha creído en mí y me ha dicho que siempre vendrán cosas mejores, por su confianza y cariño, con quien sé que cuento a pesar de la distancia. Te quiero Dano.

Al equipo del “Cubo”, compañeros que hoy en día puedo llamar amigos. Dani, una amiga que la vida puso en mi camino con objetivos y metas en común, a quien admiro y de quien siempre aprendo, aunque tu mente maquiavélica me da miedo. Gracias por correr (literal) conmigo a la par en este proceso de titulación ¡Si se pudo!

Jenni una amiga que siempre te dirá las cosas como son y sin rodeos. He aprendido mucho de ti, tu compromiso y perseverancia que te caracterizan te harán llegar lejos Josué, quien iba a pensar que la persona que yo veía más seria y difícil, sería quien me recibiría con los brazos abiertos, eres una persona capaz, comprometida e inteligente gracias por aquellos consejos que me has brindado, por tu amistad y confianza. Mich, la última incorporación al “cubo” y quien en poco tiempo se ha convertido en una buena amiga, gracias por esas pláticas, trabajo en equipo y soporte que has brindado, sin duda eres alguien que llegará lejos.

Mención especial merecen mis amiguitos SPAMEX, con quienes viví tres meses en otro país, quienes se convirtieron en mi familia, quienes me vieron reír, llorar, caer y levantar.

Andy, una amiga que cuyo espíritu luchador y explorador siempre se contagia, Sergio, aquel amigo con quien siempre me quejaba de lo que me molestaba y que resulta que a él también le molestaba lo mismo. Yen, esa amiga quien siempre nos hacía volver a la realidad y que nos traía en cintura. Sandy, una amiga dulce y sincera, quien me hizo conocer una amistad pura.

Naye, gracias por tus consejos, tu sabiduría, sencillez, motivación y apoyo, tu amistad es invaluable. Paz, un amigo entusiasta e inteligente, por ser un gran compañero de aventuras y que siempre me hacía ver lo positivo o negativo de cualquier acción.

Cesar, agradezco infinitamente que la vida me haya puesto a un amigo como tú durante este viaje, gracias por siempre tener las palabras exactas para hacerme sentir bien en los momentos de desesperación. Anibal, amigo y cómplice, gracias por esos momentos de risa, enojo y susto, en ti encontré a una persona dedicada y entregada de la cual aprendí día con día. Jessica, que te digo que no sepas, eres una mujer increíble que doy gracias a la vida por haber conocido, te convertiste en una persona muy especial y que junto con Anibal somos los tres mosqueteros, gracias por estar ahí en los momentos buenos, pero sobretodo en los difíciles, por las largas pláticas de reflexión que teníamos en mi cuarto y por preocuparnos sobre qué pasaría cuando volviéramos.

Gracias amiguitos SPAMEX por formar parte de esta etapa.

Agradezco también a mis compañeros de licenciatura, con quienes conviví por cuatro años y medio. A quienes fueron parte de ese proceso por un tiempo, infinitas gracias por su compañía.

Agradezco al Programa de Apoyo a proyectos de investigación e Innovación Tecnológica (PAPIIT) de la UNAM IN 306414 “El establishment estadounidense y su política exterior en el siglo XXI”, dirigido por el Dr. Orozco.

A mi segunda casa, la Facultad de Ciencias Políticas y sociales, por permitirme formarme en sus aulas, un honor pertenecer a esta Facultad.

“Por mi raza hablara el espíritu”

A mi Alma Máter, la UNAM, esa casa de estudios de la que estoy orgulloso de pertenecer, me siento afortunado por tener la dicha de pertenecer a la máxima casa de estudios, por poder reflexionar, para proponer una solución, gracias por formar excelentes estudiantes.

¡México, pumas, universidad!

ÍNDICE

Índice de siglas.....	1
Índice de tablas, esquemas, imágenes, mapas y gráficas.....	2
Introducción.....	3
Capítulo I. Marco teórico-conceptual sobre la ciberseguridad y los crímenes cibernéticos.....	14
1.1. Los conceptos clásicos dentro de las Ciencias Sociales y las Relaciones Internacionales: seguridad y guerra.....	15
1.1.1. De la seguridad tradicional a la ciberseguridad.....	15
1.1.2. Guerra: de las guerras tradicionales a la ciberguerra	21
1.2. La Teoría de la Globalización: explicación del Tecnoutopismo y Cybergeddon.....	26
1.3. El ciberespacio: nuevo campo de batalla.....	34
1.4. Concepto de ciberseguridad o seguridad informática y diferenciación con seguridad de la información.....	35
1.5. Tipología y categorización de los crímenes cibernéticos.....	40
1.5.1. Cibercrimen.....	40
1.5.2. Ciberguerra.....	44
1.5.3. Ciberguerrero.....	48
1.5.4. Ciberespionaje.....	49
1.5.5. Ciberterrorismo.....	50
1.5.6. Ciberactivismo y Hacktivismo	52
1.5.7. Ciberataque.....	53
1.5.8. Categorización de los ciberataques.....	55
1.6. Antecedentes de ataques cibernéticos alrededor del mundo.....	57
1.7. Balance crítico respecto a las diferencias entre ciberseguridad y ciberdefensa.....	60

Capítulo II. Ciberseguridad en Estados Unidos:

¿Un tema nuevo en su agenda?..... 62

2.1. La evolución de la ciberseguridad en EE.UU a través del tiempo..... 66

2.2. El rol de los actores no estatales en la ciberseguridad:
usuarios, empresas, hackers y crackers.....77

2.3. Barack Obama y las acciones llevadas
a cabo en materia de ciberseguridad..... 89

2.4. Hacia una ciberresiliencia..... 92

Capítulo III. El caso de Irán en 2010 como referente

de una posible ciberguerra y sus repercusiones en

la seguridad informática..... 101

3.1. La importancia geopolítica de Irán dentro del conflicto..... 102

3.2. Irán como parte de Medio Oriente y las riquezas con las que cuenta.
Infraestructura crítica: El programa nuclear iraní..... 104

3.3. La Operación Juegos Olímpicos..... 119

3.4. Las “nuevas armas” utilizadas en el conflicto:
Stuxnet, Duqu, y Flame. Sus consecuencias al ser utilizadas
en los ordenadores de infraestructuras críticas..... 126

Conclusiones..... 131

Fuentes de consulta..... 140

ÍNDICE DE SIGLAS Y ABREVIATURAS

ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
FBI	Federal Bureau Institute
ICANN	Internet Corporation for Assigned Names and Numbers
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
KGB	Komitet Gosudárstvennoy Bezopásnosti
OIEA	Organismo Internacional de Energía Atómica
PNI	Programa Nuclear Iraní
QDR	Quadriennial Defense Review
SDI	Strategic Defence Initiative
TCP	Transmission Control Protocol
TIC	Tecnologías de la información y Comunicación
UIT	Unión Internacional de Telecomunicaciones
UNODC	United Nations Office on Drugs and Crime
USCYBERCOM	United States Computen Emergency Readness Team

Índice de tablas, esquemas, imágenes, mapas y gráficas

Tablas

Tabla 1. Tipos de globalización.....	29
Tabla 2. Cinco ciberfuturos.....	33
Tabla 3. Categorización de los ciberataques.....	56
Tabla 4. Principales ciberataques a nivel mundial.....	60
Tabla 5. Funcionamiento de las centrales nucleares en Irán.....	116

Esquemas

Esquema 1. Planos de acción en la seguridad informática.....	39
Esquema 2. Características actuales de la ciberguerra.....	47
Esquema 3. Ocho maneras de ataque hechas por los ciberterroristas.....	52
Esquema 4. Línea del tiempo.....	65
Esquema 5. El proceso de la Operación Juegos Olímpicos.....	125

Imágenes

Imagen 1. Boceto inicial de ARPANET	68
Imagen 2. ARPANET en 1971.....	69
Imagen 3. Ciberataques a Estados Unidos.....	97

Mapas

Mapa 1. Ubicación Geográfica de Irán.....	104
Mapa 2. Los recursos naturales de Irán	105
Mapa 3. Centrales Nucleares existentes en Irán	114

Mapa 4. Foto satelital de la planta nuclear de QOM.....	116
Mapa 5. Foto satelital de la planta nuclear de Busherh	117
Mapa 6. Foto satelital de la planta nuclear de Isfahán.	117
Mapa 7. .Foto satelital de la planta nuclear de Natanz.....	118
Mapa 8. Foto satelital de la planta nuclear de Arak.....	118

Gráficas

Gráfica 1. Incremento de los cibercrimenes a nivel mundial en el año 2013.....	42
Gráfica 2. Enfoques criminales hacia una criminalización del cibercrimen.....	42
Gráfica 3. Frecuencia relativa de los reportes globales de noticias.....	44
Gráfica 4. Los 10 países con mayores ataques DDoS durante el primer trimestre de 2016.....	94
Gráfica 5. Mes y día del año del 2016 en los cuales se registraron mayor cantidad de ciberataques.....	95
Gráfica 6. Principales proveedores de botnets a nivel mundial.....	96

Introducción

La sociedad internacional enfrenta nuevos retos y amenazas que se han ido desarrollado con el paso del tiempo. Nuevos campos de batalla surgen para crear nuevas formas de interacción entre Estados ya sea de forma positiva o negativa.

Es a raíz de ello y en los últimos años que el prefijo “ciber” se ha popularizado con el objetivo de describir todo lo que sucede dentro del ciberespacio, es decir, del entorno virtual que se ha desarrollado gracias a las Tecnologías de la Información y Comunicación (TIC) y que se extiende por todo el mundo, que no tiene fronteras, que no es capaz de gobernarse y que debido a ello, suele ser el lugar ideal para cometer un crimen.

Por lo anterior, surge el término “cibercultura”, el cual se refiere a esa importancia que el ser humano le ha dado al ciberespacio. En palabras de Pierre Lévy¹ la cibercultura es entendida como “el conjunto de técnicas, de maneras de hacer, de maneras de ser, de valores, de representaciones que están relacionadas con la extensión del ciberespacio.”²

Jaime Alejandro Rodríguez³ estudia la inserción de lo “ciber” en la vida diaria y define a la cibercultura como

“una serie de fenómenos culturales contemporáneos ligados principal, aunque no únicamente, al profundo impacto que han venido ejerciendo las tecnologías digitales de la información y la comunicación sobre aspectos tales como la realidad, el espacio, el tiempo, el hombre mismo y sus relaciones sociales.”⁴

Rodríguez nos proporciona un elemento importante a considerar, que es el cómo los medios digitales han influido en las relaciones sociales que entabla el hombre, ello también ha provocado que estas nuevas formas de interacción lleguen a ser

¹ Escritor, filósofo, y profesor tunecino quien actualmente es profesor en el Departamento de Comunicación de la Universidad de Ottawa

² Lévy Pierre, *“CIBERCULTURA Informe al Consejo de Europa”*, Editorial Anthropos, Barcelona, 2007, pág. 18

³ Catedrático de la Universidad Nacional de Educación a Distancia (UNED) en España

⁴ Rodríguez Ruiz Jaime Alejandro, *“Trece motivos para hablar de cibercultura”*, Editorial Libros de Arena, España, 2004, pág. 31.

dañinas para la sociedad, la profesionalización de los criminales y su inducción a las TIC ha producido que conceptos tradicionales como terrorismo, espionaje, ataque, guerra y seguridad, contengan el prefijo “ciber” y comencemos a hablar de cibercrimenes, ciberataques, ciberguerras, ciberterrorismo, ciberespionaje, etc., ocasionando que los Estados comiencen a preocuparse por este nuevo fenómeno y que busquen la manera de evitarlo o erradicarlo.

Lo antes mencionado ocurre en un nuevo “lugar” que se une a los cuatro espacios tradicionales (territorial, marítimo, aéreo y exterior), hablamos del ciberespacio. Es gracias a este nuevo espacio que el usuario adquiere el don de la ubicuidad, es decir, “está en todos los lugares en los que hay un ordenador, un procesador o un cable que conecta con uno.”⁵

Según Richard Clarke, “el ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan.”⁶ En él surgen nuevas dinámicas de interacción, lo “ciber” comienza a tomar relevancia en las agendas internacionales de los países., surge un nuevo tipo de armamento, un nuevo tipo de seguridad y una nueva forma de guerra.

Entonces el ciberespacio es aquel lugar en donde suceden las nuevas dinámicas de interacción del ser humano, pero también donde se desarrollarán los conflictos no solo de ciberguerra o ciberataques, sino también de ciberespionaje o filtración de información, que tendrán un impacto en la sociedad internacional. Algunos de ellos han sido:

Wikileaks: Esta organización fundada por Julian Assange, un programador y periodista australiano, filtra en noviembre del 2010 más de 250.000 documentos diplomáticos del Gobierno de Estados Unidos a través de cinco medios: *The New York Times*, *The Guardian*, *Der Spiegel*, *Le Monde* y *El País*, en algunos de estos documentos el gobierno estadounidense da indicaciones a sus diplomáticos para que espíen a políticos extranjeros y altos funcionarios de la ONU.

⁵ Clarke A. Richard, Knake K. Robert (traducción de Noriega Luis Alfonso), “*Guerra en la red: Los nuevos campos de batalla*”, Editorial Ariel, Barcelona, 2011, pág. 103.

⁶ Ídem

Un mes más tarde, Assange es arrestado por coerción, dos cargos de abuso sexual y uno de violación, todos supuestamente cometidos en agosto de 2010 en Suiza.

Palestine Papers: Del 23 al 26 de enero de 2011 Al-Yazira en colaboración con The Guardian, revelaron cerca de 1.600 documentos secretos de las negociaciones palestino-israelíes. Estos acusaban abiertamente a la Autoridad Palestina de no velar por los derechos del pueblo palestino, esto debido a la disposición a cumplir, sin negociación alguna, lo que el pueblo israelí solicitara a expensas del pueblo palestino. Uno de los documentos filtrados señalaba que Saeb Erekat, quien en ese entonces era llamado el “Negociador-Jefe”, cedió la mayor parte de la Jerusalén Oriental Ocupada sin una negociación de por medio.

Asimismo, los *Palestine Papers* confirman el acuerdo de ambas partes respecto a la repatriación del pueblo palestino,

“Un resumen de una reunión celebrada en agosto de 2008 indicaba que Israel había hecho una oferta de intercambio de tierras que garantizaba que la mayoría de los ilegales colonos judíos permanecieran en la ocupada Cisjordania. Incluía una propuesta del entonces Primer Ministro Ehud Olmert para permitir que un total de 5.000 refugiados palestinos (de los casi seis millones) regresaran a sus hogares en el transcurso de cinco años.”⁷

Los *Palestine Papers* demostraban la poca capacidad de negociación que tenían las autoridades de la Autoridad Palestina, al no exigir ni velar por los derechos palestinos, preservar la integridad nacional del mismo pueblo y la integridad territorial de un estado palestino.

PRISM: El 5 de julio del 2013, Estados Unidos se vería envuelto en un escándalo: Edward Snowden, un consultor tecnológico estadounidense ex agente de la CIA y de la NSA reveló una serie de notas en las que aseguraba que el gobierno estadounidense vigilaba las comunicaciones de todo el mundo, a través de datos recabados directamente de los servidores de Microsoft, Yahoo, Google,

⁷ Baround Ramzy, “Los Papeles de Palestina: Entregando Palestina”, Febrero 2011, en línea, dirección URL: <http://bit.ly/2j7SFM5>, consultado el 10 de enero del 2017.

Facebook, PaITalk, AOL, Skype, YouTube y Apple, mediante un programa de nombre PRISM.

“En otra arista del escándalo surgido a raíz de las revelaciones de Snowden, la prensa británica acudo al Primer Ministro David Cameron de estar detrás de presiones al diario *The Guardian*, que junto con *The Washington Post* fueron contactados por Snowden para revelar la existencia de PRISM.”⁸

PRISM, es capaz de obtener historial de búsquedas, contenido de correos electrónicos, transferencia de archivos, chats, fotografías, videoconferencias o registros de conexiones.

Ante el descontento internacional por este suceso, el gobierno estadounidense no tuvo más que aceptar la existencia de este programa alegando que lo hacían por la seguridad del pueblo estadounidense al interior y al exterior, asegurando que las empresas implicadas tenían el completo conocimiento de PRISM (aunque Apple, Microsoft, Yahoo, entre otras aseguraban lo contrario).

La mirada internacional debatía sobre el modo en el que Estados Unidos “recababa” información a través de la red, generando nuevamente, una desconfianza en el ciberespacio.

Panamá Papers: Se trata de la filtración de más de 11 millones de documentos de la firma panameña Mossack Fonseca y en la cual figuran nombres de presidentes, ex presidentes, deportistas, artistas, entre otros y que habrían cometido evasión fiscal a través de offshores⁹. Fue impulsada por el Consorcio Internacional de Periodistas de Investigación (ICIJ, en inglés) y por el diario alemán *Süddeutsche Zeitung* el 3 de abril de 2016. Nombres como el de Mauricio Macri, Vladimir Putin, el rey de Arabia Saudí, Salmán bin Abdulaziz, y el padre del primer ministro británico, Ian Cameron, entre otros más, se vieron involucrados en este escándalo.

⁸ Orozco José Luis, Gallegos Olvera Jesús (coord.), *“El establishment estadounidense y su política exterior”*, artículo de Zamitiz Gamboa Héctor, *“Vigilancia electrónica y defensa del interés público”*, Ediciones del lirio, Ciudad de México, 2016, pág. 169.

⁹Se refiere a empresas o sociedades constituidas fuera del país de residencia para evitar pagar impuestos.

Bahamas Papers: El 21 de septiembre de 2016 se suscitó una misma situación que Panamá papers. Fue la filtración de información de, aproximadamente, 175.000 compañías offshore constituidas en las islas Bahamas con dueños de todas partes del mundo, además de ser sociedades inactivas desde hace varios años. Estos documentos de compañías, fondos y fundaciones se encuentran en este paraíso fiscal desde 1990 y hasta 2016.

Los casos anteriores ejemplifican la filtración de información con el fin de “dar a conocer” los malos manejos que las empresas hacen, y como se ha visto, estas filtraciones afectan la imagen de aquellas personas que son relacionadas con ellas. Tal es el caso de Hillary Clinton, ex candidata demócrata a la presidencia de Estados Unidos quien en plena campaña sufrió una filtración, por parte de Wikileaks, de correos electrónicos que contenían secreto de Estado, mientras ejercía su cargo como Secretaria de Estado. La polémica radica que esos correos contenían información "secreta", que no fue clasificada como tal cuando fue enviada.

Todo inició en 2015, cuando se le solicitó a Hillary Clinton entregar al FBI su cuenta personal de correo electrónico, la cual, había utilizado para enviar información relativa a asuntos de interés nacional estadounidense.

Es importante señalar que esto fue usado en su contra durante su campaña presidencial, sus principales opositores señalaban que ella no era lo suficientemente competente para ocupar el cargo de presidente, incluso el tema de los correos electrónicos fue una constante en los tres debates que tuvo con el ahora presidente Donald Trump, y que incluso, puede tomarse en cuenta como un factor que impidió que ganara la presidencia, aun siendo la favorita, debido a la desconfianza que generó en la población estadounidense

Lo expuesto anteriormente demuestra que un Estado y sus habitantes deben estar preparados ante situaciones inesperadas que ocurran en el ciberespacio, de ahí la importancia del estudio de la ciberseguridad y ciberguerra, la cual radica en hacer un análisis detallado de la evolución de los términos

tradicionales de guerra y seguridad ante un orden internacional que en el siglo XXI demuestran ser cambiantes en un contexto de globalización y surge un cambio en la concepción de ambos términos para renombrarlos y adaptarlos a la nueva realidad internacional que se vive, además de estudiar los logros y consecuencias que se han tenido en materia de ciberseguridad.

Dentro de las ciencias sociales es común la utilización de los términos de seguridad y guerra, para referirse al Estado. El debate en torno a estos conceptos es muy variado, los límites que estos deben alcanzar así como las consecuencias que tengan dentro de la sociedad.

Tradicionalmente, suele verse a la seguridad como aquel estado en donde el Estado está ausente de cualquier amenaza, usualmente esta se provee mediante recursos militares. Pero la seguridad no solo se queda ahí, ya que dentro de las ciencias sociales los estudios de seguridad abarcan diversas esferas que afectan al Estado, incluida la población. Por otra parte, la noción de guerra tradicional hace referencia a aquel conflicto armado, o no, que se da entre dos Estados o grupos de Estados.

Es así que el argumento principal de este trabajo asegura que la ciberseguridad toma mayor relevancia en la agenda internacional y nacional de los Estados Unidos a partir del año 2010 debido a la Operación Juegos Olímpicos, mediante la cual este país ataca a las centrales nucleares del Programa Nuclear de Irán, y, como consecuencia, el gobierno de Barack Obama incentivará y llevará a cabo nuevas acciones para protegerse y no ser víctima de las “nuevas” amenazas: los diversos ciberdelitos y los virus informáticos.

Si bien este ciberataque fue uno de los más representativos ante la sociedad internacional, no está (ni estará) reconocido por Estados Unidos, por ende, el motivo de este trabajo es presentar los elementos necesarios para considerar que EE.UU. desarrolló y ejecutó junto con Israel este virus y que en su momento ayudó a frenar a lo que ellos consideraban una de sus principales amenazas, es decir, el desarrollo nuclear cada vez más evidente de Irán, y que

después de ello, aumentaron sus acciones en materia de ciberseguridad involucrando a más actores.

Es así que el objetivo principal de este trabajo es el analizar la estrategia de ciberseguridad que se implementó en el gobierno de Barack Obama a raíz del ciberataque al Programa Nuclear Iraní en 2010. Entonces, es propósito de esta tesis presentar y analizar las actividades que llevo a cabo el presidente Barack Obama durante sus dos administraciones en materia de ciberseguridad, y cómo fue que manejó la situación posterior a este ataque, además de mostrar las alianzas que hizo con el sector empresarial.

Este ataque que en principio ordenó Bush y que Obama ejecutó, tuvo un gran impacto político y económico, que mostraban a un Barack Obama rígido y dispuesto a eliminar al enemigo (el ser), contrario a las promesas de campaña que había establecido, donde señalaba que no tenía políticas rígidas (deber ser).

Como primer objetivo y que ayudará a esclarecer la tipología existente en cuanto a la ciberseguridad se refiere, es preciso diferenciar los diversos crímenes cibernéticos que son campo de estudio de la ciberseguridad. Asimismo, y de acuerdo a diversas definiciones (de académicos y organizaciones internacionales) se expondrá una definición propia del termino ciberseguridad.

El segundo objetivo específico de esta tesis es el presentar el proceso evolutivo de la ciberseguridad en Estados Unidos, mostrando que no es un tema nuevo en su agenda, además de analizar las medidas que Obama implementó. Por otra parte, también es necesario introducir el término que hace referencia a un ataque inminente en el ciberespacio y que ayudará a que haya un daño mínimo, este es la ciberresiliencia.

Un tercer objetivo es el analizar los intereses que tenía (y sigue teniendo) EE.UU hacia Irán y que incentivaron los ciberataques en contra del Programa Nuclear Iraní (PNI) en 2010.

Esta tesis recupera a la globalización como el enfoque teórico que analiza a la sociedad inmersa en una verdadera “aldea global” en la llamada “era de la tecnología”, donde la utilización de recursos informáticos es cada vez más necesaria para todos los gobiernos y sus habitantes. Además, es un recurso que se ha hecho indispensable para la vida y cuyo acceso cada vez es más abierto.

Esta vía a grandes redes informáticas garantiza a los países un mejor manejo de su información y a la vez mayor facilidad para distribuirla. Toda innovación tiene como consecuencia una limitante, es entonces, que la tecnología se va a convertir en un medio para el logro de los objetivos de los Estados y estos buscarán preservarlo a toda costa, creando “nuevas armas”, que son realmente económicas, para ampliar los límites tradicionales de seguridad. Todo ello ha dado pie a que comience a hablarse de “ciberseguridad o seguridad informática” de los Estados con el fin de evitar conflictos a gran escala.

El estudio de este “nuevo” conflicto pretende aportar elementos de estudio a las Relaciones Internacionales al catalogar a EE.UU. como una ciberpotencia que pretende determinar las reglas en el ciberespacio a nivel internacional, pero que, debido a un conflicto de intereses entre los Estados, no se puede llegar a un consenso mundial sobre como regular este conflicto, dejando las medidas estadounidenses en esta materia solo en el ámbito nacional.

En la actualidad existen elementos que pueden regular estas “nuevas reglas” dentro de lo que llamamos el “ciberespacio” es en este “lugar” donde se origina la “ciberguerra”, este nuevo conflicto utiliza armas o virus informáticos, Stuxnet, Duqu o Flame son los más conocidos y más dañinos. Prueba de lo anterior es el ataque que se da en 2010 en contra del Programa Nuclear Iraní, donde, Estados Unidos ataca la central del programa de enriquecimiento de uranio con un virus informático (Stuxnet) creando así un atraso en este programa.

Esto traerá, como consecuencia, la creación de nuevas estrategias, planes y tácticas en el gobierno estadounidense, con el fin de hacerle frente a este “nuevo” conflicto internacional.

Por ello, el gobierno de Obama se encargó de crear nuevas normas para regular el ciberespacio que es el nuevo escenario de conflicto, estas propuestas son un elemento importante a estudiar ya que va a generar ataques legítimos en contra de quien se considere una amenaza. Hay que considerar que incluso sus alcances puedan traer consigo pérdidas humanas, buscar una alternativa sobre el cómo abordar este conflicto es uno de los principales objetivos de esta investigación.

En el primer capítulo se abordará la concepción tradicional de seguridad y guerra, enunciando los postulados de Hobbes o Clausewitz, y con ello ver la transformación del término tradicional a lo que hoy en día se conoce como ciberseguridad. Asimismo, la teoría de la globalización permitirá explicar la constante comunicación que existe entre los usuarios del ciberespacio, rompiendo las barreras físicas y fronteras. Conceptos como sociedad del conocimiento, sociedad de la información, big data, internet de las cosas, entre otros hacen que la comunicación no encuentre barreras de tiempo y espacio, haciéndonos sentir en lo que Octavio Ianni llamará la aldea global.

Por último, se definirá a la ciberseguridad tomando en cuenta sus diferentes elementos, para finalmente crear un nuevo concepto que englobe las características antes mencionadas y los riesgos que hay en el ciberespacio y se definirán los diversos crímenes cibernéticos que existen a nivel internacional, categorizándolas como ciberamenazas, además se realizará un breve recorrido de los diversos ciberataques que han surgido a lo largo de los años.

El segundo capítulo abordará el tema de ciberseguridad en la agenda política estadounidense, con un breve recorrido histórico se demostrará que realmente este no es un tema nuevo y que incluso ha estado en discusión desde finales de la Segunda Guerra Mundial.

Se realizará un análisis del papel de los actores no estatales dentro del proceso de ciberseguridad con el fin de explicar la actual cooperación triangular

(estado- empresas- civiles) de los actores dentro de la ciberestrategia estadounidense.

Se abordará un concepto relativamente nuevo dentro del proceso de ciberseguridad: la ciberresiliencia, la cual permitirá al Estado tener mejores respuestas ante un posible ciberataque que resulte inminente. Si bien la ciberresiliencia se encargará de minimizar los impactos de un ataque este no se enfocará en prevenirlos.

En el último capítulo, se analiza el ciberconflicto Irán- Estados Unidos, esto como un referente de ciberguerra entre dos potencias, además de que este suceso representa una convergencia de intereses de Estados Unidos ante el inminente desarrollo nuclear que Irán estaba presentando en 2010.

Para entender las repercusiones de esta Operación, finalmente se analizará el impacto de las ciberarmas en las infraestructuras críticas, hablamos de Stuxnet, Duqu y Flame. Estas tres “armas” resultaron realmente efectivas ya que lograron su objetivo principal: retrasar al PNI, si bien cada uno de estos virus es diferente y tiene propósitos diferentes que se analizarán en este último apartado, es necesario hacer mención que son parte de la misma Operación Juegos Olímpicos. Y que el lanzamiento de cada uno de ellos correspondería a un objetivo diferente y a una temporalidad diferente, desafortunadamente para Irán estas tres ciberarmas iban destinados a su gobierno.

Asimismo, se expondrá el peligro que representaría el uso de estas armas en otro tipo de infraestructuras críticas, en empresas, o en una red doméstica. Este peligro crea una necesidad en los actores involucrados, una necesidad de estar alerta ante un mundo en donde es cada vez más fácil tener acceso al ciberespacio. Y en un mundo que aún no tiene ley y que no la tendrá.

CAPÍTULO I. Marco teórico-conceptual sobre la ciberseguridad y los crímenes cibernéticos.

Sabemos que los hackers roban la identidad de las personas y se infiltran en los correos privados. Sabemos que países extranjeros y empresas roban nuestros secretos corporativos. Ahora nuestros enemigos también están buscando obtener la habilidad de sabotear nuestra red eléctrica, nuestras instituciones financieras y nuestros sistemas de control aéreo. No podemos mirar hacia atrás en el futuro y preguntarnos por qué no hicimos nada ante las amenazas reales a nuestra seguridad y economía¹⁰

Barack Obama, durante la firma del “Decreto de ciberseguridad para enfrentar los ciberataques en los Estados Unidos”, 2014.

En menos de dos décadas internet pasó por un proceso de transformación en el cual pasó de ser un recurso militar a algo cotidiano para el ser humano, ya que, prácticamente más de la mitad de la población tiene acceso a él, ya sea a través de su dispositivo móvil, computadora de escritorio o portátil e incluso desde una consola de videojuegos, es decir, en la actualidad es utilizado para ambos fines, civiles o militares.

El ciberespacio se convierte en el medio por el cual viajan nuestros datos y nos comunicamos, donde el usuario encuentra una distracción en un rato libre, busca información, realiza diversas operaciones como comprar o realizar pagos, entre muchas cosas más. Esto es aprovechado por algunos individuos, incluso por gobiernos, para crear nuevas maneras de ataque al enemigo y utilizan al ciberespacio, un “lugar” atípico, cuya regulación a nivel internacional aún está en proceso y que es de fácil de acceso, con el objetivo de realizar un ataque y con ello debilitar al oponente, pero ¿cómo se llegó a este punto?

Este primer capítulo, tiene por objetivo desarrollar el concepto de ciberseguridad y ciberguerra a partir de los conceptos tradicionales de seguridad y guerra, además de analizar con un marco teórico-conceptual los diferentes

¹⁰ Casa Blanca, discurso emitido por el presidente de los Estados Unidos, Barack Obama, durante la firma del “Decreto de ciberseguridad para enfrentar los ciberataques en los Estados Unidos” el 13 de febrero del 2014, en línea; <http://bit.ly/1QtYqS4>, consultado el 23 de agosto del 2014.

crímenes cibernéticos que existen a nivel internacional, ya que desafortunadamente, existe confusión de conceptos entre autores de distintas publicaciones y textos, incluidos los que provienen de fuentes oficiales.

1.1. Los conceptos clásicos dentro de las Ciencias Sociales y las Relaciones Internacionales: seguridad y guerra

Usar conceptos tradicionales como seguridad y guerra ayudará a identificar claramente dónde surge la transformación de un concepto a otro, cómo se incorpora lo “ciber” a las agendas de seguridad y defensa de los Estados y cómo la globalización de las tecnologías las han colocado dentro de los nuevos temas de las Relaciones Internacionales a través de la creación de nuevos conceptos que dan explicación al fenómeno.

1.1.1. De la seguridad tradicional a la ciberseguridad

Dentro de las Relaciones Internacionales, el concepto de seguridad estaba únicamente relacionado con la defensa del Estado y su integridad territorial frente a otro que lo amenazara mediante instrumentos militares. La seguridad, entonces, dependía sobre todo de la capacidad del Estado de mantener, aumentar y utilizar el poder militar.

Es por esto que la seguridad tradicional estaba únicamente ligada a los Estados. Etimológicamente la palabra seguridad (*securitas* o *securus*) significa: “*estar libre de preocupaciones o problemas*”¹¹. En el marco de los debates de las Ciencias Sociales, un autor que nos presenta una definición filosófica del término es Thomas Hobbes. Quien nos señala que: “El Leviatán (El estado) tiene la tarea de preservar la integridad de sus ciudadanos y de librar al individuo de las incertidumbres de la naturaleza anárquica del mundo”¹². Hobbes nos deja en claro que la seguridad no solo se dará en la protección de la existencia física del Estado, y, por lo tanto, amplía el concepto a nivel social, y esto permitirá a la humanidad disfrutar de una vida libre de amenazas.

¹¹ Diccionario Enciclopédico Usual Larousse (2012), México D.F., México Larousse

¹² Fragmento encontrado en: Orozco Gabriel, “*El concepto de la seguridad en la Teoría de las Relaciones Internacionales*”, en línea, Barcelona Revista CIDOB d’Afers Internacionals, núm. 72, p. 161-180, dirección URL: <http://bit.ly/1QOwkW5>, consultado el 27 de agosto del 2014

Asimismo, realiza una distinción del grado de seguridad de un Estado a nivel interno y externo, considera a la guerra como una extensión de la seguridad y la única manera de poder contenerlo es que el mismo hombre sea quien mediante voluntad propia lo haga; ello a través de un pacto voluntario, por el cual los individuos transfieren

“[...] la libertad que cada hombre tiene de usar su propio poder, como él quiera, para la preservación de su propia naturaleza, es decir, de su propia vida y, por consiguiente, de hacer toda cosa que en su propio juicio y razón, conciba como el medio más apto para aquello” a un hombre o asamblea de hombres con el fin de “erigir un poder común capaz de defenderlos de la invasión extranjera (seguridad externa) y las injurias de unos a otros (seguridad interna).¹³”

El poder del Estado se funda en el contrato y su único fin es la defensa, es decir, la seguridad y la paz interior, “La causa final, meta o designio de los hombres (que aman naturalmente la libertad y el dominio sobre otros) al introducir entre ellos esa restricción de la vida en repúblicas es cuidar de su propia preservación y conseguir una vida más dichosa.¹⁴”

La ciberseguridad la explico a través de Hobbes mediante la seguridad externa, en la cual, el Estado puede hacer valido su poder para defenderse de la invasión extranjera esto a través de todos los medios posibles (en este caso, el ciberespacio).

El ejemplo claro de una batalla tradicional entre dos Estados es la Guerra Fría la cual, es vista como un equilibrio entre “dos grandes“, parafraseando a Raymond Aron, uno de los principales representantes de esta escuela. Este conflicto se caracteriza desde una influencia completamente militar. Posterior a la Segunda Guerra Mundial, inicia un proceso de crisis y después de ruptura que se en 1947 con la doctrina Truman y su lucha contra el comunismo, este conflicto se convierte en una lucha no solo política, y económica sino también ideológica entre los dos polos de poder. A partir de este punto, comienza un periodo que dura 40 años, marcado por diversas etapas del conflicto, como por ejemplo, el que se

¹³ Hobbes, Tomas, “*El Leviatán*”, Madrid, Editora Nacional, 1979, p. 228.

¹⁴ *Ibidem* pág. 227

produce en 1962 y que se conoce con el nombre de “crisis de los misiles”, entre otros.

Raymond Aron analizó la Guerra Fría en su libro *La República Imperial* desde sus comienzos hasta 1972. En el que define a este enfrentamiento como: “[...] el estado de las relaciones entre Dos Grandes, lo único que permite distinguir las fases de la diplomacia estadounidense, por la simple razón de que sus responsables, al menos conscientemente, pensaban en sus acciones y en el mundo todo por referencia al peligro comunista.¹⁵” Esto lo convertía en una “guerra, ya que los diplomáticos no podían ni querían arreglar sus diferencias mediante negociaciones; fría, ya que no querían ni podían arreglarlos por la fuerza.¹⁶”

Alguien más que analiza este periodo es, John Gaddis donde analiza a Estados Unidos y los orígenes de la Guerra Fría 1941-1947. Estos dos autores llegan a la conclusión realista en analizar cuál fue el momento de la ruptura entre Estados Unidos y la Unión Soviética, y marcan como punto de inflexión los hechos transcurridos tras el fin de la Segunda Guerra Mundial. Franklin D. Roosevelt trató de llegar a un consenso con la ex Unión Soviética. “Para Aron el actuar del norteamericano estuvo centrada en la idea de continuidad con el legalismo y universalismo wilsonianos.

En contraposición, Gaddis opina que su accionar respondió al afán de cumplir el “gran designio” de Estados Unidos, ya que la cooperación militar con Rusia era vital para garantizar la paz de posguerra. Otro punto de coincidencia reside en lo que ellos creen que fue el motivo de la ruptura entre ambas potencias. Se centran en las diferencias en los intereses territoriales y económicos, además del factor ideológico.¹⁷”

¹⁵ Aron, Raymond, *“La república imperial”*, Editorial Emecé, Buenos Aires, Argentina, 1974. p. 42

¹⁶ *Ibidem* pág. 48

¹⁷ Delicia Zurita, María, *“La guerra Fría desde la óptica de las Relaciones Internacionales”*, Universidad Nacional de La Plata (Argentina), 2007, en línea; <http://bit.ly/1QVKtyu>, consultado el 29 de agosto del 2014

Sin embargo, el accionar de la URSS en Europa Oriental durante 1945, junto con el cambio de táctica del comunismo internacional, hicieron que Estados Unidos, a principios de 1946, comenzara a ver a su antiguo aliado como un potencial enemigo el cual tenía como fin, un programa de expansionismo ilimitado que amenazaba a Estados Unidos. Esta política de endurecimiento con Moscú tuvo se vio reflejada en la doctrina Truman, en 1947, donde se declara formalmente la Guerra Fría.

Analizando esto, ambas potencias querían la paz, pero las fuertes influencias externas llevaron a que la concibieran de una forma contradictoria. Es por eso que la Guerra Fría fue el resultado de una irónica paradoja, ya que las búsquedas simultáneas de paz condujeron a lo que no se deseaba, la bipolaridad. Fueron los objetivos políticos divergentes los que sepultaron cualquier intento de consolidar la alianza entre los Estados Unidos y la Unión Soviética.

Por otro lado, Joseph Nye coincide con Aron y Gaddis en ver a la bipolaridad como un sistema de equilibrio de poder. “Si bien antes había existido equilibrios en los cuales las alianzas se concentraban alrededor de dos Estados... nunca dos países habían estado a tal punto por encima del resto en términos de sus propios recursos de poder.”¹⁸

Al final, Nye realiza una aportación importante, el papel de Estados Unidos tras la Segunda Guerra Mundial, al afirmar que este país “[...] no buscó un imperio territorial o una hegemonía que mantuviera a las naciones perdedoras de la conflagración de 1945 en posiciones serviles. Por el contrario, estimuló su revitalización económica y su asociación estratégica para equilibrar el poderío soviético.”¹⁹

Es en este conflicto, donde surge un punto de referencia de la ciberseguridad, en el auge de la guerra fría, Estados Unidos inventa una red exclusivamente militar, con el objetivo de tener acceso a la información militar desde cualquier punto del país en caso de un ataque de la ex Unión Soviética, “El

¹⁸ Nye, Joseph. “*La naturaleza cambiante del poder norteamericano*”. Buenos Aires. GEL. 1991. p. 75.

¹⁹ *Ibidem* pág. 27

origen de Internet se remonta a 1969, cuando la Agencia de Proyectos para la Investigación Avanzada de Estados Unidos, ARPA, conectó cuatro sistemas distantes en una red que se denominó ARPANET, cuya misión era mantener las comunicaciones en caso de guerra²⁰.

ARPA surge como una agencia dependiente del Departamento de Defensa de Estados Unidos, surgió en 1958 y su fin era desarrollar proyectos de tecnología militar en plena Guerra Fría. EE.UU. quería contrarrestar los avances de la antigua URSS. En el capítulo 2 se ahondará más a fondo sobre el papel de ARPA en Estados Unidos.

Posterior a la Guerra Fría los niveles de análisis de la seguridad se ampliaron. Otra alternativa debía ofrecernos muchas más dimensiones de estudio dentro de la seguridad. En otras palabras, además de la seguridad nacional e internacional, era necesario estudiar los componentes de estas mismas.

Como consecuencia de la globalización, las amenazas dejan de poseer un carácter militar, ampliando el concepto de seguridad. Nuevos desafíos globales, transfronterizos en su mayoría, como el crimen organizado, el terrorismo, el cambio climático, guerras derivadas por los recursos naturales, los refugiados, la inmigración no regulada, la pobreza y el hambre se convirtieron en riesgos para la humanidad de una de gran importancia incluso al mismo nivel que los riesgos a nivel militar. Debido esto, surgió la necesidad de ampliar el concepto de seguridad de manera multidimensional y a distintos niveles, y que dejan de lado la defensa militar y la protección del Estados (territorio).

Es por esto, que en la década de los 80 florecieron debates académicos y políticos, en torno a la seguridad, se establecieron diversas comisiones cuyo objetivo era incorporar en la agenda de seguridad mundial y estatal, los nuevos problemas que surgían, algunas de estas comisiones son:

²⁰ Rtve.es *"Internet nació de un proyecto militar de Estados Unidos en la Guerra Fría"*, en línea, <http://bit.ly/1TbehaH>, consultado el 28 de agosto del 2014.

- Comisión Independiente sobre Problemas Internacionales de Desarrollo (Brandt): *“Promovía una estrategia basada en las personas y apoyaba firmemente el fortalecimiento de la democracia y el arresto del autoritarismo, de la corrupción y de la militarización²¹”*. Propuesta a finales de los años 80 por el ex-Presidente de Tanzania, Julius Nyerere
- Comisión Independiente sobre Asuntos de Desarme y Seguridad (Palme): *“que trató los problemas de la seguridad y de la amenaza de una nueva guerra nuclear. La Comisión Palme fomentó la concepción nueva de “seguridad común²²”*. Propuesta en 1980 por el entonces Primer Ministro de Suecia, Olof Palme
- Comisión Mundial sobre Medio Ambiente y Desarrollo (Brundtland): *“tratar de solucionar los crecientes problemas de la situación global del medioambiente²³”* Propuesta en 1987 por Gro Harlem Brundtland.

Entre las contribuciones más relevantes a la redefinición de la seguridad, destaca la *Escuela de Copenhague²⁴*, que propone la visión amplia o multidimensional de la misma, con ella se detectan nuevas amenazas y se incorporan nuevas esferas dentro de la seguridad tradicional, estas son 5:

- 1) Militar: capacidades ofensivas y defensivas de los Estados y las percepciones de estos sobre las intenciones de otros
- 2) Política: Tiene que ver con la organización estatal, el adecuado funcionamiento de las instituciones y unidad/legalidad de las mismas
- 3) Económica: referente a asegurar el acceso a los recursos mercados y finanzas necesarios para sostener los niveles de bienestar de la población y la estabilidad del Estado
- 4) Ambiental: el respeto al medio ambiente y la promoción del desarrollo sustentable, incluyendo el combate al cambio climático

²¹ Radio Radica.le “Ninguna nación puede solucionar sus problemas por sí solo”, en línea, Italia, 2005, Dirección URL: <http://bit.ly/1QuCZNe>, consultado el 1 de septiembre del 2014

²² *Ibidem*

²³ *Ibidem*

²⁴ El término “Escuela de Copenhague” fue acuñado por primera vez por Bill McSweeney en un ensayo que dio inicio a un intercambio en forma de debate entre este autor y varios de los investigadores que el adscribía a su nueva escuela, estos investigadores trabajaban en el Instituto de Investigación para la Paz de Copenhague y que en 1985 elaboraron una investigación pionera sobre “seguridad europea”.

- 5) Social: entendida como la capacidad de la sociedad de mantener los elementos de su identidad cultural y nacional, como las costumbres el lenguaje y la religión.

Como se observa, este concepto ha sufrido una evolución, desde su concepción clásica de orden público y paz pública, seguridad interior y exterior del Estado, hasta un concepto más amplio y que abarca diversas índoles.

Buzan, De Wilde, y Weaver propusieron entender la seguridad como una construcción social a partir del discurso, afirmando que “por seguridad se entiende cuando un representante del Estado declara una condición de emergencia, así que reclama el derecho de usar cualquier medio que sea necesario para bloquear el desarrollo de la amenaza²⁵”

En este sentido, la seguridad se traduce en acciones específicas del Estado para hacer frente a amenazas, ese es el principal objetivo de la ciberseguridad.

1.1.2. Guerra: de las guerras tradicionales a la ciberguerra

El conflicto armado es inherente a la historia de la humanidad. Retomando a Tomas Hobbes y su tesis que señala que “el ser humano es violento por naturaleza” entonces damos por hecho de que éste ha tratado siempre de resolver sus conflictos por medio de la violencia cuando las palabras (en el caso de las Relaciones Internacionales, la diplomacia) han fracasado. El Estado al interior tiene resuelto el asunto a través de las instituciones y el monopolio legitimo del uso de la violencia, pero al exterior la competencia es permanente. Pero el Estado debe tomar en cuenta el actuar del adversario, el cual se defenderá para tratar de impedir o minimizar un daño y con ello impedir el sometimiento de su voluntad, dando lugar a enfrentamientos.

Es aquí cuando en el marco de las Relaciones Internacionales surge el dilema de seguridad el cual, se explica de la siguiente manera:

“Es una situación que se produce cuando las acciones de un Estado que pretende mejorar su seguridad (por ejemplo, con el incremento de su poder militar o estableciendo alianzas), lleva a que otro Estado o a Estados, respondan de

²⁵ Waever, O. “Securitization and Desecuritization” en Lipschutz, R.(Ed.), On Security, Nueva York: Columbia University Press, 1995, pág. 22

manera similar, generando tensiones y conflictos a pesar de que ninguno de ellos lo desee²⁶”

Como podemos ver, el dilema de la seguridad hace referencia a la idea de que un Estado, al incrementar su capacidad militar contra la amenaza de otro Estado, lo que puede conseguir es el efecto opuesto, ya que el “otro” percibe o se da cuenta de este incremento y lo ve como una amenaza a su seguridad al ver que el enemigo puede utilizar en su contra él ese armamento militar; como consecuencia, ese otro Estado incrementa su capacidad militar como respuesta. Esto a su vez puede generar que el primer Estado vuelva a incrementar su capacidad bélica. Entrando ya en un proceso cíclico, competitivo (el objetivo es "ganar" la carrera), recíproco (los dos Estados se prestan atención y recursos) y hostil (subyacen intenciones agresivas).

El dilema de seguridad explica la lógica de la ciberguerra, esto es, cuando un Estado realiza un ciberataque en contra de la infraestructura o la información de un Estado, hace que el “otro” comience a generar nuevas formas de atacar al enemigo por esta misma vía, generando la creación de nuevos armamentos (las ciberarmas) que hagan daños catastróficos en los datos, la infraestructura, o incluso llegando a causar la pérdida de vidas humanas.

En 1648 se inicia la Paz de Westfalia la cual termina en 1914 con la Primera Guerra Mundial, en este periodo de tiempo se llevaron a cabo diversos conflictos en todo el mundo los cuales tenían en común que eran puramente militares y entre dos estados, estas características hicieron que la guerra se definiera como “guerra clásica”. Karl Von Clausewitz en su libro ‘De la guerra’ nos dice

“La guerra no es otra cosa que un duelo en una escala más amplia. Si concibiéramos a un mismo tiempo los innumerables duelos aislados que la forman, podríamos representárnosla bajo la forma de dos luchadores, cada uno de los cuales trata de imponer al otro su voluntad por medio de la fuerza física; su

²⁶ Robert Jervis, “*Cooperation under the Security Dilemma*”, *World Politics*, Vol. 30, No. 2, 1978, p.58

propósito inmediato es derribar al adversario e incapacitarlo de ese modo²⁷ y finaliza de la siguiente manera; “la guerra es un acto de fuerza para imponer nuestra voluntad al adversario²⁸” y más adelante nos otorga una frase que sería recordada por su significado; “La guerra es la mera continuación de la política por otros medios.”²⁹

A raíz de esto, Clausewitz nos ofrece un análisis de la guerra a partir de tres variantes; el Estado que monopoliza la fuerza; el ejército que ejecuta esta fuerza; y un pueblo que juega un rol mínimo dentro del conflicto y que prácticamente no es participe de este.

Posteriormente, el ser humano se dio cuenta de que el mar es el medio por el cual es posible influir en la imposición de esta voluntad, como consecuencia surgen las guerras navales y las acciones del mar sobre la costa, después aparecen de forma las guerras en el aire, en el espacio y ahora el ciberespacio. Esto se explica de una forma, cuando aparece un “nuevo campo de batalla” o “campo de influencia” ya sea real o virtual y el ser humano quiere influir o participar en él, los contendientes tratarán de conquistarlo, de ser superiores en él, con objeto de beneficiarse e impedir que el enemigo lo haga.

A lo largo de los años, las guerras han ido modificando su campo de batalla, primero, la lucha tradicional en tierra (guerra terrestre), esta engloba varios tipos de unidades diferentes de combate y de los servicios como lo son: el uso de armamento específico para este tipo de combate: infantería, blindadas, artillería, ingeniería, comunicaciones y logística.

Después, los gobiernos se dieron cuenta de que también podían atacar al adversario a través de otros espacios (el marítimo o naval y el aéreo), el combate marítimo posee la característica principal de intimidar al enemigo en los mares, océanos, o cualesquiera otros cuerpos grandes de agua, como grandes lagos y anchos ríos. Finalmente, la guerra aérea usa los aviones militares y otras máquinas que vuelan en la guerra, esta modalidad de guerra aérea involucra el

²⁷ Clausewitz, Karl Von. “*De la Guerra*”, pág. 31.

²⁸ *Ibidem*

²⁹ *Ibidem* pág. 48

uso de tecnología sumamente desarrollada, innovando cada vez más los modos de intervenir por este medio como lo son el uso de radares, aviones no tripulados.

A lo largo de estos años la guerra se llevó a cabo durante muchos años en estas tres dimensiones, pero un conflicto durante la Segunda Guerra Mundial entre EE.UU., y la ex Unión Soviética hizo posible que existiera un nuevo campo de batalla: el espacio exterior.

Estamos hablando de la SDI, un ambicioso proyecto que Ronald Reagan informo al pueblo estadounidense, el veintitrés de marzo de 1983 en una solemne intervención televisada desde el Despacho Oval ante la perplejidad de expertos militares y científicos. Esta estrategia,

“requería una red de más de dos mil doscientos satélites militares equipados con unas armas que aún no habían sido inventadas y cuyo coste estimado sobrepasaría el billón y medio de dólares (o trillón, según la escala norteamericana), el equivalente a casi la mitad todo el PIB estadounidense de aquel año.³⁰”

Su objetivo principal, era utilizar sistemas basados en la tierra y en el espacio a fin de defender a Estados Unidos contra un ataque nuclear con misiles balísticos intercontinentales.

La milicia compartía la misma preocupación que el presidente, ellos consideraban que EE.UU. era una “ventana de vulnerabilidad” y que ante un ataque masivo por parte de la URSS, estos destruirían los misiles americanos antes de que despegasen de sus sitios. El gobierno estadounidense decidió lanzar el Proyecto BAMBI y el Proyecto Excalibur.

La Agencia DARPA, dependiente del Pentágono, estaba comenzando a tantear la posibilidad de destruir los misiles enemigos apenas fueran lanzados, utilizando para ello satélites situados en órbitas encima de los silos que serían sus objetivos. Eso era el Proyecto BAMBI (Ballistic-Missile Boost Intercept). El Proyecto Excalibur por su parte experimentaba con rayos láser de alta potencia que podrían ser disparados desde el espacio y destruir sus objetivos a la velocidad de la luz, pues

³⁰ Jot Down.com “*La guerra de las galaxias de Ronald Reagan*”, 2013, en línea, <http://bit.ly/1PwJ0eb> consultado el 01 de octubre del 2014

alcanzar a un misil en movimiento no es nada fácil para un proyectil convencional³¹.

Como podemos observar, durante la Guerra Fría surge un cuarto campo de batalla en donde un Estado busca protegerse y también como se ha demostrado anteriormente se dan los cimientos de un quinto: el ciberespacio, que tomará preponderancia en el siglo XXI, con el desarrollo de nuevas tecnologías y el surgimiento de nuevas amenazas en la sociedad internacional (terrorismo, crimen organizado, migración, entre otras).

Las guerras tradicionales dejan de existir y el concepto de guerra sufre un cambio que Eric Hobsbawm explica de la siguiente manera:

“[...] a principios del siglo XXI estamos en un mundo donde las operaciones armadas ya no están fundamentalmente en manos de los gobiernos y de sus agentes autorizados, y donde las partes en conflicto no comparten características, ni estatus, ni objetivos, excepción hecha del deseo de recurrir a la violencia.”³²

Todo esto, producto de la globalización y de los cambios tan apresurados por los que ha atravesado el mundo a lo largo del tiempo.

Otra autora que redefine el concepto de Guerra es Mary Kaldor quien ubica estas “nuevas guerras” a partir de los 80 y 90, las cuales poseen ciertas características;

[...] implican un desdibujamiento de las distinciones entre guerra, crimen organizado y violación a gran escala de los derechos humanos, asimismo frente a lo que hemos [MK] definido como guerras viejas [refiriéndose a los conflictos enmarcados bajo el modelo clausewitziano]. Las nuevas guerras son diferenciables principalmente en cuanto a: 1. Objetivos de la guerra 2. Métodos de lucha y 3. Métodos de financiación³³.

La autora nos hace ver que los objetivos de la guerra ahora incluyen cuestiones relativas a la identidad, el nacionalismo, la cultura, entre otros. Asimismo, se

³¹ *Ibidem*

³² Eric Hobsbawm, Guerra y paz en el siglo XXI, Editorial Crítica, España, 2007, p. 3.

³³ Mary Kaldor, Las nuevas guerras: violencia organizada en la era global, España, Tusquets, 2001, pp. 49-79.

incluyen nuevos métodos de lucha los ejércitos, ya no solo se capacitan físicamente y para manejar armas. Las nuevas tácticas que se emplean son muy diferentes a las tradicionales, y esto ha ocasionado la formación de nuevas estrategias que se adaptan a las nuevas amenazas y que son financiados por grandes mercados (algunos negros) pertenecientes a una economía globalizada.

Por lo anterior, podemos decir entonces, que la guerra es un enfrentamiento que se va a llevar a cabo, derivado de una confrontación entre dos actores internacionales (tradicionales y no tradicionales) y esta lucha va a generar que las tácticas, estrategias y formas de adquirir el armamento se adapten a las nuevas amenazas que surgen en la sociedad internacional. Precisamente la introducción del ciberespacio como nuevo campo de batalla, da cuenta de las transformaciones del combate (las ciberguerras), lo que provoca que las políticas de seguridad de los Estados (ciberseguridad) se centren en estas nuevas amenazas, todo esto se detallará más adelante.

1.2. La Teoría de la Globalización Tecnológica: explicación del Tecnoutopismo y Cybergeddon

Dentro de las Relaciones Internacionales, las teorías ayudan a explicar la realidad internacional de manera más clara y con elementos que aportan un nivel de análisis mucho mayor a un conflicto. La teoría de la Globalización, ha sido utilizada para describir la dinámica actual del sistema internacional, el cual se integra mediante distintos actores, factores y niveles que lo conforman.

Esta teoría, comenzó a ser usada a finales de la década de los 60 y principios de los 70, fue durante esta transición de años que “el sistema internacional observo una creciente interdependencia económica y política, a la vez que se planteó la necesidad de formular explicaciones a fenómenos locales y/o nacionales en función de acontecimientos externos y/o internacionales³⁴”

³⁴ Held David and Mc Grew Anthony, *“The global transformations reader: An introduction of Globalization debate”*, Ed. Great Britian Polity Press, Gran Bretaña, 2003, pág.4

Antes de definir a la globalización tecnológica, debemos de contestar a la incógnita ¿Qué es la globalización?, una primera definición que nos indica la serie de factores que se ven influenciados por este proceso la da Isidro Morales en el artículo, *Globalización y regionalización. Hacia la construcción y gestión de un nuevo orden económico internacional*.

[...] la globalización remite a un estado de interdependencia compleja, en donde los procesos particulares, sean estos económicos, políticos, financieros o incluso socioculturales, interactúan con procesos transnacionales, ya sea en forma de refuerzo o confrontación. La globalización resulta así un proceso de interacción entre lo particular y lo general en campos específicos de las relaciones internacionales, sobretodo en la esfera financiera, productiva, comercial, política y cultural.³⁵

Esta definición nos proporciona elementos a considerar, como lo es la influencia de esta teoría en diferentes aspectos dentro del Estado (político, económico, social, etc...). En su libro *The global transformations reader: An introduction of Globalization debate*, los autores nos proporcionan un concepto

La globalización ha sido concebida como la acción a distancia (mediante el cual las acciones de los agentes sociales en un entorno regional, pueden llegar a tener consecuencias significativas para los "demás"); comprenden tiempo-espacio (en referencia a la forma en que las comunicaciones electrónicas instantáneas erosionan las limitaciones de distancia y el tiempo en la organización social de una interacción); aceleración de la interdependencia (entendida como la intensificación de un enredo entre las economías y las sociedades nacionales, de tal manera que los acontecimientos en un país tengan impacto directamente sobre otros); un mundo en disminución (la erosión de las fronteras y las barreras geográficas de la actividad económica-social); entre otros conceptos, la integración global, el reordenamiento de las relaciones de poder interregionales, la conciencia de la condición global y la intensificación de la interconexión interregional.³⁶

³⁵ Morales, Isidro, *Globalización y regionalización. Hacia la construcción y gestión de un nuevo orden económico internacional*, en Zidane Ziraoui, *Política Internacional Contemporánea* Ed. Trillas, México, 2000, pág. 287

³⁶ Held David and Mc Grew Anthony, Op Cit. pág. 6

Observamos, que el proceso de la globalización va a disminuir las brechas o limitaciones que antes existían entre los Estados, entrelazándolas más en un mundo cada vez más conectado por las comunicaciones electrónicas.

La definición anterior nos proporciona una característica relevante dentro de la ciberseguridad, pues define que las relaciones entre los Estados van a ser más estrechas debido a las tecnologías de la información, pero también va a generar que los conflictos se den en el marco de este “nuevo” espacio y, por lo tanto, sea aquí donde se lleven a cabo los conflictos. Giovanni E. Reyes, define a la globalización como,

“una teoría entre cuyos fines se encuentra la interpretación de los eventos que actualmente tienen lugar en los campos del desarrollo, la economía mundial, los escenarios sociales y las influencias culturales y políticas. La globalización es un conjunto de propuestas teóricas que subrayan especialmente dos grandes tendencias: (a) los sistemas de comunicación mundial; y (b) las condiciones económicas, especialmente aquellas relacionadas con la movilidad de los recursos financieros y comerciales.³⁷”

Nuevamente el término se refiere a una multidimensionalidad (política, económica, cultura, tecnología y ambiental) que genera una relación entre sí para permitir el desarrollo del sistema internacional. Si bien, este término denota la integración entre los Estados, esto no quiere decir que sea un proceso pacífico, igualitario o que llegue a concretarse.

Es este carácter multidimensional de la Globalización hace que este proceso sea estudiado desde una perspectiva multidisciplinaria, un autor que estudia a la Globalización de esta manera es Wolfgang Thierse que define desde cinco dimensiones las cuales van a desarrollarse con diferente intensidad. Para el autor, las cinco dimensiones son las siguientes:

³⁷ Reyes E. Giovanni, “*Teoría de la Globalización: Bases Fundamentales*”, en *Nómadas*, núm. 3, enero-junio, 2001, Universidad Complutense de Madrid, España [en línea]; <http://bit.ly/21GRw31>, consultado el 20 de octubre del 2014

-
- *Globalización como categoría económica del comercio mundial,*

- *Globalización como categoría político financiera de los mercados financieros internacionales,*

- *Globalización como categoría tecnológica de la transición a la sociedad de la información,*

- *Globalización como categoría ecológica de los riesgos ecológicos globales*

- *Globalización como categoría cultural con respecto a la transformación por una cultura universal a cambio de las costumbres heredadas u las características regionales³⁸.*

Tabla 1. Tipos de globalización, elaboración propia con base en el texto Thierse, Wolfgang, “*Globalización y capacidad de estructuración de la política*”, Materiales de Trabajo No. 10, Facultad Latinoamericana de Ciencias Sociales (FLACSO), México, 1999, Fundación Friederich Ebert, [en línea]; <http://bit.ly/1TbiGKs> pág. 8, consultado el 22 de octubre del 2014

Estas dimensiones el Estado las desarrollará de distinta manera de acuerdo a sus capacidades, la ciberseguridad se explica a través de la categoría tecnológica de la información, es decir, la globalización tecnológica.

De igual forma, este concepto es trabajado en la obra *Filosofía norteamericana del Poder*, del Dr. José Luis Orozco en donde señala que la globalización representa “la americanización de la vida [...]. Magnificada en lo tecnológico, apuntalada a escala transnacional y uniformada en el consumismo [...] mantiene una estructura empresarial corporativa que dista en todo de la igualdad social e internacional³⁹”.

³⁸ Thierse, Wolfgang, “*Globalización y capacidad de estructuración de la política*”, Materiales de Trabajo No. 10, Facultad Latinoamericana de Ciencias Sociales (FLACSO), México, 1999, Fundación Friederich Ebert, en línea, <http://bit.ly/1TbiGKs> pág. 8, consultado el 22 de octubre del 2014

³⁹ Orozco Alcántar José Luis, *Filosofía norteamericana del poder*, México, Cd. Juárez, Universidad Autónoma de Ciudad Juárez, 1995, p.101-

Tecnoutopismo y Cybergeddon

Como hemos visto, el proceso de globalización va ligado con la revolución tecnológica, una a otra se complementan. Nuevos conceptos como ciber mundo, sociedad de la información, big data y sociedad del conocimiento hacen que aparezcan nuevas teorías del cómo estos van a impactar en la humanidad. En este caso, hablamos del Tecnoutopismo y el Cybergeddon

Tecnoutopismo.

Etimológicamente, la palabra utopía se deriva del griego “ού” que quiere decir, ningún, y “*topos*” que significa lugar. Entonces, utopía⁴⁰ es “un lugar no existente”. Ante lo cual, la definimos como aquel plan, sistema, lugar, proyecto o escenario, en donde hay condiciones “perfectas” para que el ser humano solo y en sociedad pueda vivir, pero desafortunadamente esto es irrealizable.

Es innegable que desde su invención, internet ha revolucionado al mundo, ya que le ha facilitado al ser humano algunas tareas, pero también ha provocado que se vea al internet como un “milagro tecnológico” que resuelve día con día las dificultades que el ser humano presenta.

Este “milagro tecnológico” ha dado pie a la creación de teorías que expliquen las “bondades” de esta herramienta, como el tecnoutopismo o utopismo tecnológico, el cual hace alusión a “cualquier ideología basada en la creencia de que los avances en ciencia y tecnología conducirán a una utopía, o al menos ayudarán a cumplir de algún ideal utópico.”⁴¹

En otras palabras la tecnoutopia hace alusión a las creencias, donde el ser humano considera a la tecnología como aquel móvil que va solucionar todos los problemas, empezando por los económicos y de ahí desatando una ola hasta llegar a la solución de conflictos sociales.

⁴⁰ Dentro del proceso de lo “cyber”, también existen las posibilidades de realizar escenarios en donde se caiga en una utopía, para efectos de este trabajo se le llamará tecnoutopismo o utopismo tecnológico.

⁴¹ Foro Económico Mundial, “Tech utopia or cybergeddon?”, enero 2013, en línea, dirección URL: <http://bit.ly/2cVif6S>, consultado el 17 de junio del 2016. Traducción propia

Uno de los países que más han apoyado esta idea de “utopismo tecnológico” ha sido Estados Unidos, pues es cuna de uno de los principales territorios en donde se llevan a cabo numerosos avances tecnológicos, hablamos de Silicon Valley. Esta ideología californiana consideraría al internet como uno de los principales precursores de este utopismo ya que “incrementaría la libertad personal, liberando al individuo del rígido abrazo del gran gobierno burocrático⁴²”.

Bernard Gendron⁴³ en un artículo denominado *Technology and the Human Condition* enuncia 4 principios del utopismo tecnológico de la siguiente manera.

- 1) Actualmente estamos sufriendo una revolución (postindustrial) en tecnología;
- 2) En la era postindustrial, el crecimiento tecnológico será sostenido (como mínimo);
- 3) En la era postindustrial, el crecimiento tecnológico conducirá al fin de la escasez económica;
- 4) La eliminación de la escasez económica llevará a la eliminación de todos los mayores males sociales.⁴⁴

El tecnoutopismo nos presenta la premisa de que todos los bienes y servicios algún día estarán disponibles para todo el mundo, sin existir el dinero. La tecnología será una aliada que contribuirá a mejorar los niveles de productividad y que, gracias a ello, la calidad de vida será mejor gracias a una abundancia de recursos.

Actualmente, es un hecho que hay un crecimiento de las redes, del acceso a internet y que las infraestructuras han mejorado gracias a los avances tecnológicos que ha habido. Pero, desafortunadamente, el discurso tecnoutopico no incluye medidas concretas para lograr el “milagro tecnológico” y que con ello se aproveche el potencial que presenta la tecnología para el desarrollo integral de los individuos, además de que no toma en cuenta que en algunas zonas de diversos países, pensar en tecnología o acceso al ciberespacio es prácticamente imposible.

⁴² Clarke A. Richard, Knake K. Robert Op. Cit., pág. 103.

⁴³ Profesor de filosofía de la Universidad de Wisconsin-Milwaukee

⁴⁴ Gendron Bernard, 1977, *Technology and the Human Condition*, Technology and Culture Vol. 18, No. 3, pág. 518-520. Traducción propia.

Cybergeddon

El discurso de optimismo que nos ofrece el utopismo tecnológico, es contrarrestado por el cybergeddon una teoría que ve a los avances tecnológicos como los nuevos riesgos y amenazas.

“Miedos, incertidumbres y dudas alrededor de la tecnología no sabemos si el Internet está cambiando nuestro cerebro, pero sí sabemos que grandes porciones de nuestras redes de infraestructura crítica (petróleo, gas, electricidad, agua, trenes) están controlados de forma remota y que los mercados financieros -"dinero" por cualquier definición - es casi enteramente digital. También nos sorprendió encontrar una importante firma multinacional lleva a cabo operaciones en algún formato digital, en alguna parte del ciberespacio⁴⁵”.

Sean Gallagher graduado e investigador de la Universidad de Wisconsin y editor de Tecnologías de la Información en Ars Technica, página donde publica un artículo llamado: *Cybergeddon: Why the Internet could be the next “failed state”* realiza un amplio análisis prospectivo sobre los posibles 5 futuros del ciberespacio.

Escenario	Descripción
Paraíso (Technoutopismo)	La ciberseguridad se vuelve tan buena que el ciberespacio se convierte en un "lugar abrumadoramente seguro" Solamente los atacantes altamente sofisticados y que son patrocinados por los estados-nación pueden causar algún problema. El cibercrimen, el ciberespionaje y la ciberguerra contra alguna red o infraestructura se vuelve muy difícil
Status Quo	Cosas tal como están: altos niveles ciberdelincuencia y ciberespionaje, pero no hay ciberguerras masivas. Los principales proveedores de comercio electrónico continúan alerta de los ataques, el fraude afecta a un pequeño porcentaje de las transacciones, y los criminales sigan ganando dinero (pero no

⁴⁵ Op. Cit. Foro Económico Mundial.

	demasiado).
Dominio del conflicto	El ciberespacio se convierte al igual que cada dominio físico en el nuevo campo de batalla. Cibercrimenes, ciberespionaje y los conflictos entre estados nación se extienden por todo el ciberespacio.
Balkanización	Por cuestiones políticas y de seguridad, no hay un internet "único", sólo una colección de Internets nacionales. Las naciones bloquean cualquier acceso a otro contenido que no sea el propio, aunque puede haber ataques menos directos. Las empresas de Internet tendrían que duplicar la infraestructura en cada región, y la vigilancia se simplifica en gran medida a los Estados-nación.
Cybergeddon	El ciberespacio, "siempre ingobernable y rebelde", como lo expresó Healey, se convierte en un "estado fallido" en un estado casi permanente de perturbación. Cada tipo de conflicto es posible y permanente todo el tiempo. En el escenario de "Cybergeddon", escribió Healey, la cooperación para atrapar a los atacantes "es inútil, ya que los atacantes son difíciles, o imposibles de atrapar, es como tratar de gobernar un estado fallido".

Tabla 2. Cinco ciberfuturos. Tabla tomada de: Arstechnica, Gallagher Sean, "Five Internet futures", [en línea], febrero del 2014, Dirección URL: <http://bit.ly/1ETtHFP>. Traducción propia.

Como nos muestra la tabla anterior, el tecnoutopismo ya no es la realidad, cada vez es más frecuente que una empresa sea atacada, que una infraestructura crítica se vea afectada por un ciberataque, que no se midan los riesgos debido al desconocimiento humano del fenómeno. Hoy en día, cualquier persona, empresa, u oficina de gobierno que tenga su sitio web o que sus operaciones sean llevadas a cabo en el ciberespacio, tienen que lidiar a diario con amenazas que emanan de todo el mundo, pocos o ninguno se salvan de ellos, el cybergeddon es un escenario lejano, pero no por ello imposible.

1.3. El ciberespacio: nuevo campo de batalla

Ciberespacio tiene su origen en la palabra griega "cibernao" que significa pilotear una nave, este concepto se utilizó por primera vez en la novela de ciencia ficción "Neuromante" escrita por William Gibson en 1984, y a partir de ahí se popularizó su uso.

El ciberespacio puede verse como la expansión de los términos seguridad, defensa y guerra a un ámbito intangible, es decir, el ser humano se ha encargado de expandir su territorio de protección y de combate. Según Robert Knake

“El ciberespacio, es el portátil que sus hijos llevan a la escuela y el ordenador de sobremesa que tiene en el despacho. Es un edificio gris desprovisto de ventanas en el centro de la ciudad y una tubería subterránea que recorre sus calles. Está en todos los lugares en los que hay un ordenador o un procesador o un cable que conecta con uno.”⁴⁶

Entonces, si el ciberespacio no tiene un punto fijo y se encuentra disperso en cualquier parte del mundo ¿Puede regularse? La respuesta es no, ya que el ciberespacio cruza las fronteras físicas ya establecidas. “El ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan.”⁴⁷

La Orden Ministerial 10/2013 del 19 de febrero emitida por el Ministerio de Defensa español define al ciberespacio como “(el) dominio global y dinámico compuesto por infraestructuras de tecnología de la información- incluyendo internet’, redes de telecomunicaciones y sistemas de información,”⁴⁸ derivado de esta definición se puede observar los componentes del ciberespacio, el internet es uno de ellos, conceptualmente internet y ciberespacio pueden llegar a utilizarse como sinónimos, al respecto Richard Clarke y Robert Knake aseguran:

“No se trata solo de Internet. Es importante dejar en claro la diferencia. Internet es una red de redes abierta. Desde cualquier red de Internet podemos comunicarnos.

⁴⁶ Clarke A. Richard, Knake K. Robert Óp. Cit. pág. 103

⁴⁷ *Ibidem*

⁴⁸ Ministerio de Defensa de España, “Disposiciones generales. Definiciones”, emitido el 26 de febrero del 2013, en línea, dirección URL: <http://bit.ly/2bA6Afb>, consultado el 23 de junio del 2016

[...] El ciberespacio es Internet más montones de otras redes de ordenadores a las que, se supone, no es posible acceder desde internet.”⁴⁹

Algunas de estas redes pueden ser parecidas a la estructura de internet (ejemplo de ello la Deep Web), pero estas se encuentran separadas de ellas. “Otras partes del ciberespacio son las redes transaccionales que sirven para enviar y recibir datos acerca de, por ejemplo, los flujos de dinero, las operaciones en el mercado de valores y las transacciones de tarjetas de crédito.”⁵⁰

El hecho de que el ciberespacio e internet no sean lo mismo, no significa que lo que no sea parte del internet sea secreto o impenetrable. Diversos actores (hackers, hacktivistas, ciberterroristas, etc...) pueden introducirse en estas redes, controlarlas, alterarlas o hacerlas caer. “pueden robar toda la información que contiene o darle instrucciones para transferir dinero, derramar petróleo, liberar gas, volar [o alterar] generadores, descarrilar trenes, estrellar aviones, enviar pelotones a una emboscada o detonar un misil en un lugar equivocado”⁵¹

El ciberespacio es un lugar donde millones de usuarios de todo el mundo, de todos los sectores manejan información, detener una cadena de abastecimiento puede resultar desastroso o no (tal y como se demostró en 2010 con el Programa Nuclear Iraní), entonces, el ciberespacio es el área de acción de la ciberseguridad.

1.4. Concepto de ciberseguridad o seguridad informática y diferenciación con seguridad de la información

Después de exponer los fundamentos teóricos que dan explicación a la ciberseguridad o seguridad informática,⁵² y de demostrar porque el ciberespacio es de fundamental importancia para ella, es necesario definirla.

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de la Organización de las Naciones Unidas que se encarga de las

⁴⁹ Clarke A. Richard, Knake K. Robert Op. Cit. pág. 104

⁵⁰ *Ibidem*

⁵¹ *Ibidem*

⁵² A lo largo de esta investigación, se utilizará ciberseguridad o seguridad informática como sinónimos.

Tecnologías de la Información y la Comunicación, este órgano mediante la Resolución 181 *Definiciones y terminología relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación* aprobó una definición de ciberseguridad.

“La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- *disponibilidad;*
- *integridad, que puede incluir la autenticidad y el no repudio;*
- *confidencialidad.*⁵³

Esta definición, que nos ofrece la UIT, engloba diferentes características como lo son: herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías para protegerlos en el *ciberentorno*⁵⁴.

A pesar de que esta definición la ofrece este organismo internacional, no existe un consenso a nivel mundial en lo que constituye ciberseguridad. Las definiciones de cada Estado, cuando las hay, hacen alusión del cómo percibe ese Estado la naturaleza de la amenaza del Ciberespacio.

Uno de los países del continente europeo que más se ha preocupado en lo concerniente a la ciberseguridad es España, quien es parte de la Unión Europea, durante su Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el

⁵³ UIT-ONU, “*Decisiones destacadas de Guadalajara: Resolución 181: Definición de Ciberseguridad*”, en línea, dirección URL: <http://bit.ly/1PCGgzp>, consultado el 26 de marzo del 2016.

⁵⁴ Sinónimo de ciberespacio

Mando Conjunto de Ciberdefensa de las Fuerzas Armadas nos presenta una definición de ciberseguridad, la cual se comprende como el “Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan⁵⁵”.

Es un hecho que existe una proliferación de virus y programas malignos que, debido a la inconsciencia del ser humano, hacen aún más rápida su propagación en el internet, esto ha despertado el interés por diversos autores por definir o estudiar a la seguridad informática. Álvaro Gómez Vieites define a la seguridad informática como:

“cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar a daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso a usuarios autorizados al sistema.”⁵⁶

Estas tres definiciones nos ofrecen diversas características (como lo son las medidas que se toman para proteger el entorno), y elementos (protegen al usuario, el ciberentorno, las infraestructuras, servicios, sistemas informáticos) entonces para efectos de esta investigación, entenderemos a la ciberseguridad o seguridad informática como:

“Aquellas acciones, medidas y políticas de seguridad que emplee un Estado en el ciberespacio, con el objetivo de dañar, recuperarse, prevenir o aminorar el impacto de los ciberataques provenientes de otro actor (un Estado, empresa, hacker, etc...) a los ordenadores de infraestructuras críticas consideradas por el Estado de suma importancia y cuyas repercusiones pueden generar un daño o destrucción de la información o al correcto funcionamiento de estas.”

⁵⁵ Ministerio de Defensa Español, “Orden Ministerial 10/2013: Guerra Cibernética: Aspectos Organizativos”, 19 de febrero del 2013, en línea, dirección URL: <http://bit.ly/2cPIY6p>, consultado el 15/04/2016, pág. 4

⁵⁶ Vid. Gómez Vieites Álvaro, “Enciclopedia de la seguridad informática”, 2ª Edición, Editorial Alfaomega, Madrid, España, 2011, pág. 38

La seguridad informática o ciberseguridad considera diversos objetivos los cuales se van a encargar de minimizar el daño o saber cómo solucionar los daños causados por un ciberataque. Entre los objetivos destacan los siguientes:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad
- Cumplir con el marco legal y los requisitos impuestos por los Estados⁵⁷

Es necesaria la intervención de todos los actores que participan en las medidas de ciberseguridad (empresas, gobiernos y usuarios) para llevar a cabo planos de acción⁵⁸ que aseguren el logro de estos objetivos.

- Técnico: correcto uso de aplicaciones, sistemas operativos y herramientas. Así como conocer el funcionamiento, composición y actualización del Hardware y software.
- Legal: leyes a nivel nacional que garanticen medidas de seguridad en contra de los cibertatacantes, además que ayuden a la prevención de pérdidas o robos de información.
- Humano: concientización del usuario al usar un sistema informático, así como una interacción entre técnicos, usuarios y encargados de la seguridad informática para un buen uso de las diversas herramientas.
- Organizativo: crear políticas de contingencia o implementar la cultura de la prevención del ciberdelito en el usuario, asimismo, crear planes de respuesta ante un posible ciberataque.

⁵⁷ *idem* pág. 40

⁵⁸ Los 4 planos de acción son propuestos por Gómez Vieites Álvaro en su libro, pero son explicados por el escritor de la tesis en sus propias palabras.



Esquema 1. Planos de acción en la seguridad informática, elaboración propia tomando como referencia el cuadro y utilizando elementos del texto, Gómez Vieites Álvaro, “Enciclopedia de la seguridad informática”, 2ª Edición, Editorial Alfaomega, Madrid, España, 2011, pág. 40.

Por último, Vietes Gómez, sugiere que “la Seguridad Informática debe verse como un proceso y no como un producto que se pueda *comprar o instalar*⁵⁹”. Entonces, con base del Esquema 1, se entiende que es un proceso interactivo en el que se analizan todos los factores de riesgo para crear medidas de prevención, detección y respuesta ante los ciberataques.

Ya habiendo definido y analizado los niveles de acción de la ciberseguridad, es necesario hacer una diferenciación de conceptos, que pueden confundir al lector. Estos conceptos son ciberseguridad (o seguridad informática) y seguridad de la información, ya que suelen ser utilizados (erróneamente) como sinónimos.

Conceptualmente hablando, la ciberseguridad o seguridad informática se encuentra dentro de la seguridad de la información. Jeimy J. Cano en su libro, *Inseguridad de la información: una visión estratégica* nos dice, “la función de la seguridad de la información tradicional se concreta en la información y como esta

⁵⁹ *Ibidem*, pág. 41

debe ser protegida. Es decir, estudia sus detalles y sus medios de difusión o almacenamiento para establecer las medidas tecnológicas (en el amplio sentido de la palabra y no solamente computarizadas) requeridas que permitan un acceso confiable y controlado”⁶⁰

Anteriormente, se definió ciberseguridad destacando un elemento; el ciberespacio, es decir, un entorno no físico, por lo que la seguridad de la información se encargará de la protección de todos los medios de difusión ya sea físicos o no, en un entorno visible o no, la seguridad informática, entonces, solo se limita al ciberespacio.

1.5. Tipología y categorización de los crímenes cibernéticos

Para determinar cuál es el marco de acción de la ciberseguridad y los crímenes que esta persigue, definiremos primeramente, que es un cibercrimen, después definiremos a los cibrecrímenes más comunes que se han presentado en la sociedad internacional y sus características.

1.5.1. Cibercrimen

Un cibercrimen o delito informático es “cualquier comportamiento antijurídico, no ético no autorizado, relacionado con el proceso automático de datos y/o transacciones de datos,”⁶¹ entonces, una primer característica del cibercrimen es que se encuentra tipificado jurídicamente, además de que se va a encargarse de proteger los datos del usuario, pero carece de una explicación detallada sobre lo que se considera cibercrimen. Marco Galindo en su libro *Escaneando la informática* ahonda más en este concepto:

“El concepto de cibercrimen abarca desde el delito económico, como el fraude informático, el robo, la falsificación, el “computer hacking”, el espionaje informático, el sabotaje, la extorsión informática, la piratería comercial y otros crímenes contra la propiedad intelectual, la invasión de la intimidad, la distribución de contenidos

⁶⁰ Cano M. Jeimy, *“Inseguridad de la información: una visión estratégica”*, Editorial Alfaomega, Bogotá, 2013, pág. 16

⁶¹ Vid. *Definición propuesta por un grupo de expertos de la OCDE en 1993* en Gómez Vieites, Óp. Cit. pág. 665

ilegales y dañosos, la incitación a la prostitución y otras actitudes que atenten contra la moralidad⁶²”.

Naciones Unidas mediante la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC por sus siglas en inglés) realizó un estudio titulado; “Comprehensive Study on Cybercrime” publicado en febrero del 2013, establece que el cibercrimen es una amenaza global, además de existir una fragmentación a nivel internacional referente a leyes que combaten los cibercrimenes.

En este trabajo UNODC nos ofrece una perspectiva amplia que ayuda a entender el estado y las tendencias del *cibercrimen* ello con ayuda de datos recabados de diferentes Estados para aclarar el panorama internacional.

Al respecto, el estudio señala:

“los actos delictivos cibernéticos se basan principalmente en actos con motivaciones financieras, actos relacionados con contenidos informáticos y contra la confidencialidad, integridad y accesibilidad de los sistemas informáticos. Sin embargo, los gobiernos y las empresas del sector privado perciben la amenaza y el riesgo relativos de manera diferente.”⁶³

Una cosa más que nos muestra este estudio es la creciente alza de los cibercrimenes, que en comparación con los crímenes normales, presentaron un incremento considerable tal como lo muestra la siguiente figura.

Este estudio también nos ofrece la tipificación de los cibercrimenes de acuerdo al nivel de interferencia que exista dentro del ciberespacio, es decir, si la interferencia es intencional o temeraria (cruce de información). “la interferencia va desde dañar hasta borrar, alterar, suprimir, agregar o transmitir datos.”⁶⁴

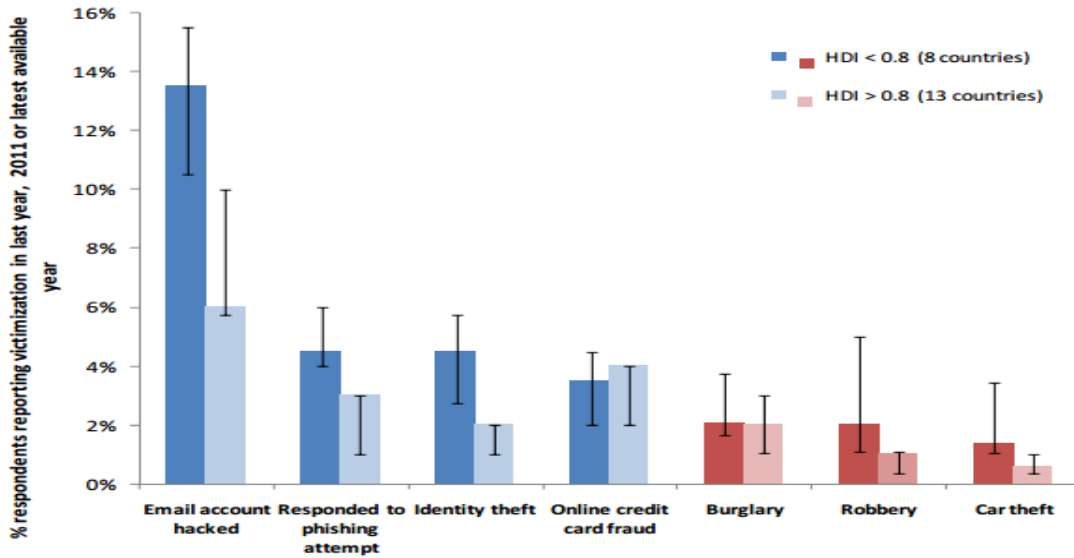
⁶² Marco Galindo María de Jesús, “Escaneando la Informática”, UOC (Universitat Oberta De Catalunya), 2010, pág. 75

Rodríguez Bernal Antonio, “Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia”, 5 de septiembre del 2006, en línea, dirección URL: <http://bit.ly/2cyZyVv>, consultado el 17 de abril del 2016.

⁶³ UNODC, “Comprehensive Study on Cybercrime”, 2013, en línea, dirección URL: <http://bit.ly/1ppgOOs>, consultado el 17 de abril de 2016. Traducción propia

⁶⁴ UNODC, *ibídem* pág. 20. Traducción propia

Cybercrime and conventional crime victimization



Grafica 1. Incremento de los cibercrimenes a nivel mundial en el año 2013. Tomado de UNODC, "Comprehensive Study on Cybercrime", 2013., en línea, dirección URL: <http://bit.ly/1ppgOOs>, pág. 16, consultado el 17 de abril de 2016

National approaches to criminalization of cybercrime acts



Grafica 2. Enfoques criminales hacia una criminalización del cibercrimen. Tomado de UNODC, *ibidem* pág. 20, consultado el 20/04/2016

En el ámbito internacional, el estudio hizo un reconocimiento de la no existencia de una legislación mundial que ayude al combate de los cibercrimenes y da carácter transnacional al cibercrimen “[el] delito cibernético existe cuando un elemento o un efecto sustancial del delito se da en otro territorio, o cuando parte el *modus operandi* del delito está en otro territorio.”⁶⁵

Además hace un énfasis en la falta de consenso por parte de los países para la creación de un marco suficiente para la criminalización y el enjuiciamiento en caso de actos de delito cibernético extraterritoriales, y criticando a los ya existentes debido a que llegan a ser insuficientes. Por lo anterior, el documento menciona en este ámbito:

“Depender de los medios tradicionales de la cooperación internacional en asuntos relacionados con el delito cibernético actualmente no ofrece la respuesta oportuna que se necesita para obtener evidencia electrónica volátil. Debido a el número creciente de delitos que involucran evidencia electrónica distribuida geográficamente, esto representa un problema no solo en el delito cibernético, sino con todos los delitos.”⁶⁶

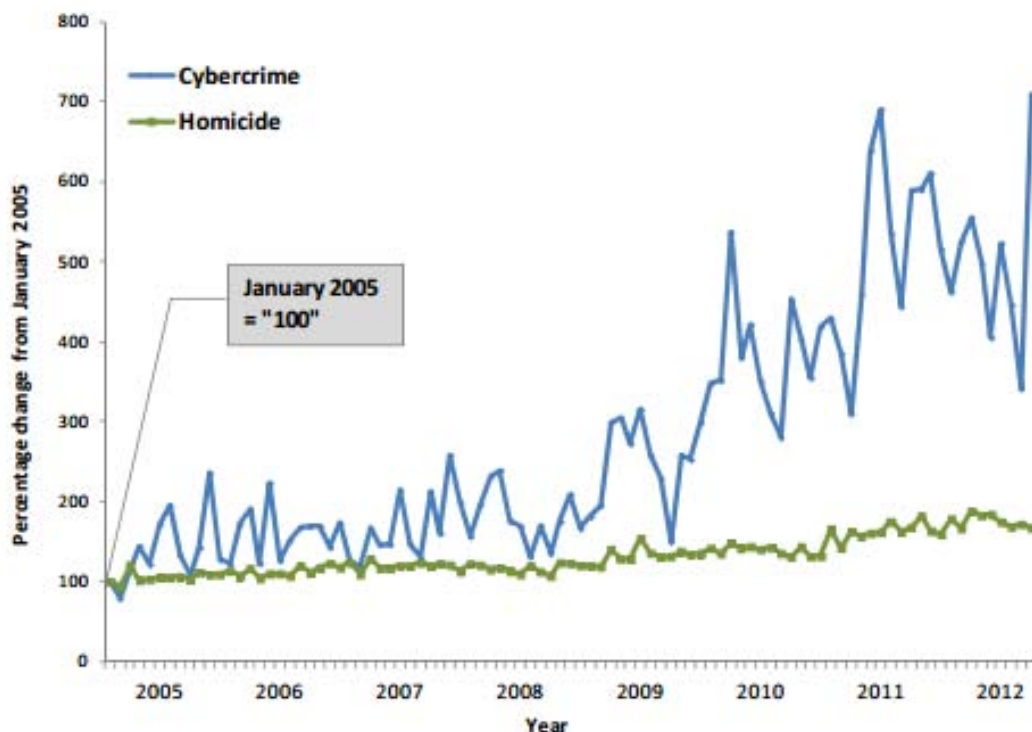
Finalmente, dentro de este reporte se hace una comparación del incremento del tema de los cibercrimenes en medios electrónicos respecto a los homicidios, ello debido a que se ha llegado a convertir en una actividad global por facilidad y lo económico que puede llegar a ser atacar un ordenador.

El documento finaliza haciendo una recomendación sobre la creación de políticas que ayuden a contrarrestar este fenómeno, en donde exista una cooperación entre el gobierno, las empresas privadas, la academia y los usuarios de la red, para crear conciencia sobre el uso de internet y el cómo actuar que hacer en caso de ser víctima de un cibercrimen, además de hacer énfasis en la necesidad de un consenso internacional que ayude a la creación de una cooperación internacional más sólida en materia de cibercrimenes.

⁶⁵ UNODC, *ibidem* pág. 24. Traducción propia

⁶⁶ UNODC, *ibidem* pág. 11

Figure 1.5: Relative frequency of global news reports 2005-2012



Grafica 3. Frecuencia relativa de los reportes globales de noticias. Tomado de UNODC, *ibidem* pág. 7
consultado el 20/04/2016

1.5.2. Ciberguerra

Como vimos anteriormente, Clausewitz en su libro de la guerra argumentaba “La guerra es la mera continuación de la política por otros medios” entonces, bajo esta lógica la ciberguerra es un duelo entre uno o más Estados dentro de un campo de batalla recientemente descubierto y que aún no está regulado: (esta “no regulación” es uno de los principales argumentos de la ciberguerra) el ciberespacio.

El Ministerio de Defensa Español bajo la Orden Ministerial 10/2013, de 19 de febrero de 2013 define a la ciberguerra como “El uso de capacidades basadas en la red de un estado, para interrumpir, denegar, degradar, manipular o destruir información residente en ordenadores y redes de ordenadores, o los propios ordenadores y las redes de otro estado⁶⁷”.

⁶⁷ Ministerio de Defensa Español, óp. cit., pág. 4

Esta definición nos ofrece un aspecto importante que no debe ser pasado por alto; las capacidades que tiene el estado en materia cibernética para afectar o destruir la red de ordenadores del enemigo. Capacidades que no establecen que características deben tener o como pueden ser adquiridas.

Richard A. Clarke, define a la ciberguerra como “la penetración no autorizada en nombre de un gobierno en las computadoras o redes de otra nación, u otra actividad que afecte sistemas computarizados con el propósito de adherir, alterar y falsificar datos o causar la interrupción o el daño a una computadora, a un dispositivo de red, o al objeto que una computadora controla.”⁶⁸

Asimismo, algunos países han definido a la ciberguerra de acuerdo a sus intereses y las características que ellos consideren. Austria por ejemplo nos dice que:

“Guerra cibernética se refiere a actos de guerra en los alrededores de espacio virtual con medios que son predominantemente asociados a las tecnologías de la información. En un sentido más amplio, esto implica el apoyo de las campañas militares en espacios operativos tradicionales - es decir en tierra, mar, aire y espacio exterior - a través de las medidas tomadas en el espacio virtual.”⁶⁹

Si analizamos esta definición, podemos encontrar que la ciberguerra no es un solo ataque son varios que se les denomina “actos de guerra”, además de mencionar que la ciberguerra es la extensión de las guerras tradicionales a un nuevo espacio.

Australia: a través del *Low Intitute for International Policy* nos menciona que la ciberguerra,

“Implica el uso de la tecnología informática, para ser más específicos internet, con el objetivo de interrumpir o degradar las actividades de un adversario. La guerra cibernética está estrechamente relacionado con otros aspectos de la seguridad cibernética, como la delincuencia cibernética, el terrorismo cibernético y el espionaje cibernético, y estas categorías pueden ser difíciles de distinguir. Pero la

⁶⁸ Clarke A. Richard, Knake K. Robert Op. Cit., pág. 230

⁶⁹ NATO, “Cyber definitions”, 2010, en línea, dirección URL: <http://bit.ly/2iYNGP7>, consultado el 12 de enero de 2016. Traducción propia

guerra cibernética tiende a ser practicada por las fuerzas militares y de seguridad de los Estados, cuyo objetivo es degradar la capacidad militar de un adversario con el fin último de coaccionar a ese adversario para un propósito político. Pero la guerra cibernética también incluye el desarrollo e implementación de estrategias de seguridad para defenderse contra las mismas.”⁷⁰

Gran Bretaña a través del diccionario de Oxford define a la ciberguerra como “el uso de la tecnología informática para interrumpir las actividades de un Estado u organización, especialmente el ataque deliberado de los sistemas de comunicación por otro Estado u organización.”⁷¹

Estados Unidos define a la ciberguerra como “el uso de ordenadores para interrumpir las actividades de un país enemigo, especialmente el ataque deliberado de los sistemas de comunicación.”⁷²

Por su parte, la definición rusa nos expone que la ciberguerra es “una escalada del conflicto cibernético entre dos o más estados en los que los ataques cibernéticos se llevan a cabo por agentes estatales contra la infraestructura cibernética como parte de una campaña militar.”⁷³

Techtarget, una empresa estadounidense encargada de proveer servicios online, además de tomar decisiones en el ámbito tecnológico, lo define como

“un conflicto llevado a cabo en Internet que implica ataques por motivos políticos en los sistemas de información y de información. Los ataques de guerra cibernética pueden desactivar sitios web y redes oficiales, interrumpir o desactivar los servicios esenciales, robar o alterar datos de anuncios, y desestabilizar sistemas financieros - entre muchas otras posibilidades.”⁷⁴

Estas definiciones comparten una característica en común que es que la ciberguerra es realizada por agentes estatales contra las infraestructuras cibernéticas del adversario.

⁷⁰ *Ibidem*

⁷¹ *Ibidem*

⁷² *Ibidem*

⁷³ *Ibidem*

⁷⁴ Techtarget, “*Cyberwarfare*” 2012, en línea, dirección URL: <http://bit.ly/1DTuMAB>, consultado el 12 de enero de 2016. Traducción propia

La realidad internacional nos ha superado, se ha creado un espacio que no puede ser controlado y que todos quieren regular para ampliar su margen de seguridad en un mundo cada vez más peligroso. Hoy en día casi todo, funciona con un click, y cada vez más máquinas están conectadas a Internet. La ciberguerra posee características cada vez más evidentes que Richard Clarke nos enlista:



Esquema 2. Características actuales de la ciberguerra. Elaboración propia con información de Clarke A. Richard, Knake K. Robert (traducción de Noriega Luis Alfonso), *“Guerra en la red: Los nuevos campos de batalla”*, Editorial Ariel, Barcelona, 2011, pág. 55.

Académicos mexicanos también se han interesado por la definición del conflicto, como María Cristina Rosas, profesora de la Universidad Nacional Autónoma de México, la cual define a la ciberguerra como:

“[las] acciones desarrolladas por individuos operando en el interior de los Estados, que efectúan acciones ofensivas y/o defensivas en el ciberespacio, empleando computadoras para atacar a otras computadoras o redes a través de

medios electrónicos. El objetivo de estas acciones es buscar ventajas sobre el adversario, al comprometer la integridad, confidencialidad y disponibilidad de la información, en particular la de carácter estratégico. Así, al privar al rival de la información estratégica que requiere para tomar decisiones, se busca debilitarlo y, eventualmente, lograr la victoria sobre él.”⁷⁵

La anterior definición introduce a los actores dentro de la ciberguerra, aquellos que operan las maquinas que atacan, aquellos individuos que están preparados para ejecutar las órdenes de un gobierno: los ciberguerreros, actores que serán analizados en el próximo apartado.

1.5.3. Ciberguerrero

Como se analiza en el apartado previo, los cibercrimenes y ciberataques tienen que ser llevados a cabo por un individuo, el cual debe poseer habilidades para dañar los sistemas informáticos de otro; hablamos de los ciberguerreros

Hoy en día no existe una definición unánime sobre los ciberguerreros, de acuerdo con el trabajo de grado de Edison Vargas:

“Los ciberguerreros son aquellos individuos que con su conocimiento pueden diseñar programas y ciberarmas capaces de infiltrar el sistema de ya sea una organización o entidad, y con esto acceder a información confidencial, colocar bombas lógicas y sabotear el correcto funcionamiento de los flujos de información ya sea de una página de internet, hasta el funcionamiento de la red eléctrica de una ciudad o hasta un país entero.”⁷⁶

De acuerdo a esta definición. ¿Qué diferencias existen entre un hacker y un ciberguerrero? Hay quienes podrían decir que no existe diferenciación alguna, y que incluso su fin es el mismo: debilitar o eliminar al enemigo, pero, la principal diferencia entre un sujeto y el otro radica en que los ciberguerreros están encuadrados dentro de la milicia de un Estado, conocen y dominan el funcionamiento del software y hardware, el fin de los ciberguerreros es proteger al

⁷⁵ María Cristina Rosas, “De la ciberguerra a la ciberpaz”, en línea, revisa Etcétera, 2011, dirección URL: <http://bit.ly/2cPIY6p>, consulta: 13 de febrero de 2013.

⁷⁶ Vargas Vargas, Edison. (2014). Ciberseguridad y Ciberdefensa: ¿Qué implicaciones tiene para la Seguridad Nacional? Especialista en Alta Gerencia de la Defensa Nacional. Universidad Militar Nueva Granada, Facultad de Relaciones Internacionales, Estrategia y Seguridad, en línea, dirección URL: <http://bit.ly/2cWcsAM>, consultado el 20 de abril del 2016

Estado, el de los hackers no se conoce, pero en algunas ocasiones este fin puede ser personal. Más adelante detallaremos el rol de los hackers dentro de este conflicto.

Es entonces cuando al analizar lo dicho anteriormente se puede concluir la siguiente oración: Los ciberguerreros son militares que han sido profesionalizados en temas de ciberseguridad. No lucen diferente a un militar, sus armas cambian ya no es un rifle o un cañón ahora su principal arma es el ordenador que esta frente a ellos.

Richard Clarke ejemplifica esto de manera satírica pero que ejemplifica exactamente la imagen de un ciberguerrero:

“En un anuncio de televisión, un hombre joven, con el pelo cortado a cepillo y un mono paracaidista camina alrededor de un centro de mando oscuro, charla con sus subordinados iluminados por una luz verdosa que emiten las pantallas de sus ordenadores [...] es aquí donde se pelearán las principales batallas [...] entonces el hombre mira directamente a la cámara y dice: *Soy el capitán Scott Hinck, y soy un ciberguerrero de la fuerza aérea*. La pantalla se funde en negro y aparecen las palabras: Aire, espacio y ciberespacio.”⁷⁷

Como hemos visto, la preparación de individuos capaces de hacer frente a los cibercrimenes y a los ciberataques comienza a ser prioritario para los Estados, es por ello que los gastos militares de estos aumenten y con ello la profesionalización en materia de ciberseguridad comience a aumentar dentro del ámbito militar. En un futuro los ciberguerreros podrán actuar en conjunto, creando, posiblemente un ciberejército.

1.5.4. Ciberespionaje

El espionaje no es nuevo, tradicionalmente este consistía en intervenir las comunicaciones del objetivo o enviar un infiltrado para que lograra entrar en las instituciones de otro país con el fin de obtener información relevante capaz de destruir, debilitar o amenazar al enemigo. Por ejemplo, en la Guerra Fría la URSS y EE.UU. recurrieron al espionaje y contraespionaje con el propósito de obtener

⁷⁷ Clarke A. Richard, Knake K. Robert Op. Cit., pág. 57

información del rival. Cada uno contaba con sus agencias que se encargaban de esta actividad, la URSS tenía el ahora extinto Comité para la Seguridad del Estado (KGB por sus siglas en ruso) y su contraparte contaba (y aún cuenta) con la Agencia Central de Inteligencia (CIA por sus siglas en inglés).

Ahora en el siglo XXI el espionaje toma un rumbo distinto, involucrando a las TIC, dando paso al ciberespionaje. Este puede ser considerado como el inicio de los cibercrimenes o ciberataques, y se define como:

“una forma de crimen cibernético en el que los piratas informáticos se dirigen a redes informáticas con el fin de tener acceso a la información clasificada o de otro tipo que pueda ser rentable o ventajosa para el usuario remoto. El Ciberespionaje es un proceso continuo que se produce con el tiempo a fin de obtener información confidencial. Puede dar lugar a todo, desde el desastre económico al terrorismo⁷⁸”.

Entonces, podemos llegar a la conclusión de que el ciberespionaje usará ciberataques “con el fin de conseguir secretos de estado, propiedad industrial, propiedad intelectual, información comercial confidencial o datos de carácter personal⁷⁹”. Este puede ser llevado a cabo por el gobierno, centros de inteligencia, policía, empresas o usuarios de la red para adquirir ventaja política, económica, comercial o militar con la información adquirida en los sistemas atacados.

1.5.5. *Ciberterrorismo*

Después de los atentados del 11 de septiembre de 2001 contra los Estados Unidos, se intensificó el debate sobre el terrorismo. La Oficina Federal de Investigación de los EEUU (FBI por sus siglas en inglés) define al terrorismo como, “el uso ilegal de la fuerza o la violencia contra personas o propiedades a fin de intimidar o cohesionar al gobierno, la población civil o cualquier otro segmento, persiguiendo objetivos sociales o políticos⁸⁰”. Asimismo, el Departamento de Estado lo define de la siguiente manera "El término terrorismo implica actos de

⁷⁸ Cory Janssen, “Cyberspyng”, en línea, Techopedia, Dirección URL: <http://bit.ly/2cMrcgT>, consultado el 04 de junio del 2016

⁷⁹ Centro Criptológico Nacional, “Ciberseguridad. Una prioridad nacional”, en línea, enero 2013, Madrid, España, Dirección URL: <http://bit.ly/2dsSexl>, consultado el 04 de junio del 2016.

⁸⁰ FBI, “Terrorism”, en línea, Estados Unidos, Dirección URL: <http://bit.ly/1nsbpT8>, consultado el 04 de junio del 2016. Traducción propia

violencia premeditada y políticamente motivada perpetrados contra objetivos no combatientes por grupos subnacionales o agentes clandestinos⁸¹".

En los 80, Barry Collin, un investigador senior del Institute for Security and Intelligence en California usó por primera vez el término "cyberterrorism" definiéndolo simple y sencillamente como "la convergencia del ciberespacio con el terrorismo"⁸²

Esta definición nos da una aproximación del alcance de este "nuevo" fenómeno, Daniel Acuña Calviño⁸³ señala que el principal impulsor del ciberterrorismo es precisamente el ciberespacio, ya que este trae problemas o vacíos consigo, como "eliminación de fronteras, anonimato, dificultad en la trazabilidad, falta de regulación internacional, etc⁸⁴". Y el mismo ofrece la siguiente definición sobre ciberterrorismo: "[es] el uso de medios de tecnologías de la información, comunicación, informática, o similar, con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno. Sus fines suelen ser económicos, políticos o religiosos,"⁸⁵ dado lo anterior, podemos hablar de una profesionalización de los terroristas, en donde las TIC toman mayor relevancia para infundir el miedo entre la población, Gabriel Weimann⁸⁶, identifica ocho maneras en la que los ciberterroristas atacan y que se representan en el esquema 3.

⁸¹ U.S. Department State, "Terrorism" ", en línea, Estados Unidos, Dirección URL: <http://bit.ly/1efkxtF>, consultado el 4 de junio del 2016. Traducción propia.

⁸² Collin Barry, "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge", en línea, Estados Unidos, Dirección URL: <http://bit.ly/2dfVXiQ>, consultado el 4 de junio del 2016

⁸³ Director de Defensa y Seguridad en Ingeniería de Sistemas para la Defensa de España (ISDEFE) en Madrid, España

⁸⁴ Acuña Calviño Daniel, "Ciberterrorismo, un reto para los próximos años", en línea, Madrid, España, Revista electrónica DINLET (Difusión de las Ingenierías informática y telecomunicaciones), marzo 2010, p.88, Dirección URL: <http://bit.ly/2djkmEC>, consultado el 04 de junio del 2016.

⁸⁵ *Ídem.*

⁸⁶ Senior Fellow en el United States Institute of Peace y profesor de comunicación en la Haifa University



Esquema 3. Ocho maneras de ataque hechas por los ciberterroristas. Elaboración propia con información de WEIMANN Gabriel "www.terror.net How modern Terrorism uses the Internet", en línea, Special Report No. 116, United States Institute of Peace, 2004, págs. 5-11, Dirección URL: <http://bit.ly/2cCjoAB>, consultado el 13 de junio del 2016

1.5.6. *Ciberactivismo y Hacktivismo*

Como hemos visto anteriormente, es inevitable que exista una interacción limitada entre los usuarios y el ciberespacio. Es por ello que el ciberespacio es una plataforma para nuevas formas de manifestación de estos usuarios, como lo son el ciberactivismo y el hacktivismo, llegando a generar cierto descontento entre los gobiernos y empresas. Pero existen diferencias entre estos dos conceptos.

Ambas actividades tienen un objetivo en claro, influir ya sea en la política nacional o internacional y con ello generar un cambio de determinada situación o descontento social.

“[El ciberactivismo] se refiere al uso normal y no destructivo de internet en función de una causa u objetivo. Las operaciones en esta área incluyen la búsqueda de información en las páginas web, construir sitios en internet y ofrecer documentación en ello, editar publicaciones electrónicas, enviar cartas mediante el correo electrónico, usar internet como espacio y foro de debate, formar coaliciones, planificar y coordinar actividades. Incluye por tanto las dimensiones anteriormente tratadas de

la democracia electrónica en el ámbito no convencional de los movimientos sociales: la información y la coordinación.”⁸⁷

El ciberactivismo no tiene por objetivo causar daños o miedo entre los demás usuarios del ciberespacio, solo usan a este espacio como medio para exigir demandas, defender o rechaza alguna causa u objetivo.

El Hacktivismo por su parte, es definido por Tim Jordan académico de la Universidad de Stanford como la:

“Acción directa de una muchedumbre virtual (Mass Virtual Direct Action) que prolonga y acompaña al activismo político no violento de la vida real. Las operaciones que abarca, emplea técnicas de hacker contra objetivos de sitios en internet con la intención de distorsionar las operaciones normales pero no causar daños serios; como por ejemplo son las sentadas y bloqueos de páginas (virtual sitins, virtual blockades), el envío automático y masivo de correos electrónicos con el efecto de bombas (e-mail bombs), alterar los contenidos de una página web (hacking), transmitir virus y gusanos para romper ordenadores o destruir un sistema (cracking).”⁸⁸

Entonces, podemos detectar que la principal diferencia entre el ciberactivismo y el Hacktivismo radica en la intención del atacante. Cuando se busca crear conciencia sobre alguna demanda o algún hecho se recurre al ciberactivismo, pero cuando se busca hacer algún daño momentáneo (no permanente ni serio) se recurre al hacktivismo.

1.5.7. Ciberataque

Con excepción del ciberactivismo, los fenómenos anteriores tienen un elemento en común, todos utilizan los ciberataques para alterar, dañar o eliminar la información del enemigo. Pero ¿qué es un ciberataque? La Orden Ministerial

⁸⁷ (como se cita en Fernández Prados Juan, *Ciberactivismo: conceptualización, hipótesis y evaluación*, 2013, p. 6) Denning, Dorothy E. “*Activism, Hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy*”, en Arquilla, J. y Ronfeldt, D. F. 2011, (Ed.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, Rand, pp. 239-288.

⁸⁸ (como se cita en Fernández Prados Juan, *Ciberactivismo: conceptualización, hipótesis y evaluación*, 2013, p. 6), Jordan, T Y Taylor, P. “*Hacktivism and Cyberwars: rebels with a cause?*”, Routledge, 2004

10/2013 del ministerio de defensa español define a un ciberataque de la siguiente manera:

“Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.”⁸⁹

La Asociación de Auditoría y Control de Sistemas de Información (ISACA por sus siglas en inglés) una asociación internacional se encarga de apoyar y patrocinar el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información. Define a un ciberataque como “toda acción intencionada que se inicia en un equipo informático, con el objetivo de comprometer la confidencialidad, disponibilidad o integridad del equipo, red o sitio web atacado y de la información contenida o transmitida a través de ellos⁹⁰”.

Dentro de la lógica de los ciberataques son necesarias dos partes uno, el individuo que sea capaz de dominar el ciberespacio y que sea capaz de crear un virus capaz de afectar el sistema, y dos, el “equipo informático” (computadora) en donde trabaja el usuario. Pero dependerá de la intención de este la gravedad del ciberataque, es por ello que a continuación se enlista una categorización.

⁸⁹ Ministerio de Defensa Español, Óp. Cit.

⁹⁰ ISACA, “Ciberataques. ¿Estamos preparados?”, en línea, Buenos Aires, Dirección URL: <http://bit.ly/2cE5RIN>, consultado el 20 de junio del 2016.

1.5.8. Categorización de los ciberataques

En la ciberguerra, los actores tendrán diferentes intenciones al ejercer un ciberataque, el Centro de Génova para el Control Democrático de las Fuerzas Armadas (DCAF, por sus siglas en inglés) ejemplifica en un cuadro de manera detallada los tipos de ciberataques.

Categorías de los ciberataques		
Categoría	Subcategoría	Ejemplos
Integridad Los ciberataques pueden utilizar técnicas de hacking para modificar, destruir o hacer otras acciones que comprometan la integridad de los datos.	Propaganda/desinformación	Modificación o manipulación de datos o introducción de datos contradictorios para influir en resultados políticos o de negocios o desestabilizar un régimen extranjero.
	Intimidación	Ataques a sitios web para ejercer coerción sobre sus propietarios (públicos o privados) para remover o modificar contenido o perseguir otros fines.
	Destrucción	Destrucción permanente de datos para afectar competidores o atacar gobiernos extranjeros. Puede ocurrir, por ejemplo, dentro de un conflicto a gran escala.
Disponibilidad Ataques de negación de servicio ejecutados por	Información Externa	Accesos denegados, etc. Ataques contra servicios del gobierno o privados disponibles para el público, por ejemplo, medios de comunicación, sitios de información gubernamentales, etc.

<p>botnets, por ejemplo, pueden ser usados para prevenir que usuarios acceden a datos que de otra manera no estarían disponibles.</p>	<p>Información Interna</p>	<p>Ataques a intranets gubernamentales o privadas, por ejemplo, redes de servicios de emergencia, sitios de banca electrónica, email corporativo, sistemas de control y comando, etc.</p>
<p>Confidencialidad Los ciberataques pueden apuntar a varios tipos de información confidencial, a menudo para propósitos criminales.</p>	<p>Espionaje</p>	<p>Firmas buscando información sobre sus competidores; estados envueltos en actividades espías (en contra de gobiernos extranjeros e individuos.)</p>
	<p>Robo de datos personales</p>	<p>Suplantación de identidad (o similares) dirigidos a usuarios débiles que engañados revelan datos personales, como números de cuentas bancarias; virus que almacenan y suben datos desde una computadora de un usuario.</p>
	<p>Robo de identidad</p>	<p>Troyanos, y demás, usados para robar la información de identidad y usarla para cometer crímenes.</p>
	<p>Extracción de datos</p>	<p>Técnicas de código abierto empleadas para descubrir, por ejemplo, información personal de los datos a disposición del público.</p>
	<p>Fraude</p>	<p>Con frecuencia enviado vía email mediante spam, el fraude incluye el popular nigeriano “419” o técnicas avanzadas de fraude, así como intentos de convencer al destinatario para comprar bienes o servicios fraudulentos.</p>

Tabla 3. Categorización de los ciberataques. Tabla tomada de: DCAF, Democratic Governance Challenges of Cyber Security, [en línea], Génova, DCAF, 2009, Dirección URL: <http://bit.ly/2cx8Apa>. Traducción y elaboración propia.

Esta tabla nos demuestra los diversos objetivos que tienen los ciberataques, no hay que dejar de lado que todos estos suceden dentro del ciberespacio y que se debe tener un amplio conocimiento para poder realizarlos.

1.6. Antecedentes de ataques cibernéticos alrededor del mundo

Como se ha demostrado, los ciberataques son fáciles de hacer, personas con el conocimiento adecuado pueden crear grandes catástrofes a nivel internacional. El siglo XXI marcó el inicio de una era: La era de los ciberataques.

Año	País Atacante	País atacado	Descripción
1982	Estados Unidos	URSS	Objetivo: gaseoducto soviético en Siberia En junio de 1982 los satélites estadounidenses que orbitaban sobre la Unión Soviética fotografiaron la explosión no nuclear más grande registrada hasta la fecha. A través de un doble agente soviético, la CIA consiguió hacer llegar al KGB un software defectuoso para controlar el transporte de gas: afectaba al control de la presión del gas en los gaseoductos y sería el culpable de la gran explosión ⁹¹ .
Entre 1998 y 2000	Rusia	Estados Unidos	Objetivo: sistemas informáticos del Pentágono, la NASA, el Departamento de Energía estadounidense y, también, universidades privadas de EE UU Los intrusos en los sistemas informáticos tuvieron acceso a miles de documentos clasificados, muchos de ellos relacionados con información del Ejército: mapas de instalaciones militares, por ejemplo, o planes de despliegue de tropas. Se rastreó la procedencia del sofisticado asalto hasta conexiones ubicadas en Rusia. Las autoridades rusas negaron estar implicadas ⁹² .
1999	Kosovo	Estados Unidos	Objetivo: penetrar en los ordenadores estratégicos de Estados Unidos y la OTAN Más de 450 expertos informáticos, "web master", hackers, periodistas, ingenieros e intérpretes yugoslavos combaten durante 24 horas al día contra los ordenadores aliados. Es el

⁹¹ González Veiguela Lino "Los ciberataques (conocidos) más importantes", en línea, Julio 2013, Dirección URL: <http://bit.ly/2cUte0W>, consultado el 26 de junio del 2016

⁹² *Ídem*

			ejército voluntario del célebre "Capitán Dragan", héroe nacional serbio durante la guerra de la Krajina (Croacia) ⁹³ .
2003	China	Taiwán	Objetivo: Hospitales, La bolsa, y algunos sistemas de control de tráfico. Fue un ciberataque que dejó sin servicio a estas infraestructuras. Mediante ciberataques de denegación de servicio (DDoS), virus y troyanos ⁹⁴ .
2007	Israel	Siria	Objetivo: defensas antiaéreas de Siria En septiembre de 2007, la aviación israelí llevó a cabo un ataque contra supuestas instalaciones nucleares sirias. Según Israel, Siria estaba desarrollando un programa nuclear con la ayuda de expertos y tecnología procedentes de Corea del Norte. La operación Huerto habría comenzado a gestarse a finales de 2006, cuando agentes del Mossad accedieron al ordenador portátil que un alto oficial sirio tenía en su habitación de un lujoso hotel londinense. Para hacerse con esa información usaron viejos métodos: allanamiento de morada. Aprovecharon la operación para inocular en el portátil un virus troyano con la intención de que les continuara suministrando información. ⁹⁵
2007	Rusia	Estonia	Objetivo: Infraestructuras críticas estonias En Estonia las páginas oficiales de varias provincias estonias, las del Gobierno y las del Partido de las Reformas quedaron paralizadas por ataques informáticos provenientes del exterior. Al mismo tiempo que los sistemas de algunos bancos y periódicos resultaron bloqueados durante varias horas por una serie de ataques distribuidos de denegación de servicios ⁹⁶ .

⁹³ EL PAIS, Fuentes Julio, "Guerra informática en Serbia", en línea, Abril 1999, España, Dirección URL: <http://bit.ly/2di65Fu>, consultado el 26 de junio del 2016.

⁹⁴ IEEE, Ureña Centeno Francisco, "Ciberataques, la mayor amenaza actual", en línea, Enero 2015, España, dirección URL: <http://bit.ly/1yj9NFt>, consultado el 26 de junio del 2016.

⁹⁵ González Veiguera Lino, Óp. Cit.

⁹⁶ Sánchez Medero Gema, "La ciberguerra: los casos de Stuxnet y Anonymous", en línea, Revista Derecom No. 11. Nueva Época. Septiembre-Noviembre, 2012, dirección URL: <http://bit.ly/2dxTsUA>, consultado el 26 de junio del 2016.

2008	Rusia	Georgia	<p>Objetivo: páginas del gobierno</p> <p>En agosto del 2008, pocos días antes del inicio de la breve guerra entre Georgia y Rusia por el control de Osetia del Sur, medios de comunicación y webs de instituciones georgianas y azerís comenzaron a sufrir ataques que inutilizaron su funcionamiento. En la página del Ministerio de Asuntos Exteriores georgiano apareció la imagen del presidente, Mikheil Saakashvili, caracterizado como Hitler antes de bloquearse su funcionamiento⁹⁷.</p>
2009	China	Estados Unidos	<p>Objetivo: los sistemas informáticos de hasta 34 compañías estadounidenses como Google, Yahoo, Symantec, Adobe, Northrop Grumman y Dow Chemical, entre otras.</p> <p>Operación Aurora. A principios de 2010, Google denunció que había detectado un ciberataque procedente de China que habría vulnerado el muro de seguridad de la compañía y tenido acceso a sus servidores. En un primer momento, se denunció que los atacantes querían sobre todo tener acceso a las cuentas del correo electrónico (gmail) de destacados opositores chinos, como Ai Weiwei. Google no facilitó la investigación puesta en marcha por el FBI en su sede de Mountain View y comenzó una disputa legal con la agencia de seguridad estadounidense para impedir que sus agentes pudiesen acceder a información sensible de la compañía relacionada con su funcionamiento técnico⁹⁸.</p>
2011	China	Canadá	<p>Objetivo: Ministerio de finanzas</p> <p>Según algunas informaciones, los asaltantes tomaron el control del sistema de contraseñas del ministerio de Finanzas en enero. Aunque las máquinas utilizadas estaban en territorio chino, no se tiene la seguridad de que los atacantes fueran de esta nacionalidad o simplemente las utilizaron remotamente⁹⁹.</p>
2012	Irán	Arabia Saudita y Qatar	<p>Objetivo: los sistemas informáticos de la compañía saudí de petróleo Aramco y de la segunda empresa gasística mundial, la catari RasGAs</p> <p>Los ataques contra Aramco y RasGas se produjeron con</p>

⁹⁷ González Veigueta Lino, Óp. Cit.

⁹⁸ *Ídem*

⁹⁹ *Ídem*

			pocos días de diferencia en agosto de 2012. Una de las características principales del virus Shamoon es que, además de robar información de los sistemas informáticos, borra grandes cantidades de datos de los sistemas infectados. Algunas fuentes señalaron que hasta treinta mil ordenadores de Aramco pudieron sufrir los efectos de Shamoon: la pérdida podría ascender hasta los tres cuartos de todos los datos almacenados por la empresa estatal saudí ¹⁰⁰ .
--	--	--	---

Tabla 4. Principales ciberataques a nivel mundial. Elaboración propia tomado con datos de diversas fuentes

1.7. Balance crítico respecto a las diferencias entre ciberdefensa y ciberseguridad

Como lo hemos visto a lo largo de este capítulo, los conflictos en el ciberespacio son ya una realidad, protegerse ante un posible ciberataque es necesario e importante. Es en este punto donde suelen confundirse y estudiarse dos aristas de este fenómeno: la ciberseguridad y la ciberdefensa. Ambos conceptos suelen ser confundidos pero cada uno posee diversas características.

La ciberdefensa se encuentra inmersa dentro de la ciberseguridad, es decir, la primera se va a encargar de ejecutar las tácticas y planes que se establezcan en una estrategia de ciberseguridad.

La ciberdefensa es definida como el,

“Conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control, la información que manejan, y garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos¹⁰¹”.

Entonces podremos hacer la diferenciación de ambos conceptos, es el Estado quien se encargará de crear las acciones, medidas y políticas de ciberseguridad, en ellas pueden intervenir otros actores como lo son la academia, empresas privadas o incluso usuarios dedicados a encontrar fallas en las redes.

¹⁰⁰ *Ídem*

¹⁰¹ Ministerio de Defensa Español, óp. cit., pág. 6

Por otro lado, la ciberdefensa será única y exclusivamente ejecutada por el ámbito militar, ningún otro actor interviene y el objetivo final será precisamente, el proteger al Estado de ciberataques que puedan dañar infraestructuras críticas importantes que se encuentren dentro de él.

CAPÍTULO II. Ciberseguridad en Estados Unidos: Un tema ¿nuevo? de su agenda

“Las amenazas a la seguridad de un país van más allá de los misiles y los drones: el ciberespacio es un nuevo lugar para la guerra y EE UU ha convertido el asunto en una prioridad y quiere hacer del ataque la mejor defensa. Los presupuestos de Defensa en EE UU no pasan por el mejor momento tras la aprobación de una reducción paulatina de 500.000 millones de dólares en los próximos diez años. A pesar de ello, el Departamento de Defensa prevé quintuplicar sus esfuerzos en seguridad cibernética de manera inmediata¹⁰²”.

Como hemos visto, la ciberseguridad involucra a diversos actores de la sociedad internacional, el gobierno, las empresas privadas y los ciudadanos están cada vez más involucrados en este proceso, los cuales crecen día con día debido a la evolución de las tecnologías de la información y comunicación.

Es por este proceso evolutivo de las TIC's que los Estados se han visto en la necesidad de crear mecanismos de protección en este “nuevo” espacio de lucha contra las ciberamenazas.

El caso de Estados Unidos es particularmente especial, ya que ha sido uno de los principales pioneros e impulsores de crear una conciencia sobre el uso y la regulación del ciberespacio en un entorno de hostilidad y en donde sus principales enemigos pueden atacarlo, por ser un espacio altamente vulnerable.

En este capítulo estudiaremos la evolución del término “ciberseguridad en la agenda de Estados Unidos, así como las tácticas y principales acciones que ha impulsado este país a nivel nacional e internacional, a través de su influencia en diversos organismos internacionales.

¹⁰² Vid. 20 minutos.es “Estados Unidos potencia la ciberseguridad por miedo a un Pearl Harbor informático” 31 de enero del 2013 , en línea, dirección URL: <http://bit.ly/1Slolgc>, consultado el 6 de noviembre del 2015

2.1. La evolución de la ciberseguridad en EE.UU a través del tiempo.



1958. Creación de ARPA

ARPANET
THE FIRST INTERNET

1969. Nace ARPANET



1971. Invención del correo electrónico. ARPANET ya contaba con 15 nodos.

Octubre 1972. ARPANET se presenta al público en la "International Conference on Computer Communications (ICC). ARPA se convierte en DARPA



1964. Primera estructura de ARPANET. Una red tipo "araña".

Septiembre – Noviembre de 1969. Instalación de los primeros nodos de ARPANET (UCLA-U. Stanford-U. California – U. Utah

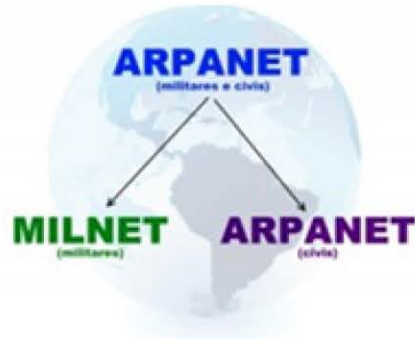


1972. Aparición del primer virus informático: creeper



2.1. La evolución de la ciberseguridad en EE.UU a través del tiempo.

1973.
ARPANET realizaba su primera conexión internacional entre la University College of London (Inglaterra) y el Royal Radar Establishment (Noruega)



División de ARPANET



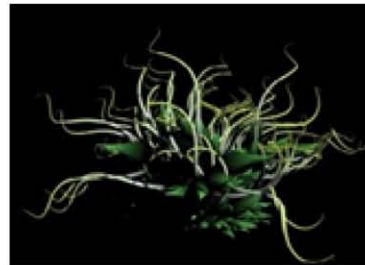
Juicio contra Robert Tappan Morris, creador del virus. Acusado de daños al gobierno de Estados Unidos.



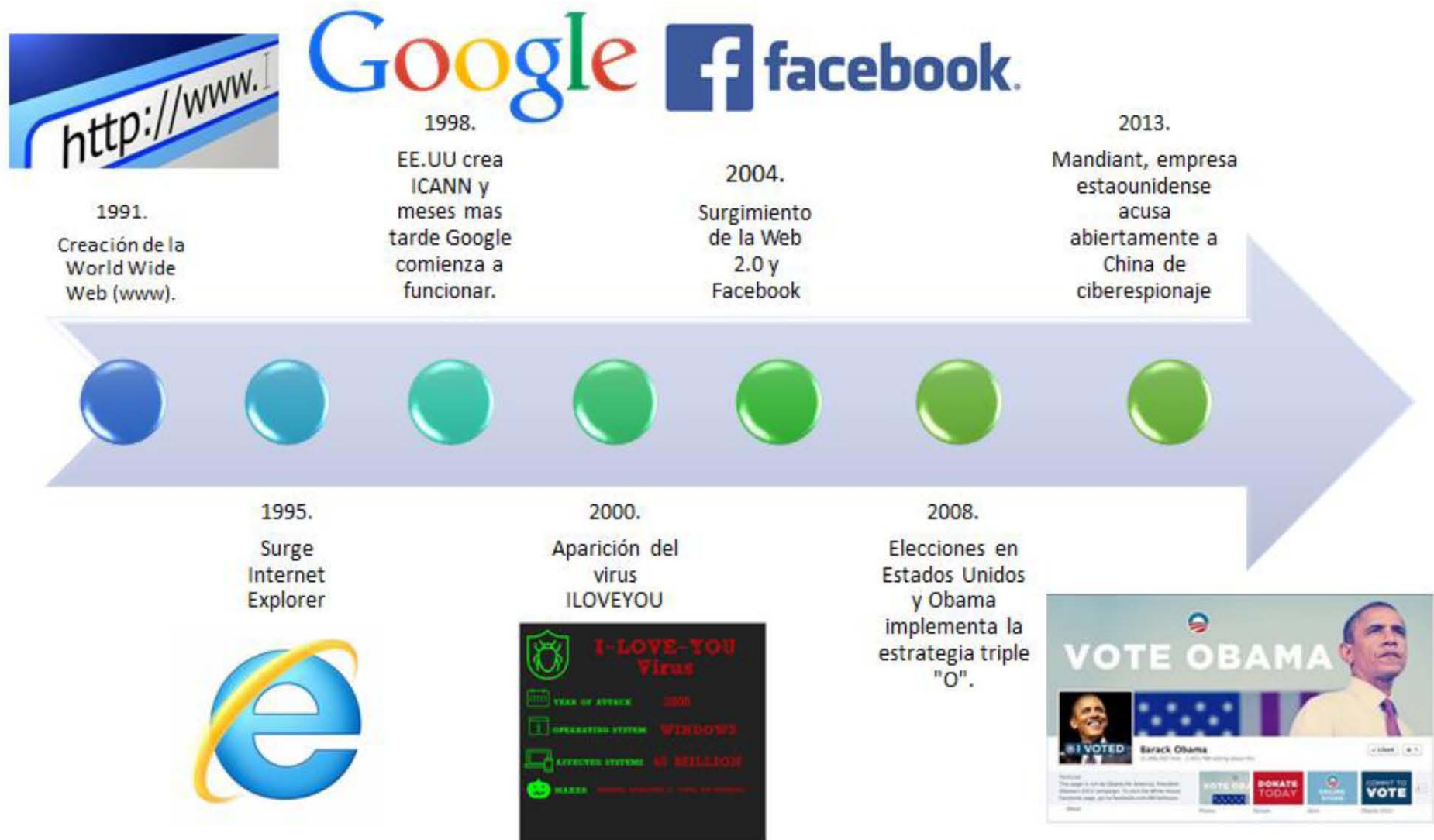
1978.
Creación del TCP/IP



1988.
Aparición del gusano "Morris".
Ante esto se crea el CERT



1990.
ARPANET desaparece y su lugar lo ocupan los protocolos TCP/IP



Esquema 4. Línea del tiempo. Elaboración propia tomando datos de diversas fuentes

2.1. La evolución de la ciberseguridad en EE.UU a través del tiempo.

El término ciberseguridad podría parecer nuevo, pero no es así, desde la aparición de la primera computadora en Estados Unidos (que curiosamente fue una red que solo se ocuparía con fines militares), se pensaba en que se debía hacer para poder proteger y evitar posibles daños a futuro.

Para entender la actualidad de la ciberseguridad y las medidas que los Estados y sobretodo Estados Unidos están tomando para protegerse de los ciberataques, es necesario hablar del origen del internet, el cual, tuvo sus orígenes en este país.

Después de la Segunda Guerra Mundial, comienza la Guerra Fría; un periodo de lucha ideológica, política y económica entre EE.UU. y la hoy extinta Unión Soviética. Pero no solo estos tres aspectos eran los que había que dominar, también estaba el terreno militar y tecnológico que iban de la mano: a mayor tecnología mejores armas para atacar al “enemigo”.

El 4 de octubre de 1957 la Unión Soviética comenzaría esta “lucha tecnológica” con el lanzamiento en órbita del *Sputnik 1*, “primer satélite artificial del mundo cuyo tamaño era de (58 cm. por 22.8 pulgadas de diámetro), sólo pesaba 83,6 kg. o 183.9 libras, y tomó cerca de 98 minutos a la órbita de la Tierra sobre su trayectoria elíptica¹⁰³”. Posteriormente, la URSS lanzaría más Sputniks, lo cual alertó al gobierno estadounidense y con ello creó nuevas estrategias para combatir a su enemigo.

La amenaza de un conflicto nuclear era cada vez más real, sería necesario crear “algo” capaz de controlar a los misiles desde distintos dispositivos, y con ello aumentar la capacidad de respuesta ante un posible ataque. “La única posibilidad de tener un cierto éxito en la defensa era utilizar ordenadores que controlasen y

¹⁰³ Vid. Administración Nacional de la Aeronáutica y del Espacio, conocida como NASA (National Aeronautics and Space Administration), “*Sputnik and The Dawn of the Space Age*”, EE.UU., NASA Main Page Multimedia Interactive Feature on 50th Anniversary of the Space Age, 10 de octubre del 2007, Dirección URL: <http://go.nasa.gov/1pww18b>, [consultado: 06 de noviembre de 2015]. Traducción Propia.

evaluasen todo; además, como es lógico, estos equipos debían estar comunicados entre sí [...] el siguiente paso era diseñar su estructura.”¹⁰⁴

Por lo anterior, la U.S Air Force solicitó a un grupo de investigadores que diseñaran la red ideal, esto a través de un estudio que contemplaba el control de los misiles en caso de un ataque nuclear, es decir, que si una parte de esta red era destruida pudiera seguir funcionando sin ningún problema desde otro ordenador.

“Si se tomaba como referencia las redes de las grandes empresas y centros científicos, ahí el asunto era muy claro: las redes estaban centralizadas, de modo que la conexión entre dos terminales siempre tenía lugar a traves de un servidor central. Sin embargo, en aquella tesitura esa alternativa no parecía muy aconsejable, porque si un misil impactaba en el servidor central, la red dejaría de estar operativa. Así que se adoptó una decisión revolucionaria, que no hubiera nodos centrales y, de este modo, la información dispusiese de múltiples caminos para viajar de un equipo a otro.”¹⁰⁵

Es así, como en 1964 Paul Baran, uno de los investigadores encargados de crear esta nueva estructura, inventa una red tipo “araña” la cual se encargaría de buscar la ruta más clara y rápida además de “esperar” en caso de que todas las demás rutas fueran inaccesibles por alguna razón. A este nuevo sistema se le denomino “conmutación de paquetes”.

Como consecuencia de todas estas investigaciones en 1969 nace ARPANET nombre que se compone por las siglas de ARPA y NET (network, red).

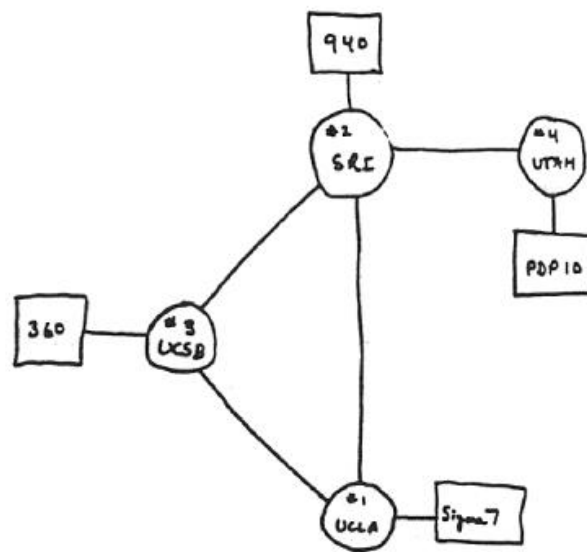
“Esta red se basaba en el principio de ser totalmente distribuida, es decir, basada en la agregación de redes independientes de menor envergadura. De esta manera, se intentaba que fuera suficientemente robusta ante los ataques, que si una o varias de las redes menores dejaban de operar,

¹⁰⁴ Trigo Aranda Vicente, *“Ciencia Divulgativa: Del Abaco A Internet”*, Editorial Creaciones Copyright, S/L, 2010, pág. 123

¹⁰⁵ *Ibidem*, pág. 124

Internet puede seguir funcionando, aunque fuera con una capacidad reducida. Pero no se detendría completamente¹⁰⁶.

ARPANET estaría compuesta por cuatro nodos conectados gradualmente en cuatro de las universidades más importantes en Estados Unidos. En septiembre se instalaría el primer nodo en la Universidad de California de Los Ángeles (UCLA), en octubre lo hacen en el Instituto de Investigación de Stanford, en noviembre lo instalan en la Universidad de California en Santa Bárbara y, finalmente, el último nodo estaría en la Universidad de Utah (Imagen 1).



THE ARPA NETWORK

DEC 1969

Imagen 1. Boceto inicial de ARPANET. Fuente: Lujan Mora Sergio, “Programación de aplicaciones web: historia, principios básicos y clientes web”, Editorial Club Universitario, Alicante, 2002, pág. 12

¹⁰⁶ Marco Galindo María de Jesús, “Escaneando la Informática”, UOC (Universitat Oberta De Catalunya), 2010, pág. 75

En 1971 ARPANET contaba con 15 nodos conectados a Internet (imagen 2). “Posteriormente en este año sería inventado por Ray Tomilson el correo electrónico, cuyo primer mensaje fue QWERTYUIOP, “@” ya era utilizado como un signo que separaba al nombre de usuario del resto de la dirección.”¹⁰⁷

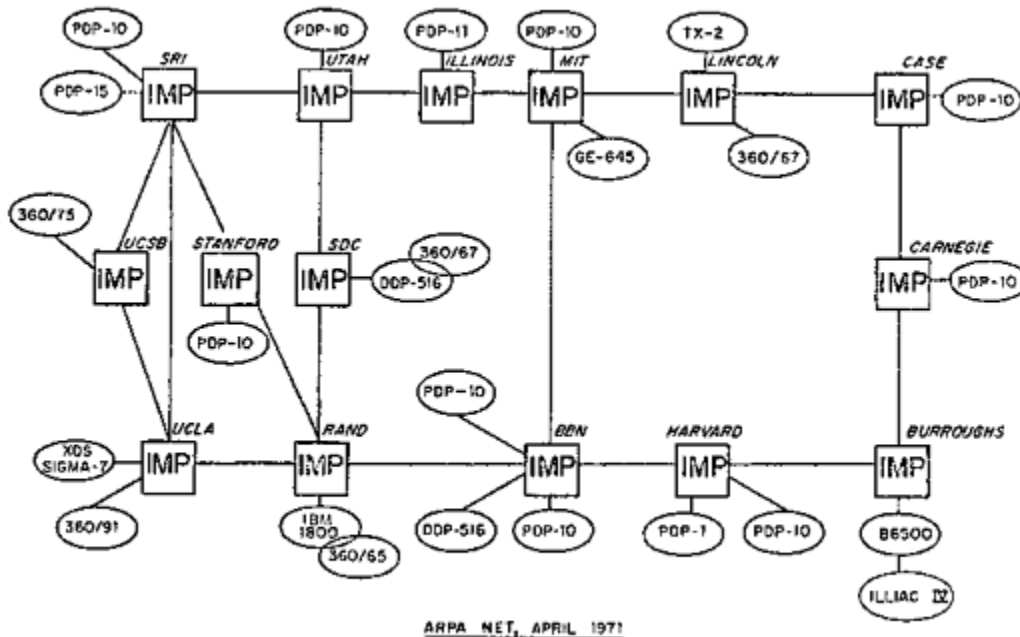


Imagen 2. ARPANET en 1971. Fuente: *Ibidem*, pág. 13

ARPANET era sinónimo de desarrollo tecnológico que innovaría en el campo militar, pero no era sinónimo de seguridad y esto se vio en 1972 con la aparición del primer *virus*¹⁰⁸ informático: creeper. “Ataco a una maquina IBM tipo serie 360 [...] el software emitía periódicamente en la pantalla el mensaje «I'm a creeper... catch me if you can!» (¡Soy una enredadera... atrápame si puedes!). Para eliminar este problema se creó el primer programa antivirus denominado reaper (cortadora).”¹⁰⁹

¹⁰⁷ Lujan Mora Sergio, “Programación de aplicaciones web: historia, principios básicos y clientes web”, Editorial Club Universitario, Alicante, 2002, pág. 13

¹⁰⁸ El término “virus” no era conocido aun en esta época, el concepto sería aceptado una década más tarde.

¹⁰⁹ David Gallo Facundo, “Inseguridad informática”, S/E, Madrid, 2012, pág.221- 222

Es necesario señalar que Creeper era un proyecto experimental, con el objetivo de saber si este “virus” era capaz de moverse y reproducirse entre ordenadores del mismo sistema operativo dentro de ARPANET.

En octubre de 1972 ARPANET se presentó al público en la “International Conference on Computer Communications (ICC) celebrada en Washington D.C.¹¹⁰”, es en estas fechas que ARPA se convierte en la Agencia de Proyectos Avanzados de Investigación para la Defensa (DARPA por sus siglas en ingles). Para esta fecha ya eran 32 los nodos conectados en la red ARPANET.

Para 1973 esta red ya realizaba su primera conexión internacional, las universidades seleccionadas para esta hazaña eran la University College of London (Inglaterra) y el Royal Radar Establishment (Noruega)¹¹¹

A mediados de este año, Robert Kahn (que se unió a la Oficina de Técnicas de Procesamiento de la Información como director de programa en 1972) y Vinton Cerf, de la Universidad de Stanford colaboraron en un proyecto para desarrollar nuevos protocolos de comunicación para el envío de paquetes de datos a través de la ARPANET.

A raíz de esta investigación publican *A Protocol for Packet Network Interconnection*, en “IEEE Transactions on Communications”, en donde dan a conocer la creación del Protocolo de Control de Transmisión (TCP). Además es en esta publicación en donde aparece por primera vez el término “Internet”, pero es hasta 1978 donde el término se divide en TCP/IP (Protocolo de Internet). “TCP se encargará de la comunicación extremo a extremo e IP de proceso de direccionamiento.”¹¹²

Ya en 1983 ARPANET es oficialmente usada en todo el mundo pero sin dejar de ser usada en materia militar, es por ello que se divide en “MILNET

¹¹⁰ Óp. Cit. Lujan Mora, pág.13

¹¹¹ *Ibidem* pág. 13.

¹¹² *Ibidem* pág. 14.

(formada por 45 nodos de carácter militar y ARPANET (formada por 68 nodos de carácter civil).”¹¹³

ARPANET marcaría un hito en cuanto a tecnología se refiere durante varios años, pasaría de ser usado solo por militares a ser usado por civiles. Incluso las grandes corporaciones dedicadas a la fabricación de computadoras repuntarían gracias al uso del ahora llamado Internet, como “IBM (quien) presenta sus primeros computadores personales a un precio de 4.500 dólares con una sorprendente repercusión logrando vender más de 65.000 unidades tan solo en los primeros cuatro meses.”¹¹⁴

Desafortunadamente, el gran invento que resultaría ser ARPANET, el trabajo y el equipo que estuviera detrás de su elaboración, dio pie a que otras personas comenzaran a pensar en si esta red era tan segura e impenetrable como se presumía; el 2 de noviembre de 1988 quedaría claro que no, marcando la historia del internet y la ciberseguridad.

Ese día se detectó un código malicioso capaz de reproducirse en todas las computadoras conectadas a ARPANET, este virus recibió el nombre de *Gusano Morris* “Programado por Robert Tappan Morris, el cual fue capaz de afectar al 10% aproximado de las maquinas conectadas en aquella época a la Red, cerca de 6.000, incluyendo equipos de organizaciones gubernamentales como la NASA [...] intentaba averiguar las contraseñas de acceso a otras computadoras.”¹¹⁵

A partir de este momento empresas, académicos dedicados a la informática, programadores y sobretodo gobiernos, se enfrentaron a la realidad de ARPANET, es decir, la vulnerabilidad ante un ataque de esta magnitud; el cual deshabilitaría en un 10% a la mayoría de las máquinas que estaban en la red, sobretodo estadounidenses.

¹¹³ *Ibidem* pág. 15.

¹¹⁴ Vid S/A, “*Internet y la World Wide Web*”, 1998, en línea, dirección URL: <http://bit.ly/1p1U36S>, consultado el 6 de noviembre del 2015.

¹¹⁵ Sábada Chalezquer Charo, Domingo Prieto Victor, et al. “*La protección y seguridad de la persona en internet: Aspectos sociales y Jurídicos*”, Editorial REUS, Madrid, España, 2014, pág. 90.

Robert Morris, estudiante de 23 años, afirmó que fue un error esparcir este gusano. “El programa tenía una amplia capacidad para reproducirse, pero el propio Morris aseguro que jamás pensó que se propagaría a esa velocidad y tan extensamente¹¹⁶”.

En esa época, el golpe de Morris fue catastrófico, ya que generó dudas sobre la seguridad de ARPANET, además, si un estudiante de 23 años podía crear un virus que provocara estos daños, evidenciaba que una persona aún más especializada podía invadir la red. Lo siguiente en la agenda era la captura de Morris, su proceso penal y lo más importante: conseguir una copia del gusano para analizarlo y con ello ver su programación y sus capacidades de ataque y destrucción.

“Cuando se pudo aislar el código y estudiarlo, se descubrió que el gusano estaba realmente programado por dos desarrolladores. Todo parecía indicar que Robert Morris utilizó parte de los programas creados por su padre en los años sesenta: El juego consistía en crear un programa que al reproducirse fuera ocupando toda la memoria, al tiempo que borraba de ella al programa del contrincante¹¹⁷”.

Finalmente, Morris fue presentado ante las autoridades correspondientes en enero de 1990, fue sometido a un juicio “[...] se le acusó de atacar al gobierno de los Estados Unidos. Fue declarado culpable por un jurado federal, lo que convirtió a Morris en la primera persona condenada por la ley de fraudes informáticos de 1986¹¹⁸”. No obstante, el juez encargado dictaminó que las acusaciones hacia Morris no eran del todo correctas, por lo cual, su sentencia fue reducida “a tres años de libertad condicional, 400 horas de trabajo social y una multa de 10.050 dólares¹¹⁹”.

Como era de esperarse, la respuesta del gobierno estadounidense no quedaría solo en el juicio contra Morris,

¹¹⁶ Vid López Michelone Manuel, “Hace 25 años salió el primer virus en Internet”, 3 de noviembre del 2013, en línea, Dirección URL: <http://bit.ly/21Kde2K>, consultado el 7 de noviembre del 2015.

¹¹⁷ *Ibidem*.

¹¹⁸ *Ibidem*.

¹¹⁹ *Ibidem*.

“la universidad Carnegie Mellon creó el primer equipo de respuesta a los incidentes de seguridad en computadoras o CERT (Computer Emergency Responce Team), registrando el nombre del mismo, para atender a los incidentes que resultaran de posibles ataques informáticos o cibernéticos.”¹²⁰

En 1990 ARPANET desapareció, dando paso a los protocolos TCP/IP¹²¹ también es en este año cuando se comienzan a registrar los dominios nacionales de países como “Argentina (.ar), Austria (.at), Bélgica (.be), Brasil (.br), Chile (.cl), Grecia (.gr), India (.in), Irlanda (.ie), Corea del Sur (.kr), España (.es) y Suiza (.ch)¹²²”.

Al siguiente año un hombre llamado Tim Berners Lee crea la World Wide Web (WWW.), y en el utiliza tres nuevos recursos: “HTML (Hypertext Markup Language), HTTP (Hypertext Transfer Protocol) y un programa cliente, llamado Web Browser”¹²³, cuyo fin era navegar por internet.

Para 1993 se crea Mosaic, el primer navegador que permitía acceder a páginas web del dominio www., la primera versión fue utilizada para Unix, posteriormente se fabricó para Windows y Macintosh. Al año siguiente se crea una de las tiendas que hoy en día sigue siendo de las más visitadas a nivel mundial para realizar compras: Amazon, asimismo, nace thewhitehouse.gov, entre otros.

En 1995 Microsoft crea Internet Explorer, quien terminara siendo el buscador preferido por los usuarios, eliminando por completo a los demás para este año “hay en el mundo 16 millones de internautas, el 0,4% de la población¹²⁴”.

Tres años más tarde Estados Unidos crea la Corporación de Internet para la Asignación de Nombres y Números (ICANN por sus siglas en inglés, con el

¹²⁰ Óp. Cit. Sábada Chalezquer Charo, Domingo Prieto Víctor, et al. pág. 91.

¹²¹ El Protocolo de Control de Transmisión y Protocolo de Internet .Según la definición de Richard Clarke, puede definirse como el formato usado para dividir la información, un correo electrónico, por ejemplo en “paquetes” digitales, cada uno de los cuales contienen su propia información de y para necesaria para su recorrido por internet.

¹²² TIME RIME, “ARPANET deja de existir”, 2015, en línea, dirección URL: <http://bit.ly/2dkHUqY>, consultado el 25 de junio del 2016

¹²³ Para Libros, “Internet y la World Wide Web”, 2008, en línea, dirección URL: <http://bit.ly/2dC98XE>, consultado el 25 de junio del 2016.

¹²⁴ BBCL, “Cronología de los sucesos más importantes de Internet”, Marzo 2014, en línea, dirección URL: <http://bit.ly/2do6y8z>, consultado el 25 de junio del 2016

objetivo de confiar la regulación mundial de los nombres de dominio extensiones en .com, .gov, etcétera) a esta corporación¹²⁵. Asimismo, el 4 de septiembre de este año, se crea Google.

El año 2000, marca el inicio de un nuevo siglo, pero también es un parteaguas a nivel internacional en materia de ciberseguridad. En mayo de este año millones de computadoras comenzaron a fallar de manera significativa, la causa de ello es el virus ILOVEYOU. Este virus “afectó a los sistemas informáticos de empresas, bancos, bolsas, compañías aéreas, editoriales, periódicos, oficinas de administraciones gubernamentales tan poderosas como las de Alemania o EEUU¹²⁶”, este virus fue tan potente que logro meterse a las computadoras del Pentágono. ILOVEYOU generó una pérdida total de más de 5500 millones de dólares.

El virus fue creado por un hombre filipino, el Gobierno de Filipinas intentó procesar y enjuiciar a este hombre, en este país era el primer delito informático, no había legislación que lo obligará a cumplir un castigo, en otras palabras, no había delito que perseguir, es por ello que el hombre fue absuelto.

En 2004 surge la Web 2.0, que es definida como:

“aquellas (paginas o aplicaciones) que sacan partido a las ventajas intrínsecas de la web, ofreciendo un servicio continuamente actualizado que mejora cuanto más gente lo use, utilizando y remezclando los datos de múltiples recursos, incluyendo los usuarios individuales, a la vez que ofrecen sus propios datos y servicios de tal forma que pueden ser reutilizados por otros, creando una “arquitectura de participación” en red, yendo más allá de la página de la web 1.0 para ofrecer experiencias de usuario cada vez más ricas.”¹²⁷

Entonces, la Web 2.0 permitirá el compartir información a través de diversas plataformas, en el existe una mayor interacción a diferencia de la Web 1.0 que es

¹²⁵ *Ídem*

¹²⁶ Díaz Viana Luis, “*El regreso de los lobos: la respuesta de las culturas populares a la era de la globalización*”, Consejo Superior de Investigaciones Científicas. Departamento de Antropología de España y América, Madrid, 2003, pág. 97

¹²⁷ Margaix Arnal, Dídac. “*Conceptos de web 2.0 y biblioteca 2.0: origen, definiciones y retos para las bibliotecas actuales*”. En: *El profesional de la información*, 2007, marzo-abril, v. 16, n. 2, pp. 95-106.

la forma más básica de internet, es decir solo permite la búsqueda de información. Es en este año donde nace la principal red social a nivel Mundial: Facebook. Un año después se confirma la existencia de mil millones de usuarios de internet a nivel mundial.

Para el año 2007 con una web “estable” Estonia es el primer país a nivel mundial en celebrar elecciones en línea, “Los votantes estonios pudieron votar desde casa o desde el trabajo y utilizar su ordenador personal o el de la oficina para elegir a su candidato por vía electrónica¹²⁸”.

Cuando Estados Unidos celebró elecciones en 2008, fue la primera vez que los candidatos políticos hicieron uso de todas las posibilidades que la red de redes les ofrecía: YouTube, redes sociales y Twitter.

Barack Obama implementó una estrategia que “supuso un antes y un después en el diseño de campañas electorales y una auténtica revolución comunicativa¹²⁹”, esta estrategia se llamó la triple “O” (Obama’s Online Operation) la cual empleo 3 pilares básicos:

1. Redes sociales, empleando además de su página web, blogs, YouTube, y por supuesto Facebook y Twitter, entre otras, redes sociales dirigidas a las minorías;
2. Mensajería mediante telefonía móvil (SMS); y
3. Bases de datos alimentadas por las redes sociales y los SMS¹³⁰.

Para 2012 Facebook ya supera los mil millones de usuarios, es también en este año que “la ONU adopta, con la adhesión de 89 estados, un tratado sobre la reglamentación de las telecomunicaciones que es rechazado por otros 55 países,

¹²⁸ EL MUNDO ES, “Estonia es el primer país que realiza sus votaciones parlamentarias por Internet”, Marzo 2007, en línea, dirección URL: <http://bit.ly/2dJ0c6O>, consultado el 13 de julio del 2016

¹²⁹ Capitán de Fragata Ponce de León y Marcos Enrique Carlos, “Las redes sociales en el ciberespacio como herramienta de la política”, en Seguridad y Defensa del Ciberespacio, Secretaria de Marina, México, 2015, pág. 213.

¹³⁰ Ídem

entre ellos Estados Unidos, en nombre de la libertad de Internet. Algunos países critican el excesivo peso de Estados Unidos en la red¹³¹”.

En 2013, cuando cerca del 40% de la población mundial, es decir, unos 2.700 millones de personas, tienen acceso a internet. Mandiant, una empresa dedicada a la ciberseguridad en Estados Unidos, acusa a China de ciberespionaje. Gary Summers, entonces vicepresidente de la firma “publicó un informe de 60 páginas que detalla alegaciones durante un período de seis años contra un grupo de hackers - conocido como miembro del equipo Comentario – que pertenecía a una división secreta del ejército chino¹³²”.

Este informe ayudó a las demás firmas estadounidenses a iniciar la ejecución de la ciberseguridad como una prioridad, que ayudara a proteger la información que poseían y que podía ser mal utilizada por otro país.

Asimismo, es en 2013 cuando existe un crecimiento en los métodos de pago alternativos (plataformas para transferencia, PayPal, tarjeta de crédito o débito).

Como hemos detallado en este capítulo, la ciberseguridad no es un tema nuevo, desde la creación de ARPANET hasta hoy en día es una prioridad que debe tomarse en serio, 2014, 2015 y lo que va del 2016 han representado años cruciales para el estudio de este problema. Los ciberataques han aumentado de manera significativa, los Estados se han esforzado por crear nuevos mecanismos que regulen el ciberespacio, desafortunadamente sin éxito. Debe atacarse el problema de manera mundial y no local, estamos en un proceso en el cual se están viendo de manera significativa las debilidades y vulnerabilidades de las infraestructuras críticas, tal y como paso en Irán.

¹³¹ BBCL, Óp. Cit.

¹³² CNN, Joy Oliver, “Mandiant: China is sponsoring cyber-espionage”, Febrero 2013, en línea, dirección URL: <http://cnn.it/2dozxJ7>, consultado el 13 de julio del 2016. Traducción propia

2.2. El rol de los actores no estatales en la ciberseguridad: los usuarios, empresas, los hackers y crackers

Para la ciberseguridad también son importantes los actores que intervienen en este proceso ya que son estos los que se encuentran navegando en el ciberespacio. Todos ellos influyen de manera directa o indirecta a que se cometan ciberdelitos y con ello a desarrollar nuevas estrategias de ciberseguridad destinadas a la protección del usuario en el ciberespacio.

A veces, la contaminación del ciberespacio se produce por diversos motivos: paquetes de información perdidos, malwares, programas pirata, etc..., pero desafortunadamente, la mayor parte de las veces el contagio tiene un origen humano. Desde el individuo que está en el ciberespacio y encuentra una “oferta” en donde ha ganado dinero, pasando por la empresa que ha sido infectada por un virus que un empleado ejecuto al abrir un correo, hasta el gobierno que es atacado en las computadoras de infraestructuras críticas.

Por lo anterior, es importante explicar detalladamente cual es el “rol” de cada uno de estos actores dentro de la ciberseguridad, su nivel de peligro y su nivel de protección.

*El usuario*¹³³.

El ciberespacio, este “nuevo” medio donde el individuo se transforma en el *usuario* y sus actividades dentro de la red se desarrollan. Para estar en él se necesita una identidad digital que confirme quien es él o ella, existen datos personales, que son sustraídos de la realidad y que son necesarios para que se identifique en el ciberespacio como lo es, por ejemplo, el número de pasaporte, datos de alguna identificación oficial, etc... Pero también, existen datos que son de único y exclusivo uso del ciberespacio como el correo electrónico.

¹³³ Por “usuario” entenderemos a aquel que utiliza el ciberespacio y que posee una “identidad” dentro de este, y, por ende, la red posee, parte o gran cantidad de sus datos personales.

Es en este momento cuando surge la pregunta, ¿El usuario, al navegar en el ciberespacio corre un riesgo? La respuesta es sí, todo a través de la identidad digital que adquiere al momento de entrar en la red, pero... ¿Qué es una identidad digital y como se adquiere?

La identidad digital se define según el Ministerio de Defensa Español como “el conjunto de todos los datos digitales disponibles relativos a una persona, independientemente de su validez, el formato que tengan o lo accesibles que sean.”¹³⁴ Es también esta publicación la que identifica tres tipos de datos, o características de un usuario, que están dentro del conjunto de datos digitales.

- *Características inherentes, ligadas a su persona íntimamente, como pueden ser su fecha y lugar de nacimiento, su nombre, nacionalidad, etc.*
- *Características adquiridas, que se acumulan a lo largo del tiempo y van creando una línea histórica. Por ejemplo: domicilio, número de cuenta bancaria, historial médico o impuestos.*
- *Preferencias: música preferida, aficiones, equipo favorito, literatura, etc.*¹³⁵

En el espacio real las actividades que realizamos son visibles y con autorización, lo que genera confianza entre los individuos relacionados con la actividad o transacción que se esté realizando ya que se ve a la persona con la que se está haciendo la actividad. Es así como la seguridad se va a dar dependiendo de la actividad, es decir, a mayor importancia de la actividad o transacción mayor grado de identificación.

Por el contrario, en el ciberespacio, estas actividades o transacciones se darán a través de la identidad digital, esto es, del intercambio de información entre las partes involucradas.

Desafortunadamente, esta identidad puede no ser del todo cierta ya que muchas veces el individuo se preocupa por mantener su privacidad y proporcionar la menor cantidad de datos posibles creando un ambiente de poca confianza entre

¹³⁴ Vid, Ministerio de Defensa Español, “*Monografía 137: Necesidad de una conciencia nacional de ciberseguridad*”, septiembre del 2013, en línea, dirección URL: <http://bit.ly/1Rsflle>, documento pdf, pág. 80-81

¹³⁵ *Ibidem* pág. 81

las partes, ya que, generalmente, una de las partes desea obtener la mayor cantidad de datos posibles con el fin de ofrecer, productos o servicios al usuario.

Como consecuencia en el ciberespacio se crea un ambiente de desconfianza, debido a que al momento de compartir su identidad digital no se sabe si su privacidad será “privada” o puede ser revelada por la empresa, el gobierno o robada por un hacker ante un ataque cibernético.

La desconfianza que se genera es producida por los cibercriminales a los que el individuo se encuentra expuesto, siendo el *phishing* el más común y el que más víctimas ha cobrado alrededor del mundo, siendo Estados Unidos uno de los países que más casos de *phishing* ha presentado.

“Phishing se refiere al envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.

Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.”¹³⁶

A raíz de ello, en marzo del 2005 se promulga en Estados Unidos por iniciativa del senador Patrick Leahy la Ley anti-phishing, la cual enunciaba que aquella persona que creara páginas falsas o enviara spam con el objetivo de estafar a otros recibirían multas o hasta encarcelamiento. Es a partir de esta fecha que las leyes en materia de cibercriminales (en particular el phishing) comienzan a ser más severas con el objetivo de proteger al individuo.

Otros de los cibercriminales más comunes que atacan a los individuos según el FBI son: “estafas, correos no deseados, falsificación de datos, la descarga de

¹³⁶ Vid s/a, Panda Security, “Phishing”, Agosto 2009, en línea, dirección URL: <http://bit.ly/1QuDx5R>, consultado el 12 de noviembre del 2015

programas con virus y páginas engañosas que ofrecen soluciones milagro o grandes cantidades de dinero.”¹³⁷

Las empresas.

Es innegable que el ciberespacio se ha convertido en un “mal necesario” para la sociedad actual. Como se mencionó anteriormente el individuo crea una identidad digital para estar en él y con ello disfrutar las “maravillas del internet”.

La evolución de los medios de comunicación nos ha hecho entrar en un mundo que nos mantiene atrapados, estudios como "Futuro Digital Latinoamérica 2013", explican que un latinoamericano pasa aproximadamente “26.1 horas al mes en internet, mientras que un estadounidense pasa 51.6 horas.”¹³⁸

Esto hace que las empresas se comiencen a interesar en nuevas maneras de atraer la atención de los consumidores, nuevas formas de marketing para ofrecer productos o servicios

Como se ha demostrado en apartados anteriores, los usuarios de internet han buscado la manera de obtener grandes beneficios de la red sin importar las consecuencias. En la actualidad las empresas se han encargado de facilitarnos la compra y venta de bienes y servicios, se puede hacer desde casa con una laptop, Tablet o el celular, aplicaciones conocidas como “apps” hacen todo el trabajo y las hay para todos o casi todos los sectores (bancario, transporte, consumo, ocio, etc...), aquí es donde comienza uno de los mayores riesgos ya que a través de las paginas o las apps los usuarios facilitan sus datos, desconociendo si detrás de ese medio, se encuentra algún hacker, criminales, grupos terroristas, activistas antisistema, empresas y Estados.

¹³⁷ Vid, FBI, “Los delitos cibernéticos más recientes”, septiembre 2015, en línea, dirección URL: <https://www.fbi.gov/espanol/historias/los-delitos-ciberneticos-mas-recientes>, consultado el 12 de noviembre del 2015.

¹³⁸ Vid. Fayer Wayer, “En Latinoamérica pasamos 26,1 horas conectados a Internet en promedio al mes”, mayo 2013, en línea, dirección URL: <http://bit.ly/1QuDx5R>, consultado el 12 de noviembre del 2015.

Lo anterior es conocido mundialmente como *Internet de las cosas*, un concepto cuyo origen se le atribuye al Instituto Tecnológico de Massachusetts (MIT por sus siglas en inglés), este concepto se define como

“es una idea que se basa en que exista una capa de conectividad digital para cosas existentes, donde “cosas” se refiere a todo tipo de objetos cotidianos, e incluso a sus componentes. Se espera que esta idea traiga consigo beneficios en el corto plazo, en aspectos como: optimización de la cadena de abastecimiento, efectividad de costos, mejoras en las experiencias de los consumidores, y beneficios en aspectos de seguridad y servicios de emergencia.”¹³⁹

Actualmente, Internet de las Cosas puede aplicarse a gran cantidad de ámbitos, derivado de la cantidad de usos que el individuo quiera darle a los productos y servicios, también dependerá de la creatividad e ingenio de los desarrolladores

Internet de las Cosas nos permite integrar objetos inteligentes de todo tipo y función, redes de sensores, y recursos de la Internet actual con las personas, y el propósito de ello es aumentar el conocimiento y tomar decisiones que mejoren nuestra calidad de vida en cualquier aspecto posible: social, económico, cultural, ambiental, entre otros.

Y es precisamente, en el aspecto económico que se ha dado el surgimiento de un proceso ahora cotidiano entre la empresa y el consumidor: hablamos del comercio electrónico, esta nueva forma de venta ha adquirido popularidad entre los usuarios del ciberespacio ya que permite hacer una compra desde cualquier parte, pero es también un gran riesgo para los actores involucrados, debido a la gran cantidad de piratas informáticos que hay en la red.

Por comercio electrónico entenderemos, “al proceso de compra, venta o intercambio de bienes, servicios e información a través de las redes de comunicación.”¹⁴⁰

¹³⁹ About.com, “¿Qué es el Internet de las cosas (IoT)?”, enero 2016, en línea, dirección URL: <http://abt.cm/1BNwGgc>, consultado el 20 de diciembre del 2016

¹⁴⁰ Procuraduría Federal del Consumidor (PROFECO), “Comercio electrónico”, enero 2012, en línea, dirección URL: <http://bit.ly/1dziHh7>, consultado el 13 de noviembre del 2015

El comercio electrónico de la mano con las tiendas en línea ha resultado ser un negocio rentable para una empresa debido a que es un componente vital en los negocios, que hace ganar dinero. Es un hecho, las empresas se están adaptando a su entorno, aunque muchas veces no tomen en cuenta a la ciberseguridad dentro de este nuevo entorno.

Si bien el robo de datos de los clientes cuando se realiza una transacción por medio del comercio electrónico en una empresa es una de las preocupaciones de ésta, no es la principal, cosas como la propiedad intelectual, estrategias comerciales, investigaciones de mercado, planes de expansión, patentes, etc... fuerzan a una empresa a reforzar sus estrategias en materia de ciberseguridad.

La empresa siempre buscará innovar, creando nuevos productos o mejorando los ya existentes estas invenciones son el blanco de la competencia, es decir, otras empresas, de hackers, de curiosos e incluso del gobierno, los cuales, intentarán robar esta información y utilizarla como mejor les convenga o que mayor beneficio les traiga.

Es necesario que las empresas comiencen a identificar cuáles son los perfiles de los ciberatacantes que roban o espían la información, esto

“con el objetivo de crear una conciencia la prevención (la cual) es una pieza clave para tener una postura de defensa adecuada y entender las amenazas de manera correcta, así como el establecimiento de mecanismos para detectar brechas de seguridad y establecer respuestas ante un probable incidente.”¹⁴¹

Todo esto ayudará a la empresa a anticiparse ante un ciberataque.

La cultura de la ciberseguridad está aún en desarrollo en las empresas, algunas afirman que sus estrategias de ciberdefensa son buenas y no deben ser cambiadas, otros piensan que los ataques no pueden ser tan fuertes como para dañarlos, hay quienes incluso consideran a los ciberataques como algo irreal, que solo pasa en películas, pero no. Los ciberataques suceden en la vida real y han

¹⁴¹ CEN Expansión, “5 ‘fails’ de las empresas en ciberseguridad”, 18 de noviembre del 2014, en línea, dirección URL: <http://bit.ly/1xNlcsj>, consultado el 13 de noviembre del 2015.

causado grandes controversias a nivel internacional, como lo fue el ciberataque a Sony Pictures Entertainment en el año 2014.

Este ciberataque se llevó a cabo el 24 de noviembre del 2014 en las instalaciones de Sony Pictures Entertainment en California, Estados Unidos. Debido al anonimato de los ciberataques el gobierno estadounidense tiene dos posibles teorías de este atentado:

La primera es que Corea del Norte, como reacción ante el estreno de la película *The Interview*, cuya trama era giraba en torno a una conspiración para asesinar al líder de Norcorea Kim Jong-Un, había realizado el ciberataque.

La segunda igual de probable que la anterior es un ataque de alguien que conocía la estructura de la compañía Sony, "Al parecer, todo se llevó a cabo gracias a la colaboración de la antigua empleada, una experta en cuestiones tecnológicas, que tras prestar durante diez años sus servicios, fue despedida de Sony Pictures en el mes de mayo, debido a un expediente de regulación de empleo."¹⁴² Las consecuencias de este ataque fueron desastrosas para la empresa, robo y filtración de información vital para esta productora y sus empleados, entre ellos, guiones de película e información de empleados que ponía en riesgo la privacidad y estabilidad de estos.

Por otra parte, ninguna de las dos versiones anteriores sobre el quien realizo el ataque han sido esclarecida, pero el gobierno de los Estados Unidos, a través del FBI señala como principal responsable a Corea del Norte, ya que el cifrado de la información se encontraba en Coreano, además, el gobierno de Kim Jong- Un festejaba este ataque denominándolo como "una acción justa", pro en ningún momento mencionaba que ellos habían sido los responsables.

Como respuesta ante este ataque, el gobierno estadounidense se pronunció en contra de este ciberataque llegando a condenar las acciones de los responsables, e incluso lo llamo un ataque severo a la seguridad nacional de este

¹⁴² Gijón Anastasio, "Hallados los Responsables del Ataque a Sony Pictures", 31 de diciembre del 2014, en línea, dirección URL: <http://bit.ly/21Kdyi9>, consultado el 2015

país. El gobierno se comprometía a encontrar a los responsables ante el pánico que surgió entre la gente al considerar a este ciberataque como una advertencia si se exhibía *The Interview* en las salas de cine, lo que podría traer como consecuencia un atentado terrorista.

Posterior a este ataque la productora Sony decidió invertir más en su ciberseguridad. En 2015 se decidió “invertir USD \$15 millones para buscar las fallas en materia de seguridad en Sony Pictures y enmendar en la mejor medida lo sufrido con este hack¹⁴³”.

Sony se encargaría de blindar sus equipos de cómputo y su información para que evitar volver a ser ciberatacados o, por el contrario, si lo eran, el golpe no fuera tan devastador.

“Sony [contrato] a expertos en Madiant, una empresa de seguridad especializada, para sondear el hackeo. Su investigación, según sus voceros, es similar a la que emprenden los forenses en un caso de asesinato: estudian y registran los datos y hechos, revisan la comunicación en las redes de Sony, especialmente a nivel código, y emparejan lo encontrado con distintas hipótesis de motivos. Esto incluye “anuncios” en la “dark web”, donde los hackers suelen acudir para encontrar asesoramientos sobre problemas técnicos.”¹⁴⁴

Mucho se especuló sobre si esta inversión sería solamente para resolver y reforzar los problemas de Sony en materia de ciberseguridad, ya que 9 meses después, Corea del Norte sería víctima de un “ciberapagón” en su red de internet donde las principales páginas web de este país permanecieron inactivas por más de 9 horas. Esta sospecha surge ante la respuesta de Barack Obama después del ciberataque que sufrió SONY ya que prometió “una respuesta proporcionada”.

¹⁴³ Fayer Wayer, “A Sony le costará USD \$15 millones arreglar el ataque a Sony Pictures”, 4 de febrero del 2015, en línea, dirección URL: <http://bit.ly/21Kdy19>, consultado el 17 de noviembre del 2015

¹⁴⁴ S/A, “Todo sobre el ataque norcoreano a Sony”, 19 de diciembre del 2014, en línea, dirección URL: <http://bit.ly/1oSethR>, consultado el 17 de noviembre del 2015.

Hackers y Crackers

Ya hemos hablado de tres actores que se ven involucrados dentro del proceso de ciberseguridad, los dos actores restantes son la amenaza de estos, es decir, el hacker y cracker. Estos “individuos” generalmente se encuentra observando las fallas o vulnerabilidades del sistema que utilizan los 3 actores antes mencionados, el cómo utilicen estas vulnerabilidades marca la principal diferencia entre ellos. Ambos crean programas capaces de destruir la información de una computadora personal, hasta inhabilitar sistemas elementales para cualquier gobierno, pero en sí, ¿Que o quienes son un hacker o cracker?

Richard A. Clarke y Robert K. Knake, definen a un hacker de la siguiente manera:

“Originalmente la palabra designaba al usuario habilidoso de software o hardware que podía adaptar los sistemas para que hicieran cosas distintas de lo que en un principio se los había diseñado para hacer. En el lenguaje cotidiano, sin embargo, el término ha pasado a denotar quien usa sus destrezas para acceder sin autorización a un ordenador o una red. Como verbo “hackear” significa penetrar ilegalmente un sistema.”¹⁴⁵

Esta definición nos aporta tres elementos fundamentales para analizar el comportamiento de un hacker: 1) adapta los sistemas con el objetivo de modificar sus funciones iniciales, 2) penetra un ordenador o una red mediante sus conocimientos, 3) lo hace de manera ilegal.

Si bien, estas características nos adentran al mundo hacker, existen definiciones que defienden el trabajo de estas personas y que incluso vinculan las acciones del hacker como meramente de investigación, como Néstor Marroquín quien en su libro *Tras los pasos de un... Hacker* define a este individuo como:

“Personaje del *underground* que tiene el máximo conocimiento en un tema especializado y una filosofía de vida dedicada a la investigación y comúnmente a compartir estos conocimientos con el fin de que si existiera algún error en la implementación de algún sistema, este se pueda corregir.

¹⁴⁵Op. cit. Clarke A. Richard, Knake K. Robert, pág. 362.

Para algunos organismos de control y de investigación del mundo y la prensa es el primer eslabón de la sociedad “delictiva” en la internet. Estos personajes son expertos en sistemas avanzados. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. [...] normalmente son quienes alertan de un fallo en algún programa comercial y lo comunican al fabricante. También es frecuente que un buen hacker sea finalmente contratado por alguna importante empresa de seguridad.”¹⁴⁶

Es con esta definición que encontramos otras características del hacker. 1) se especializa en un tema de la informática y se dedica a la investigación, 2) si encuentra algún fallo en un sistema lo comparte con el fin de arreglarlo, 3) es considerado un delincuente menor, 4) las fallas que son encontradas en el sistema las comparten con el fin de que se arreglen, 5) algunas veces esta puede ser la puerta de entrada a ser contratados por diversas empresas.

Entonces, de acuerdo a las características mencionadas anteriormente un hacker es aquella persona que mediante sus conocimientos entra de manera no permitida a los ordenadores de diversas dependencias con el fin de encontrar fallas en los sistemas y repararlos, sin ocasionar algún daño o desperfecto.

Después de estas definiciones nos damos cuenta que la percepción que la sociedad tiene una idea errónea sobre lo que es un hacker ya que muchas veces se asocia con el término “pirata informático”, es decir,

“aquellos que con conocimientos de informática persiguen objetivos malignos, como robos de contraseñas de tarjetas de crédito o introducción de virus en masa. No obstante, la verdadera definición de hacker dista mucho de estas características, que en cambio sí corresponden a los conocidos como crackers.”¹⁴⁷

Un cracker se encargará de debilitar al enemigo, de dejarlo sin recursos o información si es necesario, y utilizar esta como mejor le convenga, ya sea dándola a alguien más o destruyéndola completamente. Las características de un cracker no distan mucho de un hacker pero el cómo hacen su trabajo es lo que los diferencia.

¹⁴⁶ Marroquín Néstor, “*Tras los pasos de un... Hacker*”, Editorial Independiente, Quito, 2010, pág., 547

¹⁴⁷ Vid. Como Hacer para, “*Diferencias entre un Hacker y un Cracker*”, 10 de abril del 2014, en línea, dirección URL: <http://bit.ly/1zWjHy4>, consultado el 3 de diciembre del 2015.

El termino cracker surge en 1985 como una combinación de dos palabras “criminal” y “hacker”, esto con el fin de diferenciar los objetivos de unos y otros.

“Los hackers tienen su origen en la cultura post Vietnam de los años 70, basada en la sospecha hacia las autoridades y en el ejercicio de las libertades civiles, incluyendo la creencia de que es ético y moral hackear. Así, los hackers se diferencian de los crackers, quienes no se rigen por principios éticos ni morales.”¹⁴⁸

Esta es una de las principales diferencias de un cracker, pero hay definiciones que aportan más características para conocer a los verdaderos “piratas informáticos”. Orlando López, Catedrático e Investigador de la Universidad del Bosque en Colombia, define a un cracker como:

“Cracker es el término acuñado hacia 1985 para referirse a una persona con excepcionales conocimientos y habilidades para el manejo de computadoras, acompañado por una actitud, que raya en lo patológico, para franquear los métodos de control de acceso y demás mecanismos de seguridad de los sistemas de información automatizados, alterar los mecanismos de protección, los datos mismos o la forma de operación del sistema imponiendo así sus intenciones haciendo caso omiso de toda restricción o norma.”¹⁴⁹

De acuerdo a esta definición observamos que un cracker tendrá una actitud “superior” a la de un hacker, además que impone su voluntad con el fin de satisfacer sus propios intereses.

“[...] los crackers son lo opuesto a los primeros: sujetos con conocimientos (no siempre altos) de redes e informática que persiguen objetivos ilegales, como el robo de contraseñas, destrozarse la seguridad de una red doméstica o esparcir un virus informático a un gran número de computadoras.

Los crackers pueden hacer todo su trabajo buscando tanto recompensas económicas (sustracción de dinero de tarjetas de crédito, estafas online...) como el placer de creerse superiores al resto de la humanidad, o incluso

¹⁴⁸ Rosas González María Cristina, “Ciberespacio, Crimen Organizado y Seguridad Nacional” en Revista del Centro de Estudios Superiores Navales, julio- septiembre del 2011, documento pdf, en línea, dirección URL: <http://bit.ly/1p1UJji>, pág.13.

¹⁴⁹ López C. Orlando, “Hackers & Crackers & phreakers: una perspectiva ética” en Revista Tecnológica Volumen 2 de la Universidad del Bosque, julio-diciembre 2003, documento pdf, en línea, dirección URL: <http://bit.ly/24DNSGg>, pág. 60, consultado el 5 de diciembre del 2015

por morbo; un ejemplo sería infestar con un virus los ordenadores de una universidad determinada.”¹⁵⁰

Por lo anterior observamos que el cracker al igual que el hacker se encuentra interesado por el ciberespacio y todo lo que hay dentro de él. La diferencia se va a dar dependiendo del fin que le den a sus conocimientos el cracker dañara los sistemas y ordenadores, romper y producir el mayor daño posible.

Los cracker son los verdaderos “piratas informáticos” ya que adoptan este tipo de vandalismo como un medio de vida con fines lucrativos, no aportan ningún beneficio o alguna mejora, solo se dedican a alterar la información y realizar ataques a otros sistemas con una finalidad dañina o destructiva.

Como se señaló anteriormente, el hacker buscará la solución ante un problema que él haya encontrado en los sistemas informáticos, contrario al cracker quien sólo busca dañar los sistemas de los usuarios, las empresas o el gobierno. Entonces, se ha llamado equívocamente a los hackers, medios de comunicación los llaman “piraras informáticos” cuando en realidad los verdaderos piratas son los crackers.

Estos cuatro actores intervienen dentro del proceso de ciberseguridad, ya sea de manera directa o indirecta se debe buscar una cooperación usuario-empresa-gobierno-hacker (por lo explicado anteriormente sería casi imposible que un cracker participe en esta cooperación), con el fin de generar normas que beneficien a todos ellos, que ayuden a crear una política de ciberdefensa que sea capaz de proteger a todos los actores y sobretodo garantizar su ciberseguridad.

¹⁵⁰ Óp. Cit. “*Cómo Hacer para*”, en línea, consultado el 5 de diciembre del 2015.

2.3. Barack Obama y las acciones llevadas a cabo en materia de ciberseguridad

El 9 de enero del 2009 Barack Obama llega a la presidencia de Estados Unidos, con varios objetivos por cumplir, uno de ellos era reforzar la protección de este país en materia de ciberseguridad, esto a través de la creación de nuevos centros, nuevas leyes, reforzando su influencia en organizaciones internacionales y abriendo relaciones con otros países en materia de ciberseguridad. El comienzo no fue fácil.

“El colapso de las hipotecas subprime y las complejas operaciones en los mercados de derivados habían creado la peor crisis financiera desde 1929. La crisis económica venía a sumarse al resto de problemas que exigían la atención inmediata del presidente, la guerra de Irak, la guerra de Afganistán, la amenaza de una pandemia de gripe, la reforma de la sanidad pública y el calentamiento global, de modo que Obama no pudo concentrarse en el tema de la ciberseguridad.”¹⁵¹

Poco a poco comenzó a ponerse este tema sobre la mesa, con Robert Knake como consejero, fue quien introdujo a la ciberseguridad como un tema importante dentro de la agenda de Obama “estaba dirigiendo la campaña presidencial más avanzada y dependiente del ciberespacio de la historia.”¹⁵² Afirma el ex consejero de Obama. En 2008 en uno de sus discursos de campaña, el ahora presidente se atrevió a hablar del tema, prometió “convertir a la ciberseguridad en una de las principales prioridades del gobierno federal.”¹⁵³ El presidente logró incluir dentro de la agenda estadounidense el tema, ahora tendría que llevar a cabo acciones para asegurar la ciberseguridad del Estado.

Estas acciones se comenzaron a llevar a cabo rápidamente debido a que el gobierno estadounidense, en particular el departamento de defensa, fue objeto de ciberataques en 2008. Un malware infectó los ordenadores del departamento y esto obligo a los militares a prohibir el uso de los sistemas de almacenamiento thumb drive entre los soldados para evitar la propagación del mismo.

¹⁵¹ Clarke A. Richard, Knake K. Robert Op. Cit. pág. 159

¹⁵² *Ídem.*

¹⁵³ *Ídem*

- *Creación del cibercomando de Estados Unidos (USCYBERCOM)*

El 21 de mayo de 2010 entra en operaciones USCYBERCOM este comando se encontraba bajo el Comando Estratégico de Estados Unidos creado por el Secretario de Defensa Robert Gates. El comandante actual a cargo de la USCC es el general Keith B. Alexander de la Agencia de Seguridad Nacional y a su vez se encarga de otras organizaciones.

Dentro de las principales funciones de USCYBERCOM está el proteger a las estructuras militares (no a las públicas ni a las privadas) de ciberataques “USCYBERCOM planifica, coordina, sincroniza y realiza actividades para dirigir operaciones militares en el ciberespacio y la defensa de determinadas redes informáticas del Departamento de Defensa.”¹⁵⁴

Este cibercomando surge como una medida que hace legítimos a los ciberataques ejecutar ya que valida estos en casos de un conflicto o un ciberataque en contra de Estados Unidos, sus intereses o sus aliados. O en otras palabras, proteger los intereses de Estados Unidos en el ciberespacio.

- *Cooperación con las empresas: Decreto de ciberseguridad de 2013.*

El 12 de febrero del 2013, Barack Obama firmo un decreto de ciberseguridad que, entre otras cosas, permite al gobierno intercambiar con empresas privadas las “ciberamenazas” que ellos consideren un riesgo para el país. Este decreto hace facilita el flujo de información entre el gobierno y las compañías, este decreto incluye a las infraestructuras críticas, es decir, aquellas empresas y/o dependencias fuera del sector de defensa (como energía, comunicaciones, agua, empresas químicas, etc).

En este decreto el presidente Obama señala la importancia de que Estados Unidos enfrente la amenaza que representan los ciberataques. En una declaración apunto: “Sabemos que los hackers roban la identidad de las personas y se infiltran en los correos privados. Sabemos que países extranjeros y empresas roban

¹⁵⁴ Vid. Fayer Wayer, “*Texto cifrado en el logo del USCYBERCOM (Actualizado)*”, 7 de julio del 2010, en línea, dirección URL: <http://bit.ly/1QuEwCZ>, consultado el 25 de julio del 2016.

nuestros secretos corporativos. Ahora nuestros enemigos también están buscando obtener la habilidad de sabotear nuestra red eléctrica, nuestras instituciones financieras y nuestros sistemas de control aéreo. No podemos mirar hacia atrás en el futuro y preguntarnos por qué no hicimos nada ante las amenazas reales a nuestra seguridad y economía¹⁵⁵.

El propósito consistía en permitir una cooperación más fluida entre el sector privado y público, esto incluía a otras empresas que no se dedicaran a la defensa. Asimismo se instauró el Instituto Nacional de Estándares y Tecnología, agencia ligada al Departamento de Comercio, quien sería la encargada de diseñar los procesos para que las empresas puedan prepararse para posibles ciberataques.

- Cybersecurity National Action Plan

Este plan lo define el presidente Barack Obama como “la piedra angular del esfuerzo nacional de seguridad cibernética”. Se describe como la culminación de más de siete años por parte de la administración de Obama, para llevar acciones en un corto plazo y pone en marcha una estrategia a largo plazo, para asegurar una triangulación entre el gobierno, las empresas y los ciudadanos estadounidenses con el fin de tener un mejor control de la seguridad informática. Los objetivos de este plan son:

- ❖ Establecer una Comisión Nacional para la mejora de la Ciberseguridad traerá pensadores estratégicos de alto nivel, de negocio, y técnicos fuera del gobierno para hacer recomendaciones críticas del cómo podemos usar nuevas soluciones técnicas y las mejores prácticas para proteger nuestra intimidad y la seguridad pública,
- ❖ Transformar la manera en que el gobierno se encargue de la ciberseguridad a través de la propuesta de un Fondo de Modernización de Tecnologías de la Información de \$ 3.1 mil millones de USD y la implementación de un nuevo Oficial de Seguridad de Información Federal que ayudará a retirar, sustituir y modernizar el legado de las TIC’s en todo el gobierno.
- ❖ Facultar a los estadounidenses para asegurar sus cuentas en línea mediante el uso de herramientas de seguridad adicionales - como múltiples factores de

¹⁵⁵ Tecnología 21, Paredes Meylin, “Obama firma decreto ley sobre ciberseguridad”, Febrero 2013, en línea, dirección URL: <http://bit.ly/2dR4shc>, consultado el 28 de agosto del 2016.

autenticación y otros pasos de procesamiento de identidad – además trabajar con Google, Facebook, Dropbox, Microsoft, Visa, PayPal, y Venmo para proteger las cuentas en línea y las transacciones financieras.

- ❖ Invertir más de \$ 19 mil millones de USD para la seguridad informática como parte del presupuesto del presidente - un aumento de más del 35 por ciento desde la solicitud del año pasado y con ello asegurar el futuro de la nación.¹⁵⁶

El plan también tiene contemplado hacer uso de campañas que ayuden a elevar la concientización de los usuarios estadounidenses cuando compren algún software oficial o servicio como el blindar sus cuentas y perfiles en línea, e implementar acciones más complejas que el uso del password.

2.4. Hacia una ciberresiliencia

Como se ha expuesto anteriormente, sufrir un ataque cibernético es inminente, las 24 horas del día, los 365 días del año un país, una empresa o un individuo pueden ser objetivo de estos ataques. Estar preparados ya no es suficiente, es por ello que se deben crear mecanismos que reduzcan el impacto de un ciberataque.

Estados Unidos se ha convertido en uno de los principales países que sufren mayor número de ciberataques por día, infraestructuras críticas y empresas se han visto afectadas por ellos, siendo las últimas una de las más afectadas, es por ello que EE.UU. siempre ha estado entre los 3 países que más ciberataques sufre por día, como lo demuestra la siguiente imagen.

Los ciberataques van desde el envío masivo de correos spam hasta algunos más complejos como un ataque de denegación de servicio (DDoS). Un ataque distribuido DDoS es:

“una técnica utilizada por hackers o ciberguerreros en la que un sitio de internet, un servidor o un router recibe una avalancha de solicitudes de datos que supera su

¹⁵⁶ The White house, Daniel Michael, Scott Tony, “*Presidents national cybersecurity plan what you need know*”, Febrero 2016, en línea, dirección URL: <http://bit.ly/20LUYZG>, consultado el 28 de agosto del 2016. Traducción propia.

capacidad para responderlas o procesarlas. El resultado es que el tráfico legítimo o puede acceder al sitio y este termina colapsando.”¹⁵⁷

Estos ciberataques utilizan botnets, es decir, “una red de ordenadores que han sido obligados a funcionar a órdenes de un usuario remoto no autorizado, por lo general sin conocimiento de sus propietarios o usuarios. Esta red de ordenadores “robot” se usa para realizar ataques contra estos sistemas.”¹⁵⁸

Los ataques DDoS fueron constantes durante 2016. Kaspersky Lab se encargó de darlos a conocer a lo largo de ese año, divididos por trimestres, los resultados de estos ataques fueron, durante el primer trimestre de ese año:

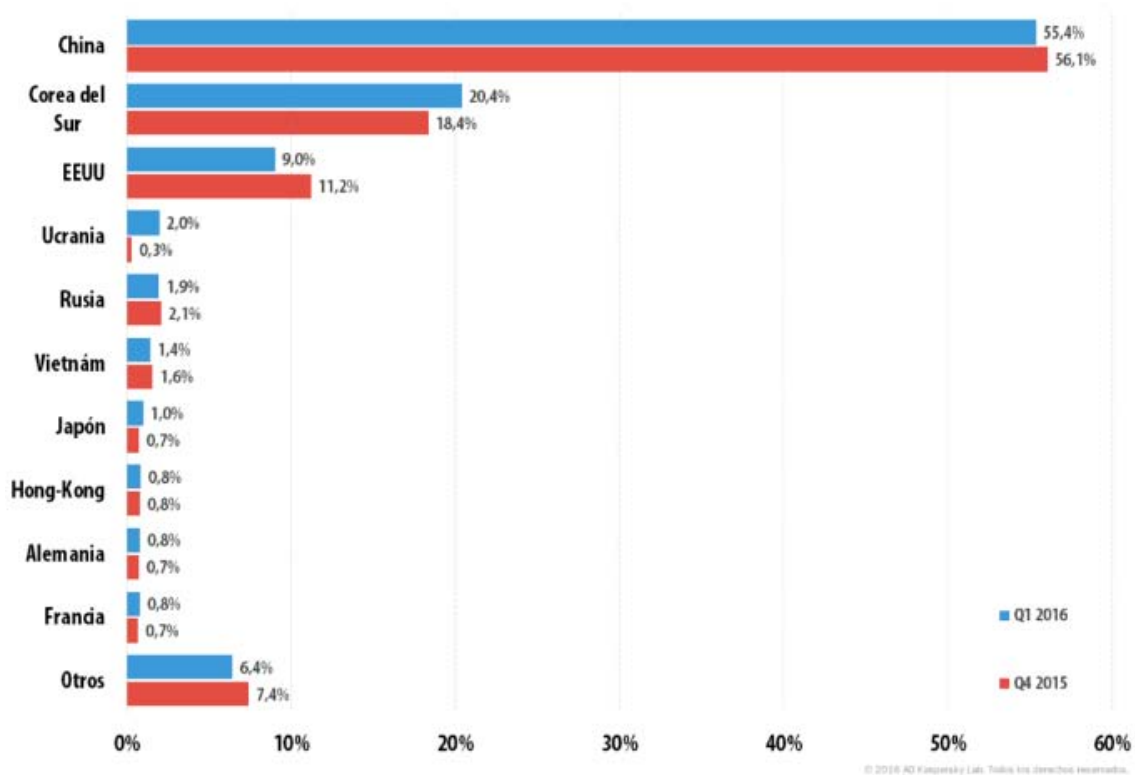
- *Ataque DDoS con “reflejo” de potencia récord:* estos ataques se caracterizan por ser de potencia máxima, llegando a alcanzar los 450-500 Gbit/seg, comparado con los 800-900 Mbit/seg de un ataque “normal”.
- *Ataques DDoS contra Trump:* Durante las fiestas de fin de año, los recursos oficiales de la BBC y el sitio oficial de Donald Trump sufrieron un ataque DDoS cuya potencia, según fuentes no comprobadas, alcanzó los 602 Gbits/sec.
- *Ataques contra las compañías que protegen contra ataques DDoS:* Los delincuentes cibernéticos atacaron a la compañía californiana Staminus Communications, que presta servicios de hosting y protección contra ataques DDoS.
- *Ataques contra compañías de seguridad informática:* compañías de China, USA y Corea del Sur fueron las principales víctimas de ataques DDoS.¹⁵⁹

Esta primera parte del reporte, nos muestra que los ataques responden a tres características principales: 1) el contexto en el que se vive, 2) la potencia y frecuencia con la que se hace un ataque y 3) que los principales objetivos de los ataques DDoS son en contra de las mismas empresas que quieren combatirlos. La grafica 4 identifica a los 10 principales países que reciben este tipo de ciberataques y que corresponden al 93,6% de los mismos.

¹⁵⁷ Clarke A. Richard, Knake K. Robert Óp. Cit. pág. 359

¹⁵⁸ *Ibidem* pág. 360

¹⁵⁹ Kaspersky Lab, “*Los ataques DDoS en el primer trimestre de 2016*”, Abril 2016, en línea, dirección URL: <http://bit.ly/2jO51O2>, consultado 20 de diciembre del 2016.



Grafica 4. Los 10 países con mayores ataques DDoS durante el primer trimestre de 2016 Tomado de Kaspersky Lab, “Los ataques DDoS en el primer trimestre de 2016”, Abril 2016, en línea, dirección URL: <http://bit.ly/2jO51O2>, consultado 20 de diciembre del 2016.

Durante el segundo semestre del 2016, los resultados fueron los siguientes:

- Los ataques DDoS lanzados contra las billeteras de criptomoneda en línea han jugado un papel importante en la vida de estos servicios. Así, en el segundo trimestre de 2016 dos empresas, CoinWallet y Coinkite, anunciaron al mismo tiempo que dejarían de funcionar, por culpa de los prolongados ataques DDoS que sufrieron.
- Se descubrió una nueva botnet, denominada Jaku y que se encuentra principalmente en Japón y Corea del Sur. Los investigadores señalan que los operadores de la botnet están orientados a blancos de gran envergadura: empresas de ingeniería, organizaciones internacionales no gubernamentales e instituciones científicas.
- En el segundo trimestre de 2016 se registraron ataques DDoS contra objetivos situados en 70 países.
- En el segundo trimestre de 2016 el 77,4% de los ataques DDoS afectó a objetivos ubicados en China.

- Tanto por el número de ataques, como por el de objetivos de los ataques DDoS, los países más afectados son China, Corea del Sur y los Estados Unidos.¹⁶⁰

En este segundo trimestre, el informe arrojó nuevos datos, señalando a las instituciones financieras como las más vulnerables a recibir estos ataques distribuidos en diferentes meses del año, como lo muestra la gráfica 5.



Grafica 5. Mes y día del año del 2016 en los cuales se registraron mayor cantidad de ciberataques. *Ibidem*

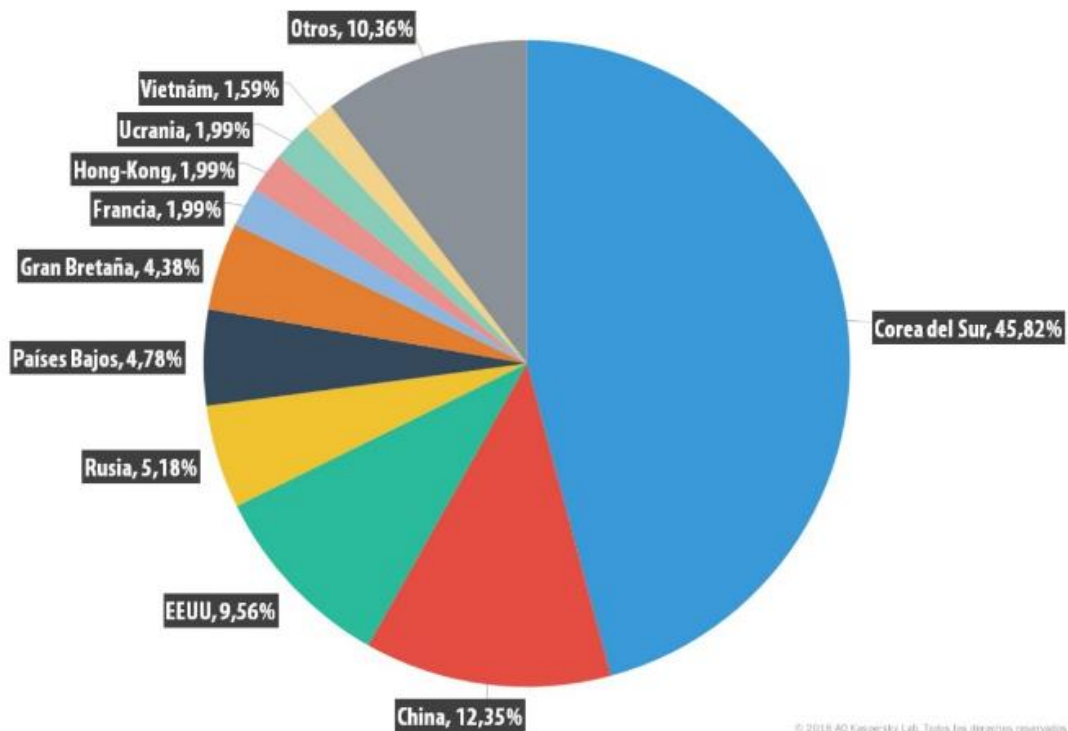
Por último, en el tercer trimestre del año el informe arrojó los siguientes datos.

- Ciberdelincuencia como servicio: Durante los últimos meses se ha visto el alcance masivo de la infraestructura “Ciberdelincuencia como servicio” global, que vende DDoS como uno de sus servicios más populares para lanzar ataques de una magnitud y complejidad tecnológica nunca antes vista
- Ataque contra una compañía de corretaje: Los cibercriminales descubrieron cuales son los blancos más vulnerables a extorsión mediante ataques DDoS. Se trataba de compañías de corretaje, cuyas actividades se caracterizan por el movimiento de grandes capitales y que dependen en alto grado de los servicios web.

¹⁶⁰ *Ibidem*

- Tanto por el número de ataques DDoS, y el número de sus objetivos los primeros puestos les pertenecen a China, los EE.UU. y Corea del Sur. Italia apareció en ambas clasificaciones por primera vez.¹⁶¹

Asimismo, este último reporte nos muestra a los principales administradores de botnets a nivel mundial, siendo Corea del Sur, China y Estados Unidos, los primeros lugares.



Gráfica 6. Principales proveedores de botnets a nivel mundial. Tomado de Kaspersky Lab, “Los ataques DDoS en el tercer trimestre de 2016”, Octubre 2016, en línea, dirección URL: <http://bit.ly/2keig7x>, consultado 20 de diciembre del 2016.

Como hemos visto, a lo largo de 2016 los ataques DDoS fueron constantes, Estados Unidos se mantiene en el tercer lugar con cerca de 500 mil ciberataques por hora, tal y como lo muestra la imagen 3. Un ataque DDoS destinado a un proveedor de internet lograría inhabilitar grandes páginas y servicios que dependieran de este proveedor tal y como sucedió el pasado 20 de octubre del 2016 en Estados Unidos.

¹⁶¹ Kaspersky Lab, “Los ataques DDoS en el tercer trimestre de 2016”, Octubre 2016, en línea, dirección URL: <http://bit.ly/2keig7x>, consultado 20 de diciembre del 2016.

CIBERAMENAZA MAPA EN TIEMPO REAL








ES

MAPA ESTADÍSTICAS FUENTES DE INFORMACIÓN ZUMBIDO WIDGET

Compar

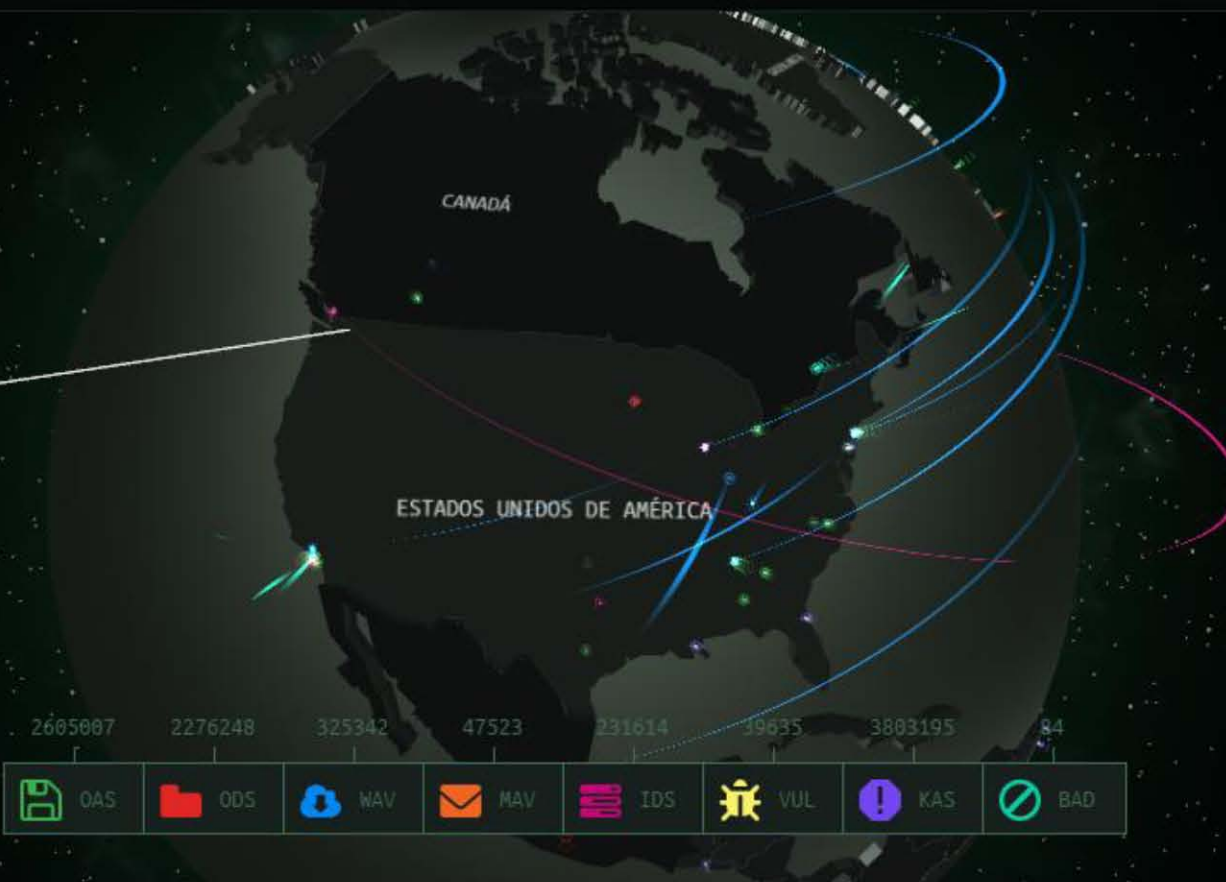
ESTADOS UNIDOS DE AMÉRICA



3 EL PAÍS MAS ATACADO

 OAS	497960
 ODS	239927
 MAV	30562
 MAV	804
 IDS	14211
 VUL	11540
 KAS	262095
 BAD	33

Detección realizada desde las 00:00 GMT

Compartir información



2605007	2276248	325342	47523	231614	39635	3803195	84
 OAS	 ODS	 MAV	 MAV	 IDS	 VUL	 KAS	 BAD

KASPERSKY

© 2016 AO Kaspersky Lab. Todos los derechos reservados. [Términos de servicio](#)

Basado en los datos de Kaspersky Lab.

[DESCARGAR SALVAPANTALLAS](#)

Imagen 3. Ciberataques a Estados Unidos. Fuente: Kaspersky Lab, "Cybermap", [en línea] Dirección URL:

<http://bit.ly/1xz0jBg>, consultado el 23/10/2016

Este ciberataque alcanzó dimensiones globales al afectar a usuarios de varias plataformas, pero su origen y los primeros afectados tuvieron lugar en la Costa Este de Estados Unidos, el objetivo de este ataque fue el proveedor de internet Dyn y se logró interrumpir el servicio de importantes compañías de EE.UU a nivel nacional e internacional, estas fueron:

1. *Twitter*. Debido a fallos de los servidores DNS¹⁶² el servicio de este servicio se suspendió en algunos países cerca de dos horas.
2. *Amazon y Netflix*. A pesar de haber sufrido ataques cuyo daño fue mínimo, el servicio de ambas plataformas se detuvo durante algunos minutos.
3. *PayPal*. Impedía que los usuarios de este servicio realizaran pagos a través de él.
4. Las webs de numerosos medios de comunicación sufrieron la caída de sus páginas por algunas horas, estas páginas fueron: CNN, *The New York Times*, *Boston Globe*, *Financial Times* y *The Guardian*.
5. *Spotify, Reddit, Airbnb y The Verge*. Afectando a millones de usuarios en el mundo, estas plataformas presentaron fallas.
6. *Otras compañías*. EBay, Etsy, Soundcloud, Heroku, Pagerduty, Shopify, Okta, Swapbox, Zendesk, Outbrain y Business Insider también resultaron afectadas.¹⁶³

Este incidente se produce en un contexto de ciberamenazas en Estados Unidos, donde los hackers han irrumpido en organizaciones políticas y agencias electorales. El portavoz de Barack Obama anunció que EEUU investigaría la interrupción de estos servicios.

El grupo *New World Hackers*, quienes se encuentran esparcidos en China y Rusia, se responsabilizó de este ataque. El grupo “explicó que el ciberataque se

¹⁶² El sistema DNS según Richard Clarke se define como “una jerarquía de ordenadores que convierte las palabras (como www.google.com) en direcciones numéricas que las redes puedan usar de verdad para encaminar el tráfico de mensajes (como 192.60.521.7294). Los ordenadores de nivel más alto del DNS pueden contener información de un dominio nacional. *Ibidem* pág. 366-367

¹⁶³ La lista de las empresas dañadas fue obtenida de: El país “*Lista de empresas afectadas por el ciberataque*”, octubre del 2016, en línea, dirección URL: <http://bit.ly/2dLfzJY>, consultado el 23 de octubre del 2016.

hizo a través de las redes de computadoras “zombies” que lanzaron en simultáneo 1,2 terabits de datos por segundo a los servidores gestionados por Dyn, firma que ofrece servicio en EEUU a las compañías afectadas¹⁶⁴”. El objetivo de este ataque, según los responsables pretendía “probar su poder”.

Ejemplos como el anterior, muestran la gran vulnerabilidad que aún, hoy en día, presenta el ciberespacio, ya no basta con identificar a los ciberataques, debido a que la mayoría de ellos suelen aparecer cuando ya han hecho algún daño (mínimo o catastrófico). Es por ello que en los últimos años, empresas y el gobierno de países de la Unión Europea y en menor medida de EE.UU., han trabajado en reducir los daños ante un ciberataque, por medio de la ciberresiliencia.

El concepto resiliencia por sí solo, hace alusión a la capacidad que tiene un sistema para soportar y recuperarse ante un desastre o perturbación, entonces, la ciberresiliencia, “se trata de la administración de riesgos, no de su eliminación. La eliminación no solo es imposible, sino que impide la agilidad; un entorno con un nivel aceptable de riesgo admite innovación¹⁶⁵”.

Por lo tanto, cuando un sistema informático no sea capaz de soportar un ciberataque pero pueda crear mecanismos que disminuyan el impacto para disminuir las consecuencias y seguir funcionando, entonces hablamos de un sistema ciberresiliente.

Una empresa o gobierno que sea capaz de hacer que su infraestructura sea ciberresiliente ante una potencial ciberamenaza, debe poseer un adecuado nivel de seguridad además de fortalecer algunas capacidades como lo son “identificación, detección, prevención, contención, recuperación, cooperación y mejora continua, frente a las distintas ciberamenazas. El conjunto de dichas

¹⁶⁴ La nación, “¿Hackers rusos y chinos, autores del ciberataque?”, octubre del 2016, en línea, dirección URL: <http://bit.ly/2ejZVbA>, consultado el 23 de octubre del 2016.

¹⁶⁵ Symantec, “Ciber- resiliencia”, febrero 2013, en línea, dirección URL: <http://symc.ly/2dzv4Bl>, consultado el 23 de octubre del 2016.

capacidades y su operación cuando son necesarias define realmente la disposición de una organización a construir y mantener la ciberresiliencia¹⁶⁶”.

Desafortunadamente el camino hacia la ciberresiliencia aún es algo lejano, ya que los gobiernos a nivel internacional se ocupan más en prevenir un ciberataque que en trabajar sobre un impacto menor.

Desarrollar un plan ciberresiliente debe ser prioritario al manejar información y controlar grandes infraestructuras del ciberespacio. No tener el correcto conocimiento del impacto de un ciberataque podría resultar catastrófico, las infraestructuras deben de ser programadas para actuar al recibir un ataque cibernético para reducir las consecuencias y que no dejen de funcionar.

En 2010 la falta de conocimiento y preparación para un posible ciberataque le costó al gobierno iraní retrasar su programa de enriquecimiento de uranio, el cual había estado desarrollando desde la guerra fría.

¹⁶⁶ R. Suarez Héctor, D. Peláez Álvarez Juan, *“Ciber- resiliencia: Aproximación a un marco de medición”*, INTECO (Instituto Nacional de Tecnologías de la Comunicación), España, S/A, pág. 19, en línea, dirección URL: <http://bit.ly/2eD8GvD>, consultado el 23 de octubre del 2016.

Capítulo III. El caso de Irán en 2010 como referente de una ciberguerra y sus repercusiones en la seguridad informática.

“La sangre sigue ahí, manchando las conciencias. Pero ese rojo pegajoso ya no se adhiere físicamente a un soldado. Hoy se mata a distancia, y el que aprieta el gatillo está en una base militar, a miles de kilómetros de la zona en conflicto. Como si asesinar fuera cauterizar una herida: algo higiénico, sanitario. La informática deviene en el arma del siglo XXI y así nace la ciberguerra, vendida como algo casi elegante.”¹⁶⁷ Belinchon Gregorio, El país, 2016

Fue a principios de enero del año 2010 cuando los inspectores de la OIEA al realizar una visita rutinaria en la planta de enriquecimiento de uranio de Natanz en Irán descubrieron que las centrifugadoras utilizadas para realizar el proceso de enriquecimiento misteriosamente estaban fallando notablemente. No se sabía cuál era la causa, sorprendentemente los mismos técnicos que trabajaban y daban mantenimiento a la planta también se mostraron asombrados e intrigados sobre la causa de este fallo. Comenzó un proceso de sustitución de maquinaria que, evidentemente, retrasaría dicho programa de enriquecimiento. Meses después se sabría el porqué de este acontecimiento:

“Una empresa de seguridad informática en Bielorrusia fue llamada para reparar una serie de computadoras en Irán que se reiniciaban constantemente. Una vez más, la causa del problema era un misterio hasta que los investigadores encontraron un puñado de archivos maliciosos en uno de los sistemas y así descubrieron la primera arma digital del mundo.”¹⁶⁸

Hablamos de Stuxnet, quien recibía órdenes con el objetivo de dañar las computadoras industriales de Natanz. Fue hasta noviembre de 2010, cuando el presidente iraní, Mahmoud Ahmadinejad, aceptó públicamente que un gusano informático había creado problemas en sus centrifugadoras nucleares.

¹⁶⁷ EL PAIS, Belinchon Gregorio, “*La ciberguerra, la nueva arma de destrucción masiva*”, Febrero 2016, en línea, dirección URL: <http://bit.ly/2dUTU2e>, consultado el 10 de septiembre del 2016.

¹⁶⁸ Amador José, “*Guerra informática: el lado desconocido del acuerdo de Irán sobre su programa nuclear*”, julio 2015, en línea, dirección URL: <http://bit.ly/2etAwKs>, consultado el 10 de septiembre del 2016.

3.1. La importancia geopolítica de Irán dentro del conflicto.

La República Islámica de Irán, posee una ubicación geográfica sumamente importante, siendo parte de Medio Oriente, bordeando el Golfo de Omán, el Golfo Pérsico y el Mar Caspio, entre Irak y Pakistán. Posee una frontera con varios países y lugares estratégicos,

“Al norte: al lado occidental del mar Caspio, Armenia y Azerbaiyán y, al lado oriental: Turkmenistán. Al oeste: Turquía e Irak; al sur: comparte el golfo Pérsico con Kuwait, Arabia Saudí, Bahrein, Qatar, Emiratos Árabes Unidos y con Omán el mar de su nombre. Al este: Pakistán y Afganistán.”¹⁶⁹

Tiene una extensión territorial de 1 650 000 km² y posee una posición privilegiada entre Europa y Asia, y es, después de Arabia Saudita, el país con mayor extensión territorial.

Irán ha sabido utilizar su ubicación geográfica para influir en la política de Medio Oriente mediante una serie de alianzas, que han dado pie a que sea considerado un país con una geopolítica destacada.

Para comprender mejor la situación de Irán ahondaremos un poco en el concepto de geopolítica. Este concepto se le atribuye al Dr. Rudolf Kjellen (1864-1922) quien establecía una similitud entre el ciclo de vida de cualquier organismo y el Estado “(El estado) es una entidad del mismo tipo fundamental que el hombre individualmente: en una palabra es una revelación biológica o un ser viviente. En consecuencia, los Estados están sujetos a la ley del crecimiento¹⁷⁰”. Entonces, de acuerdo a esta lógica “el Estado como organismo vivo: nace, se desarrolla y muere o en algunos casos se transforma”.

Friederich Ratzel, estudia este concepto desde una visión “antropogeografica” en donde la humanidad y el territorio van de la mano, es decir,

¹⁶⁹ Núñez García- Sauco, Antonio, “*Irán como pivote geopolítico*”, Junio 2010, en línea, dirección URL: <http://bit.ly/1dBNrTB>, consultado el 10 de septiembre del 2016.

¹⁷⁰ Kjellen Rudolf, *El Estado como forma de vida*, Citado por Rosales Ariza Gustavo, “*geopolítica geoestrategia, liderazgo y poder*”, 2005, Universidad Militar de Nueva Granada, Colombia, pág. 17, en línea, dirección URL: <http://bit.ly/1hqzvdF>, consultado el 10 de septiembre del 2016.

no se puede estudiar uno sin el otro, llega a concebir al estado como un “organismo territorial”. Ratzel define a la geopolítica como:

“la ciencia que establece que las características y condiciones geográficas y, muy especialmente, los grandes espacios, desempeñan un papel decisivo en la vida de los Estados, y que el individuo y la sociedad humana dependen del suelo en que viven, estando su destino determinado por las leyes de la Geografía. Proporcionando al conductor político el sentido geográfico necesario para gobernar¹⁷¹”.

Por último, Sir, Halford Mackinder (1861-1947) define a la geopolítica de la siguiente manera:

“La Geopolítica estudia los hechos políticos considerando al mundo como una unidad cerrada, en la que tienen repercusión según la importancia de los Estados. En este sentido, los factores geográficos -principalmente, la situación, extensión, población, recursos y comunicaciones de los Estados -, si bien no son determinantes, tienen gran importancia, y deben ser tenidos en cuenta para orientar la política exterior¹⁷²”.

De acuerdo a lo anterior, la posición geográfica de Irán es un factor geopolítico importante por las riquezas naturales con las que cuenta, su extensión territorial y su colindancia con Estados y mares importantes para establecer sus relaciones con otros países.

¹⁷¹ Definición de Friedrich Ratzel, *ibidem*, pág. 28.

¹⁷² Definición de Sir. Halford J. Mackinder, *idem*.



Mapa 1. Ubicación Geográfica de Irán. Fuente: CIA, The World Factbook, "Irán", en línea, dirección URL: <http://bit.ly/19CPKjm>, consultado el 10 de septiembre del 2016.

3.2. Irán como parte de Medio Oriente y las riquezas con las que cuenta.

Infraestructura crítica: El programa nuclear iraní

La República Islámica de Irán cuenta con recursos naturales tales como petróleo, gas natural, carbón, cromita, cobre, mineral de hierro, plomo, manganeso, zinc, sulfuro, uranio, esmeraldas, turquesas y pescado.

Como se señaló anteriormente, este país posee dos salidas al mar: en el norte al Caspio, en el sur al golfo Pérsico y al mar de Omán. Si la primera es importante en relación al transporte del gas, las segundas son fundamentales para el paso del petróleo.

“Irán cuenta con 57.000 toneladas de reservas probadas de minerales; es el cuarto país en reservas petroleras después de Venezuela, Arabia Saudí y Canadá; es el segundo país en reservas de gas después de Rusia. Además, en términos demográficos, cuenta con una fuerza de trabajo muy potente con un total de diez millones de personas con grados universitarios.”¹⁷³”



Mapa 2. Los recursos naturales de Irán. Fuente: SIA, “Petróleo Iraní en tiempos de bloqueo”, en línea, dirección URL: <http://bit.ly/2jkZ6fR>, consultado el 03 de enero del 2017.

¹⁷³ Secretaría de Estado de Comercio de España, “Irán, la importancia de la geopolítica y su vuelta a la comunidad internacional”, Boletín electrónico, Mayo 2015, en línea, dirección URL: <http://bit.ly/2eS8AxD>, consultado el 24 de septiembre del 2016.

Después de haber hablado sobre las características que hace de Irán un lugar geopolítico por los recursos naturales con los que cuenta, nos centraremos en el programa nuclear iraní, no sin antes de hablar de la importancia de este programa y de las instalaciones que lo albergan, que son consideradas infraestructura crítica.

El Homeland Security de los Estados Unidos define a las infraestructuras críticas como: “los activos, sistemas y redes, ya sea físico o virtual, tan vital para los Estados Unidos de que su incapacidad o destrucción tendría un efecto debilitante en la seguridad, la seguridad económica nacional, la salud pública, la seguridad nacional o cualquier combinación de los mismos¹⁷⁴”.

Asimismo, España establece en el su Plan Nacional de Protección de Infraestructuras Críticas que estas son:

“Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas.”¹⁷⁵

Es por ello que hoy en día, en las dentro de las estrategias de seguridad nacional de aquellos Estados que cuentan con infraestructuras críticas, se encuentre la debida protección de estas, ya que se encuentran amenazadas, principalmente por ataques provenientes del ciberespacio, es por ello que la protección se vuelve fundamental, por un lado, evaluar el tipo de daño que causaría un ciberataque a gran escala, por otro, diseñar un plan que ayude a contrarrestar el efecto al ya ser atacada, asimismo, tomar medidas de prevención, protección y resiliencia, ante un ataque físico o un ciberataque.

¹⁷⁴ Departamento del Homeland Security de los Estados Unidos, “*What Is Critical Infrastructure?*”, 2015, en línea, dirección URL: <http://bit.ly/2fbhgQ3>, consultado el 04 de octubre del 2016.

¹⁷⁵ Plan Nacional de Protección de Infraestructuras Críticas, “*Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*”, abril 2011, en línea, dirección URL: <http://bit.ly/2ffQpBg>, consultado el 04 de octubre del 2016.

De acuerdo con estas dos definiciones una infraestructura crítica contara con dos partes fundamentales, la física y la virtual, siendo esta última la más vulnerable para ser atacada. Entonces, se considerará infraestructura a:

“Administración (servicios básicos, instalaciones, redes de información, y principales activos y monumentos del patrimonio nacional); **Instalaciones del Espacio; Industria Química y Nuclear (producción, almacenamiento y transporte de mercancías peligrosas, materiales químicos, biológicos, radiológicos, etc.); Agua (embalses, almacenamiento, tratamiento y redes); Centrales y Redes de energía (producción y distribución);** Tecnologías de la Información y las Comunicaciones (TIC); Salud (sector e infraestructura sanitaria); Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico, etc.); Alimentación (producción, almacenamiento y distribución); y Sistema Financiero y Tributario (entidades bancarias, información, valores e inversiones)¹⁷⁶”.

Es de vital importancia proteger estas infraestructuras, ya que con ello garantizan el correcto funcionamiento de estas, la estabilidad (en cuanto al correcto funcionamiento de ellas) y la credibilidad de la sociedad nacional e internacional respecto al combate de las nuevas amenazas, ante una nueva redefinición de la seguridad tradicional. Un ataque a gran escala pondría en juego todos los factores antes mencionados y debilitaría la imagen del Estado ante las “nuevas” ciberamenazas.

La planta de enriquecimiento de uranio de Natanz ubicada en Irán, es una infraestructura crítica que quedó expuesta ante la opinión pública nacional e internacional, al ser ciberatacada de manera significativa. Esta planta de enriquecimiento de uranio pertenece al Programa Nuclear Iraní (PNI) el cual representa una amenaza para otros países (incluido Estados Unidos) ya que el uso de armamento nuclear en un ataque o en una guerra sería catastrófico, por ello, los gobiernos y organismos internacionales, se han visto en la necesidad de intervenir en el PNI, ya sea por la vía diplomática o por otros medios.

¹⁷⁶ Sánchez Manuel, “*Infraestructuras Críticas y Ciberseguridad*”, julio 2011, en línea, dirección URL: <http://bit.ly/2eISGNB>, consultado el 04 de octubre del 2016.

Antes de hablar del ciberataque que causó gran revuelo internacional, es necesario explicar el origen y evolución del PNI el cual tiene sus orígenes en 1957, “cuando el Sha Reza Pahlavi inició un ambicioso programa que incluía la construcción de 23 centrales nucleares para antes del fin el siglo XX, y así satisfacer las demandas energéticas iraníes de inicios del siglo XXI.”¹⁷⁷

En un principio, Irán recibió apoyo de Estados Unidos, ya que consideraban a este país como un aliado estratégico en la zona de Medio Oriente, además Irán se había adherido recientemente al Tratado de No Proliferación de armas nucleares en 1968. “Con el apoyo alemán comenzaron la construcción de dos reactores nucleares en Busher y con la asistencia francesa una tercera en Darkhouin.”¹⁷⁸ Pero en 1979 Irán pararía estos ya que:

“La Revolución Islámica del Ayatolá Ruhollah Jomeini desencadenó un movimiento en el que se consideró mal vista la investigación en general y la nuclear, en particular, por tratarse de una ciencia occidental. El gobierno del primer ministro Mehdi Bazargan pensó que Irán no necesitaba energía nuclear y se dieron instrucciones para la paralización de los centros de Bushehr que, por entonces, se hallaban en un avanzado estado de construcción.”¹⁷⁹

En 1980, durante la guerra Irán- Irak, los cimientos de las primeras tres instalaciones, quedaron reducidas a cenizas, debido a un bombardeo que destruyó estos reactores.

A mediados de los años 80 Irán impulsó una política de apoyo estudiantil, dirigida a aquellos que se interesaran en el estudio de energía nuclear y técnicas nucleares, enviando a un gran número de estudiantes al extranjero. Es también por estas fechas en la que Irán hace un gran descubrimiento: Uranio en abundantes cantidades.

¹⁷⁷ Ortega García Julián, Instituto Español de Estudios Estratégicos, “Programa Nuclear Iraní: Una Visión Técnica”, septiembre 2012, en línea, dirección URL: <http://bit.ly/2f8ChNC>, consultado el 07 de octubre del 2016, pág. 2

¹⁷⁸ *Ibidem*.

¹⁷⁹ Núñez García- Sauco, Antonio, Óp. Cit. Pág.32.

Al término de la guerra con Irak era necesaria la creación de nuevo armamento que dejara ver a un Irán fuerte ante sus enemigos, es por ello que comenzó a implementar la creación de armamento nuclear, por ello, el presidente Hashemi Rafsanjani retomó el proyecto del PNI y con ello demostrar que Irán se preocupaba por su seguridad. “Intentó reconstruir los reactores de Busher con ayuda española y alemana, aunque por la negativa de éstos lo hizo con ayuda de Rusia, construyendo un reactor nuclear de agua a presión PWR¹⁸⁰”.

A partir de los 90, Irán comienza a establecer alianzas (que hoy en día siguen vigentes) firmaron acuerdos de asistencia técnica por parte de China y de asesoría por parte de Rusia.¹⁸¹ Asimismo, Irán mediante el hojatoleslam Alí Akbar Hashemi Rafsanyani implementó un discurso nacionalista, antiimperialista e islamista, cuyo objetivo era traer de vuelta a los nacionales que se encontraran en el extranjero estudiando temas relativos a la energía nuclear, quien regresara y ayudara a su país recibiría ayuda económica. “Según la investigación llevada a cabo por Jack Boureston y Charles D. Ferguson, cerca de 100.000 expatriados volvieron a Irán.”¹⁸² Es, a partir de este momento, que Irán impulsa realmente su Programa Nuclear. En 1995:

“Teherán solicitó después ayuda al Kremlin, mediante la firma un amplio acuerdo de cooperación, por el cuál, las autoridades de la ya Federación Rusa, reconstruirían las instalaciones bombardeadas por la aviación iraquí en los años 1987 y 1988 de las centrales nucleares de Bushehr I y II y ayudarían a la construcción de una planta para la producción de uranio enriquecido¹⁸³”.

Las tensiones entre Irán y Estados Unidos incrementaron en el año 2002, cuando Alireza Jafarzadeh, líder del grupo opositor Moyahedin-e Jalq en Irán informará al Organismo Internacional de Energía Atómica (OIEA) que en Teherán

¹⁸⁰ Ortega García Julián. Óp. Cit., pág. 4

¹⁸¹ Es importante señalar que Irán recibiría ayuda de Alemania y España para el término de sus centrales nucleares, pero esto no se concretó ya que esta alianza no era bien vista por Estados Unidos, ya que tenía tensiones en su relación con Irán por la toma de rehenes en la embajada de EE.UU en Irán en 1979.

¹⁸² Boureston, Jack and Ferguson, Charles D.: «Schooling Iran’s atom squad», *Bulletin of the Atomic Scientists*, volumen 60, número 3, pp. 31-35, mayo-junio de 2004, citado en Núñez García- Saucó, “Irán como pivote geopolítico”.

¹⁸³ Núñez García- Saucó, Antonio, Óp. Cit., pág.34

se estaba desarrollando armamento nuclear en instalaciones secretas, ubicadas en Natanz y Arak, confirmándose de esta manera que el Programa Nuclear de Irán no era solo un hecho, sino que estaba muy avanzado.

Por lo anterior, en febrero de 2003 al gobierno iraní encabezado por el presidente Muhammad Jatami hace pública la existencia de la planta de enriquecimiento de uranio expresa que Irán producirá su propio combustible nuclear e invita a la OIEA a hacer un recorrido en sus instalaciones. “Parece ser que en el año 2001 se empezó la construcción de su Planta Piloto de Enriquecimiento de Combustible (PFEP), y entre los años 2002 y 2003 se instalaron cerca de 200 ultracentrifugadoras¹⁸⁴”.

Es también en este año, que Irán comienza a recibir presión internacional por medio de la OIEA, la cual le pide de manera imperativa que detenga su programa de enriquecimiento de uranio, ante lo cual Irán acepta y lo suspende, además, de firmar la adhesión al Protocolo Adicional del TNP.

Entre 2005 y 2006 ya con Mahmud Ahmadineyad en el poder, Irán informa que ha retomado el programa de enriquecimiento de uranio en Natanz, asimismo, anuncia una nueva central, dedicada a la conversión de uranio: Isfahán. Por lo anterior, el Consejo de Seguridad de la ONU aprueba de manera unánime la resolución 1737, la cual impone sanciones a Irán.

La resolución 1737 tomada por unanimidad por parte de los países miembros, solicitaba la finalización de las actividades de enriquecimiento de uranio y los proyectos de investigación en reactores de agua pesada.

La resolución también incluía la congelación de los activos financieros de personas y entidades vinculadas al programa nuclear y que se reflejaban en distintos anexos al final del Documento. Naciones Unidas asimismo hacía un llamamiento a la imposición de restricciones al comercio con Irán de productos, tecnología, equipos, etc., que pudiesen ser empleados en estas actividades o en el desarrollo de sistemas de lanzamiento de armas nucleares¹⁸⁵.

¹⁸⁴ *Ídem*, pág. 36

¹⁸⁵ *Ídem*, pág. 40

Irán rechaza esta resolución, por considerarla inválida e ilegal. Y al año siguiente, Ahmadineyad prohíbe la entrada de 38 inspectores de la OIEA a las instalaciones de cualquier planta nuclear, es por ello, que el Consejo de Seguridad aprueba la resolución 1747 que impone nuevas sanciones, Irán lo toma en cuenta y en junio de 2007 le ofrece a este organismo el acceso a sus plantas nucleares, incluso permite la entrada a lugares que no habían sido explorados con anterioridad.

Obama, este establece un acercamiento con Irán con el objetivo de disuadir lo que Estados Unidos consideraba una amenaza latente, Mahmud Ahmadineyad rechaza este acercamiento y, lejos de anunciar una suspensión del PNI, indica que se han instalado “cerca de 6000 centrifugadoras nuevas en Natanz.”¹⁸⁶

En 2010 en un contexto donde “Ahmadineyad anuncia que ha ordenado iniciar el proceso de enriquecimiento uranio al 20%.”¹⁸⁷ países miembros del consejo de seguridad hacen públicas sus sospechas sobre la construcción de una nueva central nuclear.

En este mismo sentido, mandatarios comienzan no solo a defender la postura de Irán sino también hacen negociaciones en torno al uranio producido; Luiz Inácio Lula da Silva, presidente de Brasil, y el primer ministro turco, Recep Tayeb Erdogan, “arrancan un compromiso con Irán para que intercambie su uranio en el exterior y se abra así la puerta a una solución dialogada”¹⁸⁸.

Ante la situación iraní “El Consejo de Seguridad de la ONU se reúne de urgencia para estudiar un proyecto de resolución acordado por sus cinco miembros permanentes (EE UU, Rusia, China, Francia, Reino Unido) más Alemania, que endurece el régimen de sanciones a Irán”¹⁸⁹.

¹⁸⁶ S/A, RTVE, “Cronología de la crisis nuclear iraní”, enero 2016, en línea, dirección URL: <http://bit.ly/2f9reE6>, consultado el 14 de octubre del 2016

¹⁸⁷ *Ibidem*

¹⁸⁸ *Ibidem*

¹⁸⁹ *Ibidem*

En el último trimestre del año, la OIEA presenta un informe el cual asegura que Irán ha producido ya más de tres toneladas de uranio enriquecido, suficientes para tres bombas atómicas. La sociedad internacional no encontraba la forma de hacer que este país suspendiera de forma parcial o definitiva su programa de enriquecimiento de uranio y de pronto algo sucedió. A mediados de noviembre había llegado a oídos del Consejo de Seguridad de la ONU que Irán suspendía temporalmente el enriquecimiento de uranio, era evidente que había un problema, pero no se sabía con exactitud cuál era ese problema.

El 31 de octubre del 2011 Irán (sorpresivamente) anuncia la creación de un cibercomando nacional cuyo objetivo será “vigilar, identificar y contraatacar cuando se produzcan amenazas informáticas contra las infraestructuras nacionales¹⁹⁰”. Era la primera vez que se hablaba sobre el cibertaque sufrido en 2010, Irán reconocía que se había dañado seriamente a una infraestructura de vital importancia para su gobierno, pero que con la creación de este cibercomando no pasaría lo mismo que con Stuxnet.

Para 2014, Irán hace público que Natanz ya no es la única planta de enriquecimiento de Uranio, existe una segunda planta ubicada en Qom, al sur de Teherán. Es en este punto en donde ya se pueden detectar todas las plantas nucleares y a que se dedican cada una.

La perspectiva estadounidense es clara, el PNI representa un peligro para sus intereses, pero ¿Qué representa el PNI para Irán? Primero que nada se debe entender que EE.UU. no se ha permitido conocer, el proceso de toma de decisiones de Irán, asimismo, no sabe cuál es su estrategia hacia ellos.

¹⁹⁰ S/A, RTVE, “Irán crea un cibercomando especializado en la lucha contra los ataques informáticos”, octubre 2011, en línea, dirección URL: <http://bit.ly/2fgxk1T>, consultado el 14 de octubre del 2016.

Para Irán su programa nuclear representa una fuente de poder nacional “se ha convertido en una manera de equilibrar la estructura interna del poder. Esto faculta al papel del Estado en el proceso de desarrollo y progreso.”¹⁹¹

Los críticos iraníes aseguran que el Estado es la causa principal de su estatus de subdesarrollo, que ha frenado la riqueza nacional y el débil poder que representa Irán a nivel internacional. Para Irán el PNI es sinónimo de desarrollo y avance tecnológico, algo que les gusta “presumir”, es parte de su identidad, ya que están aprovechando los recursos con los que cuentan, y que les dará estabilidad nacional y presencia internacional.

“Por esta razón, todos los partidos políticos en Irán exigen la búsqueda de una postura coherente en el proceso de conversaciones nucleares. En este sentido, a pesar de las diferencias de medios y estilos diplomáticos en las negociaciones sobre el programa nuclear y el mantenimiento de la capacidad de enriquecimiento, los reformistas y de política de línea dura hacen que los constantes desacuerdos se disipen. Tal condición aporta cohesión política y popularidad para el Gobierno iraní, posteriormente, refuerza la posición de Irán en las conversaciones nucleares.”¹⁹²

Contantemente no entendemos la política iraní en cuanto a su programa de enriquecimiento de uranio se refiere, pero después de estas características que hemos mencionado, se deja en claro que Irán vela (como cualquier Estado) por sus intereses, que busca el desarrollo y avance tecnológico a raíz de los recursos con los que cuenta. El mapa 3 nos muestra las centrales nucleares con las que Irán cuenta actualmente

¹⁹¹ Center for Strategic Research of Harvard, Barzegar Kayhan, “*Iran's Nuclear Program: An Opportunity for Dialogue*”, Mayo 2009, en línea, dirección URL: <http://bit.ly/2kr5Xsp>, consultado el 18 de enero de 2017.

Traducción propia.

¹⁹² *Ibidem*.



Mapa 3. Centrales Nucleares existentes en Irán. Fuente: BBC, "Las plantas nucleares de Irán", 2014, en línea, dirección URL: <http://bbc.in/2f9D8xC>, consultado el 14 de octubre del 2016

Cada una de estas centrales nucleares tiene diferentes funciones, si bien Natanz y Arak son las más importantes, las demás también juegan un rol importante que se explica a continuación.

Central Nuclear	Función
<p>Qom - Planta de enriquecimiento de uranio Situada al noreste de Qom, cerca de la autopista Qom-Aliabad.</p>	<p>Las construcciones comenzaron a mediados de 2006.</p> <p>No está en funcionamiento, debido a que aún sigue en construcción. Podría llegar a tener una capacidad para 3000 centrifugadoras de enriquecimiento de uranio.</p>
<p>Bushehr - Planta de energía nuclear</p>	<p>La planta nuclear pionera del Programa Nuclear Iraní. Rusia suministró en 2007 uranio enriquecido con el fin de abastecer esta planta. Aquí se encuentran dos reactores de agua a presión, se cree que uno funciona desde 2008.</p>
<p>Isfahán - Planta de conversión de uranio</p>	<p>Su objetivo es procesar mineral de uranio de tres maneras:</p> <ul style="list-style-type: none"> • Gas de hexafluoruro de uranio, que se utiliza en las centrifugadoras de gas. • Óxido de uranio, que se usa para alimentar los reactores, aunque no los del tipo que está construyendo Irán. • Metal, a menudo empleado en las cabezas de las bombas nucleares. el OIEA está preocupado sobre los usos del metal, ya que los reactores que posee Irán no lo necesitan como combustible.
<p>Natanz - Planta de enriquecimiento de uranio</p>	<p>La planta nuclear más polémica y la que sufrió el ciberataque.</p> <p>El Consejo de Seguridad y la OIEA están</p>

	preocupados porque la tecnología utilizada para producir combustible para centrales nucleares también puede usarse para enriquecer uranio en niveles lo suficientemente elevados como para generar una explosión nuclear.
Arak - Planta de agua pesada	El agua pesada se utiliza para moderar la reacción en cadena generada por una fisión nuclear en ciertos tipos de reactores, si bien no en los que Irán está construyendo. Este material también sirve para fabricar el plutonio que se usa en las bombas nucleares.

Tabla 5. Funcionamiento de las centrales nucleares en Irán. Fuente: BBC, "Las plantas nucleares de Irán", 2014, [en línea], Dirección URL: <http://bbc.in/2f9D8xC>, consultado el 14 de octubre del 2016. Elaboración propia con información tomada del artículo.

Existen pocas imágenes de las plantas antes mencionadas, pero a continuación se presentan fotos satelitales de cada una.



Mapa 4. Foto satelital de la planta nuclear de QOM. Fuente: Pulso Internacional, "EE. UU. exige a Irán desmantelar de inmediato instalaciones nucleares de Fordo", 2014, en línea, dirección URL: <http://bit.ly/2fglByW>, consultado el 14 de octubre del 2016.



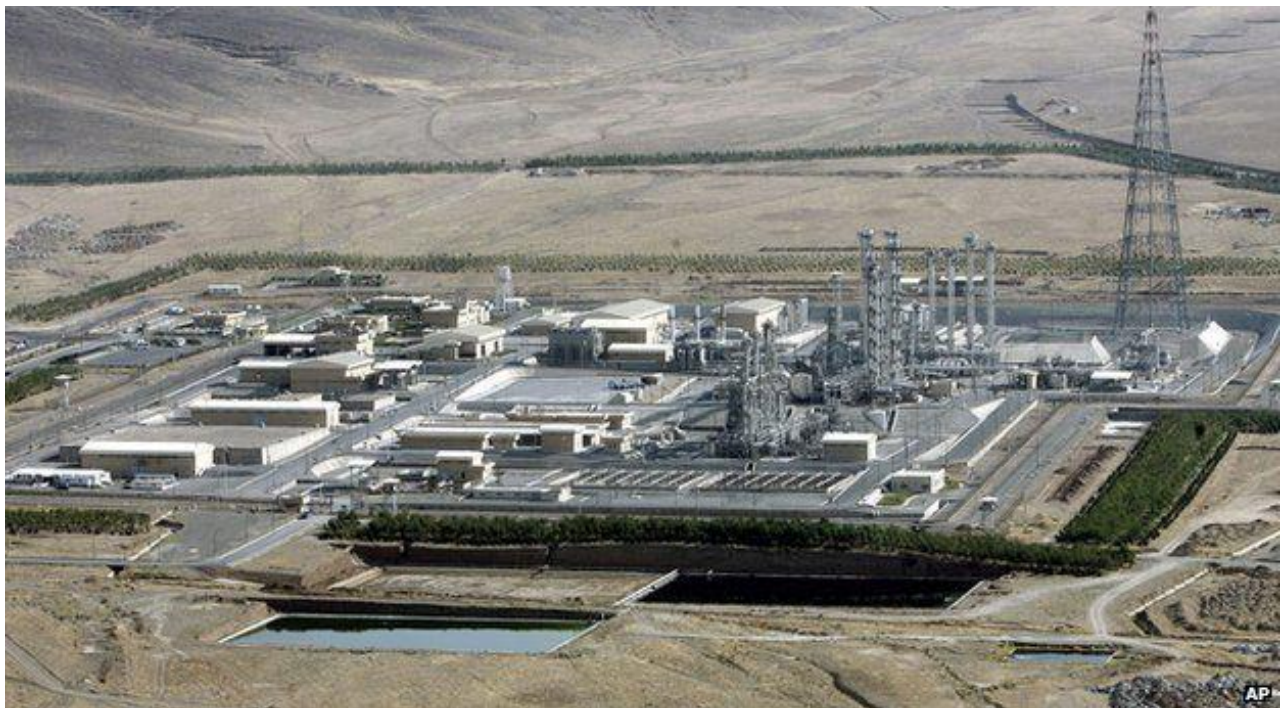
Mapa 5. Foto satelital de la planta nuclear de Busherh. Fuente: Te interesa.es, “*Las principales instalaciones nucleares de Irán*”, 2014, en línea, dirección URL: <http://bit.ly/2fbQHKK>, consultado el 14 de octubre del 2016.



Mapa 6. Foto satelital de la planta nuclear de Isfahán. Fuente: BBC, “*Las plantas nucleares de Irán*”, 2014, en línea, dirección URL: <http://bbc.in/2f9D8xC>, consultado el 14 de octubre del 2016.



Mapa 7. Foto satelital de la planta nuclear de Natanz. Fuente: Benson Pam, CNN Security Clearance, “How far will newest U.N. nuclear report on Iran go?”, Octubre 2011, en línea, dirección URL: <http://cnn.it/2fuqYku>, consultado el 14 de octubre del 2016.



Mapa 8. Foto satelital de la planta nuclear de Arak. Fuente: BBC, “Iran’s key nuclear sites”, Julio 2015, [en línea], Dirección URL: <http://bbc.in/20iPh01>, consultado el 14 de octubre del 2016.

Como hemos observado, estas plantas nucleares de Irán han sido el motivo de diversos intentos fallidos de embargos y sanciones en contra de Irán. Pero esto cambiaría con la llegada de Hasán Rohaní al poder en enero del 2016. Estados Unidos, el Consejo de Seguridad de la ONU y la Unión Europea, levantan las sanciones que habían impuesto contra Irán y este podrá vender libremente gas y petróleo a mercados internacionales. Pero el embargo de armas desaparecerá de forma gradual, en un tiempo estimado de entre cinco y ocho años.

Si bien se ha llegado a un acuerdo nuclear, el PNI no puede suspender operaciones de inmediato, y con el proyecto de la planta de Qom aún en pie, es difícil pensar en que podría haber una suspensión total del Programa Nuclear, es por ello que los gobiernos comienzan a buscar nuevas formas de ataque, que sean más cautelosas y menos visibles. Prueba de ello es la “Operación Juegos Olímpicos”, que utilizó al virus Stuxnet para hacer daño a la planta ubicada en Natanz.

3.3. La Operación Juegos Olímpicos

Como se mencionó en el apartado anterior, durante el gobierno de Ahmadinejad, se reforzó a la planta de enriquecimiento de uranio ubicada en Natanz, entonces, esta era la principal amenaza ante un posible desastre nuclear. Era necesario contener ese crecimiento a como diera lugar, Bush ideó el plan, Obama sería quien lo llevaría a cabo.

Antecedentes. George W. Bush: La mente detrás de Stuxnet

Las relaciones Estados Unidos-Irán, como hemos visto, no han sido del todo amistosas, con el paso del tiempo se han ido deteriorando por diversos factores. Pero el punto más álgido de esta tensa relación se dio cuando el presidente Ahmadinejad anunció que iniciaría el enriquecimiento de uranio al 20%. Inmediatamente este país se colocó como una de las principales prioridades de la agenda de George W. Bush.

Irán en todo momento defendía su proyecto, alegando que el PNI solo tenía fines científicos y de creación de nuevas formas de energía. Argumento que el

Consejo de Seguridad de la ONU y sobretodo Estados Unidos, desmentía. El gobierno de Bush hijo decía que el fin del PNI era militar, es decir, la creación de nuevo armamento nuclear que ponía en peligro el statu quo.

“La administración Bush reiteró en muchas ocasiones que estaba a favor de que el tema se resolviera de forma negociada, pero siempre insistió en que “todas las opciones de respuesta están abiertas”, incluyendo la alternativa bélica.”¹⁹³

Si bien, esta alternativa bélica parecía una opción en el discurso, la realidad era otra. Luis Mesa del Monte señala que una guerra no hubiera sido la opción ya que las fuerzas armadas venían de una reciente guerra en Irak y podría suceder lo mismo “los problemas no resueltos en Afganistán y el alto nivel de preparación combativa de las dos principales estructuras militares iraníes (el ejército y los Cuerpos de Guardianes de la Revolución Islámica), especialmente para el llamado “combate asimétrico”, la extensa geografía del país, el factor demográfico, la ideología de base islámico-chiita, entre otros factores.”¹⁹⁴

En 2005 la comunidad de inteligencia de Estados Unidos había asegurado que el programa nuclear se encontraba suspendido desde 2003, pero increíblemente en 2008 el discurso era totalmente diferente: Irán se encontraba desarrollando armamento nuclear de carácter bélico. “La comunidad de inteligencia de Estados Unidos daba un giro de 180 grados respecto a sus propias aseveraciones expresadas en 2005. Algunos incluso afirmaron que este informe se convertía en un “golpe” demoledor para los argumentos de la administración republicana.”¹⁹⁵

Bush intentaba a toda costa evitar que Irán siguiera adelante con su producción nuclear, necesitaba agotar todos los medios posibles para detener a la “amenaza iraní”, el siguiente paso fue utilizar su influencia dentro del Consejo de Seguridad de la ONU para castigar a Irán.

¹⁹³ Mesa del Monte Luis, *“Las políticas de Bush y Obama hacia la República Islámica de Irán. La centralidad del factor nuclear”*, El Colegio de México, A.C., Foro Internacional, vol. XLIX, núm. 4, octubre-diciembre, 2009, pág. 836

¹⁹⁴ *Ídem*

¹⁹⁵ *Ibidem*, pág. 839.

“En el primer semestre de 2008 la administración de Bush logró incidir en las discusiones dentro del Consejo de Seguridad de la ONU para que en marzo aprobara la Resolución 1803 con una tercera serie de sanciones económicas en contra de Irán por no haber demostrado “que se hayan suspendido de forma completa y sostenida todas las actividades relacionadas con el enriquecimiento y el reprocesamiento y los proyectos relacionados con el agua pesada”, ni haber adoptado otras medidas “que son esenciales para fomentar la confianza”¹⁹⁶.

Nuevamente (como las alternativas anteriores), el plan falló. El presidente Mahmud Ahmadinejad alegaba que esas sanciones eran injustas y que no las acataría y, por el contrario, fortalecería al PNI.

Entonces George W. Bush ejecutaría su último as bajo la manga, un ataque que había sido planeado desde 2006, si bien una guerra tradicional no era la opción, habría que explorar la oportunidad de atacar desde un medio distinto y que no levantara sospechas, era momento de iniciar la ciberguerra.

La idea de atacar a Irán por internet surgió en 2006, como un recurso secreto y de bajo perfil, después de las oleadas de críticas recibidas por la Casa Blanca a causa de la invasión de Irak. Primero, un programa subrepticio (de manera oculta) se infiltró en las redes informáticas de Natanz, para enviar información de su funcionamiento a la Agencia de Seguridad Nacional, especializada en técnicas de espionaje. Con esos datos, EE UU diseñó el virus, con la ayuda de Israel¹⁹⁷.

Barack Obama: El ejecutor

Después de una charla secreta entre George W. Bush y Barack Obama, se acordaría que este último llevaría a cabo el ciberataque a Irán. Y a partir de sus primeros meses en el cargo, Obama ordenó que comenzarán los ciberataques con un virus cuyos daños aún no eran calculados. El objetivo primordial era la planta de enriquecimiento de uranio ubicada en Natanz.

Obama decidió acelerar los ataques (esta serie de ataques recibió el nombre de Operación o programa Juegos Olímpicos) después de que una parte

¹⁹⁶ *Ibidem*, pág. 842

¹⁹⁷ Alandente David, “Obama ordenó un ataque cibernético contra Irán del que perdió el control”, junio del 2012, en línea, dirección URL: <http://bit.ly/2eU16wk>, consultado el 17 de octubre del 2016

del programa accidentalmente se hizo público en el verano de 2010 debido a un error de programación que le permitió escapar de la planta de Natanz de Irán y fue distribuido por el mundo a través de Internet. Expertos en ciberseguridad comenzaron a estudiar a este “gusano”, que, con ayuda de Israel había desarrollado Estados Unidos y lo nombraron Stuxnet.

“Obama decidió que los ataques cibernéticos deberían proceder. En las siguientes semanas, la planta de Natanz fue golpeada por una versión mejorada de la computadora, y después de esto hubo un tercer ataque. Este último de esta serie de ataques, se detectó un par de semanas después de que Stuxnet se detectara en todo el mundo, de manera temporal sacó casi 1.000 de las 5.000 centrifugadoras que Irán había puesto en ejecución en el momento de purificar uranio.”¹⁹⁸

El ataque había sido ejecutado muy fácil, llegó a Natanz (se cree) por un infiltrado, el cual, conectó una memoria USB que llevaba a Stuxnet al sistema operativo Windows de la planta de enriquecimiento de uranio. Medios estadounidenses como New York Times y The New Yorker catalogaron a la "Operación Juegos Olímpicos" como el primer acto ofensivo formal de sabotaje cibernético puro por parte de Estados Unidos contra otro país.

Aun así, a finales de 2016, a punto de que Obama termine su gobierno, no existe justificación alguna por parte del gobierno estadounidense sobre este ataque encubierto en contra de las centrifugadoras. Aunque con lo expuesto anteriormente, es fácil deducir que este ciberataque fue utilizado para retrasar la capacidad de creación de armas nucleares por parte de Irán, al menos unos meses y con ello poder ofrecer un dialogo diplomático que permitiera la suspensión del PNI, entonces, podemos decir que Stuxnet logro su objetivo.

“Irán negó inicialmente que sus instalaciones de enriquecimiento habían sido golpeadas por Stuxnet, y luego dijo que había encontrado este gusano y lo había contenido. Posteriormente, Irán anunció que había iniciado su propio cibercomando militar. El general Gholamreza Jalali, jefe de la Organización de Defensa Pasiva de Irán, dijo que los militares iraníes se prepararon "para luchar contra nuestros

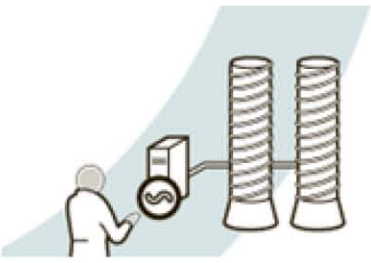
¹⁹⁸ E. Sanger David, NYTimes, *“Obama Order Sped Up Wave of Cyberattacks Against Irán”*, junio del 2012, en línea, dirección URL: <http://nyti.ms/1EhRr87>, consultado el 17 de octubre del 2016. Traducción propia

enemigos" en el "ciberespacio y la ciberguerra." Pero no ha habido poca evidencia de que se ha comenzado a contraatacar¹⁹⁹.

El ataque de Stuxnet fue, en su momento, un golpe duro para Irán que evidenciaba la poca capacidad de ciberseguridad que poseía la planta de Natanz, y se mostraba como un programa débil en cuanto a estructura cibernética. La siguiente imagen, muestra el proceso de entrada y ataque a la planta de Natanz.

¹⁹⁹ *Ídem.*

Continúa...



5. A través de varios métodos, el nuevo programa se introduce en los controladores de la computadora de la planta, y se extienden a miles de centrifugadoras.

1. Los programadores de la Agencia Nacional de Seguridad y en el ejército israelí diseñaron un programa de "guía" que pudiera recrear el funcionamiento de la planta.

Programa "guía"

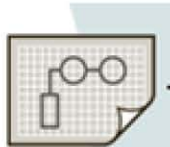


¿Cómo funciona un programa secreto de ciberguerra?

Los programadores de la Agencia de Seguridad Nacional de EE.UU. y las Fuerzas Armadas israelíes crearon una serie de virus para atacar los ordenadores que controlan el centro de enriquecimiento nuclear de Irán en Natanz. Los ataques se repitieron durante varios años, y cada vez que los programas variaban eran más difíciles de detectar. Una de las variantes escapó de Natanz y se hizo público.

4. Usando esos datos, los programadores diseñan un complejo programa "gusano" para interrumpir en la planta.

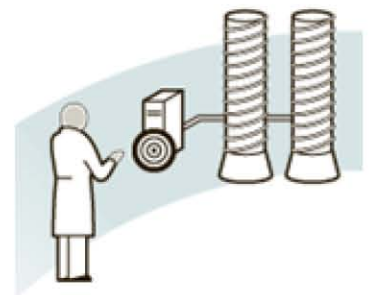
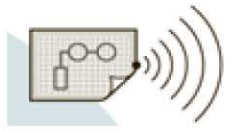
2. El programa se introduce en una computadora del controlador de la planta, posiblemente de manera involuntaria por un trabajador de la planta.

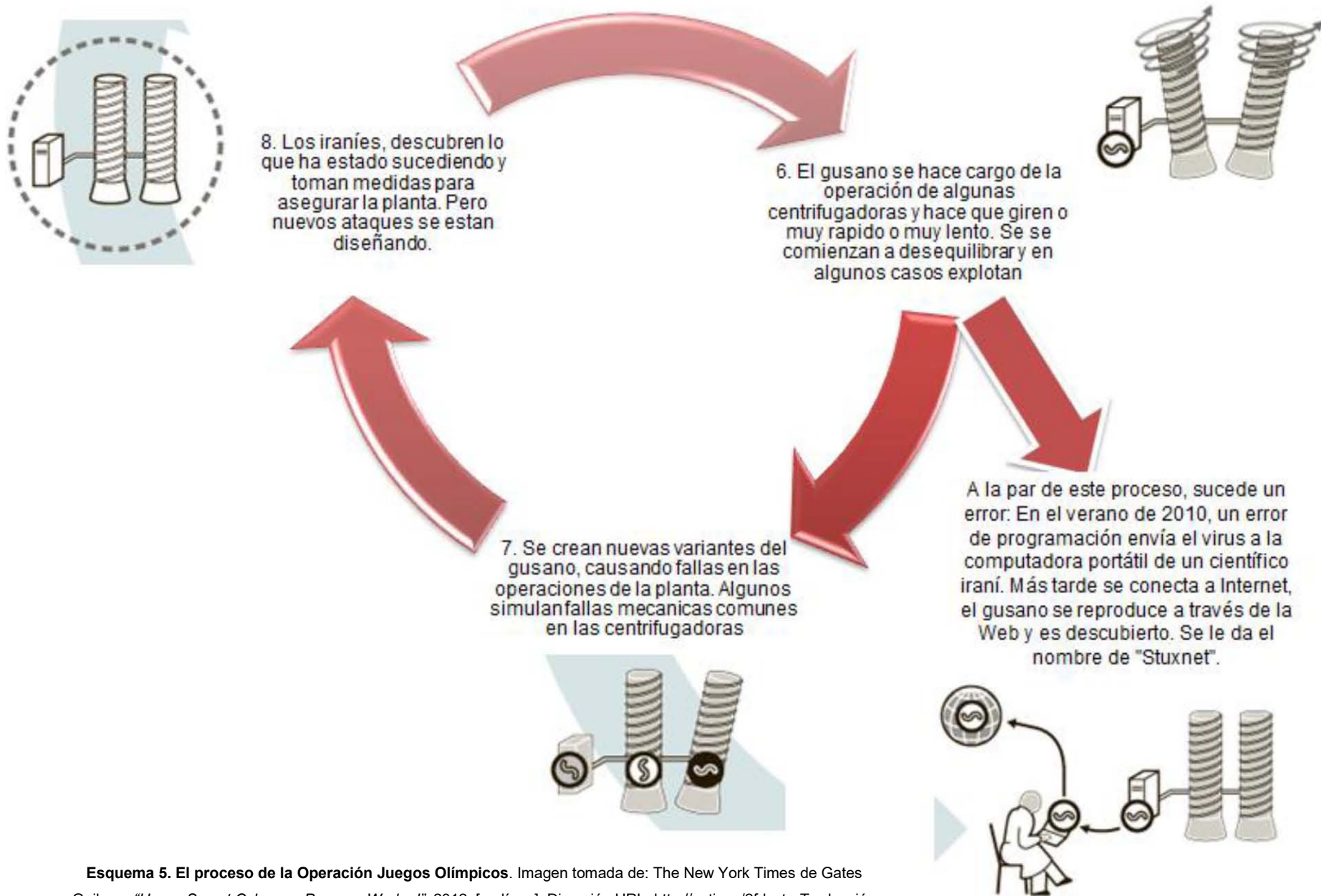


Programa "gusano" (stuxnet)



3. El programa recoge información sobre cómo se configuran las computadoras de la planta y transmite los datos a las agencias de inteligencia.





Esquema 5. El proceso de la Operación Juegos Olímpicos. Imagen tomada de: The New York Times de Gates Guilver , "How a Secret Cyberwar Program Worked", 2012, [en línea], Dirección URL: <http://nyti.ms/2fdxatr>. Traducción propia.

Stuxnet es una realidad, pero su origen sigue siendo un mito, tanto Estados Unidos como Israel no aceptan haber sido la mente y la mano de la Operación Juegos Olímpicos, “El gobierno de los Estados Unidos sólo ha reconocido recientemente el desarrollo de armas cibernéticas, pero nunca ha admitido su uso²⁰⁰”, han existido ataques a ordenadores de otros países pero todo ha quedado en ciberespionaje, Juegos Olímpicos demuestra la complejidad, alcance e impacto de un ataque a gran escala en una infraestructura crítica.

Como lo demuestra el esquema 5, Stuxnet logro desestabilizar el PNI, pero al ser descubierto comenzó a erradicarse y eliminarse. Pero nuevas variantes de este virus surgirían, con capacidades más potentes, nuevas funciones y casi imposibles de descubrir.

3.4. Las “nuevas armas” utilizadas en el conflicto: Stuxnet, Flame y Duqu y sus consecuencias al ser utilizadas en los ordenadores de infraestructuras críticas.

Stuxnet hubiera sido un éxito para Estados Unidos si por un error este no se hubiera propagado en internet, probablemente su impacto habría provocado el colapso de las centrifugadoras que se encontraban en Natanz. Nuevas variantes han sido creadas con el objetivo de dañar aún más cualquier infraestructura crítica, estas nuevas ciberarmas son además de casi indetectables, bastante económicas y su nivel de destrucción puede llegar a compararse con el impacto de una bomba dentro de las instalaciones. Por todo esto, no resulta sorprendente que se estén creando nuevas variantes de Stuxnet, pero ¿Cómo funcionan estas ciberarmas?

Stuxnet

Varios analistas en seguridad informática y empresas estudiaron a Stuxnet, una de ellas es la empresa Symantec, creadora del primer antivirus Norton (en 1999) estudio y definió a Stuxnet como “un gusano informático que apunta a los sistemas industriales de control que se utilizan para controlar instalaciones

²⁰⁰ E. Sanger David, NYTimes, Op. Cit. Traducing propia.

industriales como plantas de energía eléctrica, represas, sistemas de procesamiento de desechos entre otras operaciones industriales.”²⁰¹

Stuxnet modifica los códigos para permitir que atacantes “anónimos” tomen el control de cualquier infraestructura, esto lo hace copiando el código de funcionamiento del sistema, después lo modifica y lo reproduce en bucle para que no se note anomalía alguna. Permite a un hacker manipular desde cualquier parte del mundo manipular equipo físico.

“El gusano esta hecho de un complejo código que requiere de muchas y diferentes habilidades para juntarlos. Los expertos de Symantec estiman que tomó entre cinco y diez personas durante seis meses para armar este proyecto además de que los involucrados deben tener conocimiento de los sistemas de control industrial y acceso a dichos sistemas para realizar pruebas de calidad; una vez más indicando que esto fue un proyecto con mucha organización y fondos disponibles²⁰²”.

Stuxnet a final de cuentas sigue siendo un malware que aprovechó las vulnerabilidades de un sistema informático en una infraestructura crítica, estas fallas son aprovechadas para entrar al sistema, un antivirus común no lo puede detectar debido a que el Stuxnet era un virus con programación más compleja.

Después de que Stuxnet saliera de Natanz, este fue detectado por una empresa Bielorrusa encargada de la ciberseguridad de ese país, debido a su complejidad se aseguró que podría haber estado en la red desde un año antes. Al principio se pensó que solo era un virus común, dedicado a robar información y hasta cierto punto “inofensivo”.

Actúa en una infraestructura crítica de dos formas, “En primer lugar, hace que las centrifugadoras giraran peligrosamente rápido, durante unos 15 minutos, antes de volver a la velocidad normal. Luego, aproximadamente un mes después,

²⁰¹ Symantec, “*El gusano Stuxnet*”, 2010, en línea, dirección URL: <http://symc.ly/2fcaOLg>, consultado el 18 de octubre del 2016.

²⁰² *Ídem*

desaceleró las centrifugadoras durante unos 50 minutos.”²⁰³ Esto se repitió varias veces antes de ser detectado y con el tiempo, el cambio excesivo de velocidades en las maquinas infectadas causó que unas 1000 (alrededor del 20% de las centrifugadoras de Natanz), se desintegraran y dejaran de funcionar.

Duqu

Un año después de Stuxnet, salió a la luz un nuevo virus: Duqu el cual tiene por objetivo los sistemas de las PC, entrando a través del correo electrónico, propagándose a los contactos y cuando se abre el documento de Word adjunto, el código malicioso toma el control del sistema, una vez dentro obtiene los datos privados y con esto se lleva a cabo más fácilmente el ataque. Al lograr reunir los datos necesarios, los comparte con los propietarios. La información en la que se centran los ciberatacantes son: documentos secretos, archivos y otros datos que puedan ayudarles a iniciar futuros ataques y afectar a los productos, tecnologías y servicios de las empresas. Aún en la actualidad, es muy complicado darse cuenta de esta infiltración, y algunas herramientas de seguridad muy sofisticadas pueden ayudar a detectarlo.

El primer punto de propagación fue la región de Medio Oriente, le siguió Asia (en particular Hong Kong) y por último, África. Una peculiaridad de este virus es su permanencia en la memoria del sistema sin la necesidad de insertar sus archivos en el disco.

Nuevamente, Duqu al igual que su antecesor Stuxnet, aprovecho las vulnerabilidades que presentaba el sistema operativo Windows y se infiltró en los ordenadores “Los autores de Duqu escogen a sus víctimas a través del correo. Si se abre un documento de Word, éste infecta el ordenador y el atacante obtiene el control de la máquina. A través de ella puede contagiar el sistema informático de la corporación atacada y robar datos.”²⁰⁴ Este virus solo está pensado para robar

²⁰³ BBC, “*El virus que tomó control de mil máquinas y les ordenó autodestruirse*”, julio 2015, en línea, dirección URL: <http://bbc.in/1GDvzCY>, consultado el 18 de octubre del 2016.

²⁰⁴ El país, “*El virus Duqu aprovecha un agujero de Windows para infiltrarse*”, noviembre 2011, en línea Dirección URL:<http://bit.ly/2fcJuw4>, consultado el 18 de octubre del 2016.

información, de ahí que su periodo de vida sea corto, ya que después de 36 días de estar en la red de ordenadores, se autodestruye.

A principios del año 2015 Kaspersky detectó una irregularidad en un contexto de negociaciones internacionales con Irán, un virus afectaba a sus sistemas internos, inmediatamente, al detectar al intruso el laboratorio se puso a ver qué era lo que estaba pasando. El resultado: un virus el cual es difícil de detectar, ya que no modifica ni crea datos: solo los sustrae, inmediatamente Kaspersky lo bautiza como Duqu 2.0.

Este virus ya no solo ataca a las infraestructuras críticas de los Estados, también se encontraron rastros de él en empresas privadas dedicadas a la seguridad informática. Países de Asia, Medio Oriente y Occidente eran los principales atacados por Duqu 2.0, particularmente, algunas de las nuevas infecciones estaban vinculadas al P5+1 (Estados Unidos, Rusia, China, Francia, Reino Unido y Alemania) y las negociaciones que se estaban llevando a cabo en materia del Acuerdo Nuclear Iraní. Los ataques se centraban en los lugares donde habían reuniones para tratar el tema de este acuerdo.

Flame

Después de Stuxnet y Duqu, surgió el virus informativo más poderoso de los tres, nos referimos a Flame. Nuevamente, Kaspersky fue quien alertó de la existencia de este virus, lo definió como “un sofisticado programa malicioso que está siendo activamente utilizado como un arma cibernética cuyo objetivo son infraestructuras de varios países.”²⁰⁵

Este virus fue encontrado por expertos de esta firma rusa durante una investigación que fue promovida por la UIT de la ONU, en su informe conjunto establecieron las características de este virus, el cual robaba información valiosa a través de diversas tácticas, como el robar información confidencial de la computadora en donde está alojado el virus, tomaba capturas de pantalla, e

²⁰⁵ Kaspersky Lab, “*What is Flame Malware?*”, 2012, en línea, dirección URL: <http://bit.ly/2fj1iIG>, consultado el 18 de octubre del 2016.

incluso grababa conversaciones si la computadora tenía un micrófono. Asimismo, Flame es capaz de capturar la información de las bandejas de entrada, incluidas las contraseñas ocultas por asteriscos y recopilar información acerca de los dispositivos Bluetooth cercanos que se puedan descubrir. “El virus carga toda esta información a los servidores de comando y control, de los cuales hay alrededor de una docena repartidos por todo el mundo.”²⁰⁶

Flame fue utilizado, al igual que Stuxnet, contra Irán, este virus había sido 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.”²⁰⁷

Según Kaspersky, Flame es un programa altamente sofisticado y dañino que ha sido realizado. Incluso ha llegado a recrear información de alta confidencialidad evidenciando que es un virus fabricado por mentes altamente capaces, y no por un hacker que se encuentra en su casa.

“El virus fue ideado para exportar la información mientras se hace pasar por una rutina de actualización de software de Microsoft y es capaz de evitar ser detectado durante varios años mediante el uso de un sofisticado programa para romper un algoritmo encriptado.”²⁰⁸

Recientemente, se ha descubierto que Flame es una extensión de la Operación Juegos Olímpicos, y fue desarrollado a la par de Stuxnet pero se esperó al momento indicado para utilizarlo.

Como hemos visto, estos tres virus son altamente sofisticados requirieron importantes fondos económicos para ser desarrollados y no existen en la actualidad muchos grupos que puedan desarrollar una amenaza de este tipo. Además estos virus (a excepción de Duqu 2.0) tienen como objetivo, las infraestructuras críticas, especialmente las de Irán.

²⁰⁶ Revista soluciones, “*Qué es y Cómo Funciona el Virus Flame*”, mayo 2012, en línea, dirección URL: <http://bit.ly/2f2h8C2>, consultado el 18 de octubre del 2016.

²⁰⁷ El mundo.es, “*EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán*”, junio 2012, en línea, dirección URL: <http://bit.ly/2epmARh>, consultado el 18 de octubre del 2016.

²⁰⁸ *Ídem*.

Conclusiones

Desde su creación en 1969 bajo el nombre de ARPANET, Internet, pero sobretodo el ciberespacio lograría lo imposible: crear una nueva dimensión en donde no solo las personas interactuamos, sino también crearían un nuevo campo de batalla difícil de gobernar.

El tema de los cibercrimenes suele ser un tanto confuso. Es por ello que la tipificación que se elabora en este trabajo tiene también como finalidad esclarecer un poco como es que se constituyen los diversos crímenes cibernéticos.

En el ámbito político el juego es diferente, el objetivo no es robar grandes cantidades de dinero, sino debilitar al enemigo por medio de sus vulnerabilidades en sus infraestructuras críticas, que por ejemplo, hacen funcionar correctamente un aeropuerto, que contienen la información del Estado o que proveen salud a la población, son ahora el punto central de ataque.

Crear un virus informático, requiere grandes cantidades de dinero y mentes lo bastante capaces para calcular los daños que causaría un ciberataque con este virus a gran escala. Pero a pesar que requiere grandes cantidades de dinero, el costo es bajo si se compara con una guerra tradicional, además a largo plazo representaría menos pérdidas humanas y un mayor daño, ya que el enemigo no es visible a simple vista.

Como vimos, Estados Unidos pensó en su ciberseguridad casi inmediatamente después de crear ARPANET, por lo tanto, no es un tema reciente. Si bien hubo temas más importantes después de los ataques del 11 de septiembre, el tema de ciberseguridad siempre estuvo presente.

Así lo demuestra el Quadrennial Defense Review de 2001 que por primera vez incluye el tema concerniente al ciberespacio, en el que Estados Unidos asumía que se debían atender de manera rápida, los nuevos escenarios de competencia militar, ya que consideraba que los avances tecnológicos eran potencialmente peligrosos y en donde se desarrollarían nuevos conflictos.

Aseguraba que la explotación de este espacio, crearía en un futuro un caos que la milicia estadounidense tenía que atender. Ello debido a que existiría una tendencia a querer controlar al ciberespacio, pero incluso reconocían que ello era imposible y planteaban la idea de negar el uso del ciberespacio para que se desarrollara un conflicto.

También reconocía que los Estados se encontrarían deseosos de desarrollar operaciones de carácter ofensivo y defensivo dentro del ciberespacio, enfatizaba en la obligación que tenía Estados Unidos de dedicar recursos que se encargaran de proteger infraestructuras de información crítica de manera física o en el ciberespacio.

A través de un manejo de riesgos el QDR recalca la necesidad de que Estados Unidos se enfrentara a un mundo en el que el cambio era constante, y que debía prepararse para los viejos y nuevos desafíos. Algunos eran “familiares”, y alertaban de la posibilidad de una gran guerra. Otros riesgos eran ataques terroristas con un número significativo de víctimas y las ciberguerras.

Como si este QDR hubiera sido un profeta, pasaría por una gran guerra (con Irak), un ataque terrorista a gran escala (11-s) y una ciberguerra (la que tendría con Irán en 2010).

En el 2006, EE.UU. lanza un nuevo QDR, en él enfatiza más en el tema de la ciberseguridad, reconoce que los terroristas deben ser localizados y rastreados en todos los dominios, incluido el ciberespacio. Asimismo, reconocía el derecho de responder violentamente ante cualquier ataque al territorio, de EE.UU., personas e infraestructura crítica a través de cualquier medio (incluyendo al ciberespacio).

Este QDR mencionaba la preocupación que China representaba para EE.UU., en donde aseguraba que este país hacía grandes inversiones militares en el área informática, y que era un potencial incitador de la ciberguerra.

Por último, hacía un llamado a la respuesta y gestión de riesgos ante desastres naturales (como el huracán Katrina), un posible ataque con Armas de

Destrucción Masiva y la defensa en y de todos los espacios (aire, tierra, mar, espacio exterior y añadía el ciberespacio), esto se lograría a través de la coordinación de misiones cibernéticas defensivas y ofensivas en el Departamento de Defensa.

El año 2010 será recordado como el “ciber año” en Estados Unidos, ya que como se menciona en la hipótesis que sustenta esta investigación, la ciberseguridad toma mayor relevancia en la agenda estadounidense. En este QDR se le dedica por primera vez un apartado específicamente al área de ciberseguridad, y las acciones que debían ser llevadas a cabo.

Enfatizaba en que las fuerzas armadas debían (ya no era una opción) dominar el ciberespacio ya que en este se llevan a cabo operaciones efectivas de alto ritmo. Hacia un llamado a que el Departamento de Defensa tenía que defender activamente las redes en donde se llevaban a cabo estas operaciones.

Asimismo, enunciaba las acciones del Departamento de Defensa que iban encaminadas a fortalecer las capacidades de las fuerzas armadas en el ciberespacio, estos logros eran:

- Desarrollar un enfoque más integral de las operaciones del Departamento de Defensa en el ciberespacio;
- Desarrollar una mayor experiencia y sensibilización cibernética,
- Centralizar el mando de operaciones cibernéticas; y
- Mejorar las asociaciones con otros organismos y gobiernos.²⁰⁹

Lo destacable de este QDR es que realiza el anuncio oficial de la creación del USCYBERCOM, un comando Estratégico, para liderar, integrar y coordinar mejor la defensa, y el funcionamiento de las redes del Departamento de defensa. También este documento invita por primera vez a la cooperación internacional en materia de ciberseguridad, mediante el intercambio de información, el apoyo a la aplicación de la ley, lo anterior en defensa de la patria estadounidense.

²⁰⁹ Departamento de Defensa de Estados Unidos, “*Quadrennial Defense Review 2010*”, enero del 2010, en línea, dirección URL: <http://bit.ly/2fU1pFL>, consultado el 14 de noviembre del 2016.

Un nuevo QDR es lanzado en 2014, en él se enfatiza en las inversiones que se están haciendo en materia de ciberseguridad y se mencionan los logros que se han obtenido, también se menciona sobre el apoyo a los Comandantes Combatientes que planean y ejecutan misiones militares para hacer frente a ciberataques contra Estados Unidos.

Además, señala la continuidad y el buen trabajo que se ha llevado a cabo con otros departamentos y agencias de los Estados Unidos, así como con aliados y socios internacionales, ello con el objetivo de crear capacidades de defensa cibernética y poder eliminar los riesgos que hay en el ciberespacio.

Las lecciones que deja el análisis de estos documentos, es la creciente relevancia que comenzó a tener el ciberespacio y la ciberseguridad en la agenda estadounidense, asimismo, es necesario precisar el objetivo que establecen sobre la profesionalización de las fuerzas armadas en materia cibernética, ya que con ello lograrán una mejor protección.

Este análisis también nos permite observar cómo percibe EE.UU. a las amenazas en el ciberespacio, y también el cómo actuar ante ellas. Su preocupación es constante, lo que hace que comience a planear como combatirla en los próximos años, y ello lo explican en el Plan Estratégico de Seguridad Nacional de Estados Unidos para los años fiscales 2014-2018.

En este documento se establecen metas que se lograrán en 4 años, ello gracias a una estrecha cooperación entre el gobierno y los socios del sector privado para fortalecer las capacidades de ciberseguridad, asimismo, investigar el cibercrimen y compartir información útil para asegurar un ciberespacio seguro y resiliente que proteja la privacidad y los derechos civiles. Lo anterior se realizará con la puesta en marcha de cuatro prioridades estratégicas que se establecieron en el QDR de 2014 que ayudarán a salvaguardar y asegurar el ciberespacio:

- 1) Fortalecer la seguridad y la resistencia de la Infraestructura crítica contra los ciberataques y otros peligros;
- 2) Asegurar la empresa de tecnologías de la información del gobierno civil federal;
- 3) Promover la aplicación de la ley

cibernética, la respuesta a incidentes y la capacidad de informar; y 4) Fortalecer el ecosistema cibernético.²¹⁰

Con el Plan Estratégico de Seguridad Nacional de Estados Unidos para los años fiscales 2014-2018 se busca reducir el riesgo cibernético nacional a través del Marco de Seguridad Cibernética, ayudándose de campañas de concientización pública y mejores prácticas, lo cual incrementará las capacidades básicas de la infraestructura crítica.

Como podemos observar, este Plan ya no solo buscará que el Estado actúe para combatir al cibercrimen, también fomenta la cooperación entre el sector privado y los usuarios domésticos del ciberespacio, ello a través de campañas de concientización cuyo objetivo será disminuir los riesgos e impactos de un ciberataque.

El compromiso de todo Estado, pero, principalmente de Estados Unidos, será el proteger a todo usuario, infraestructura crítica o empresa que utilice el ciberespacio ante un posible ataque. Es por esto que los presidentes se han encargado de fomentar políticas que ayuden a mejorar la protección en este nuevo espacio.

Comenzó a debatirse el tema con George W. Bush, Barack Obama lo puso en marcha y llevo a cabo acciones que ayudaron a poner a la ciberseguridad, como un tema prioritario en la agenda de riesgos no solo de Estados Unidos, si no en la agenda global.

El reto del próximo presidente electo Donald Trump será darle continuidad a las políticas implementadas por Obama, dentro de sus promesas de campaña y debates presidenciales, el ahora presidente electo, promete ordenar de manera inmediata una revisión de todas las defensas y vulnerabilidades cibernéticas de Estados Unidos, incluyendo a las infraestructuras críticas, ello a través de la

²¹⁰ Departamento del Homeland Security, *"Fiscal Years 2014-2018 Strategic Plan"*, 2014, en línea, dirección URL: <http://bit.ly/29Rukpt>, consultado el 14 de noviembre del 2016.

conformación de un Equipo de Revisión Cibernética que se conformará por el ejército, la policía y el sector privado.

Este Equipo de Revisión Cibernética, bridaré recomendaciones específicas para salvaguardar a diferentes entidades, proporcionando la mejor tecnología en materia de defensa para combatir las posibles ciberamenazas, además de hacer un seguimiento periódico en varias agencias y departamentos federales.

En este mismo sentido, Donald Trump propone una mejora del USCYBERCOM mediante una revisión que harán el Secretario de Defensa y el Presidente del Estado Mayor Conjunto quienes proporcionarían recomendaciones para mejorar este Comando.

Un punto que causa conmoción dentro de estas acciones que el presidente electo planea ejecutar, es el desarrollo de capacidades cibernéticas en materia ofensiva, con el objetivo de disuadir a los enemigos estatales o no estatales y si es el caso, responder adecuadamente ante un ataque.

Estados Unidos se encuentra preparado para responder ciberataques, la nueva administración tiene el reto de hacer aún más fuerte la capacidad cibernética de este país, el desarrollo de ciberarmamento comienza a ser un secreto a voces que hace evidente la preocupación de los mandatarios en proteger la integridad del Estado.

Así lo demostró George W. Bush, quien aún en sus últimos momentos como presidente ideó y puso en marcha una Operación estratégica que bien o mal, lograría su objetivo primordial: retrasar el programa de enriquecimiento de uranio que se estaba llevando a cabo en Irán

La Operación Juegos Olímpicos quedará vista como el inicio de la era ciber en el siglo XXI, ya que por primera vez un virus era capaz de hacer tanto daño a una infraestructura física que provocaría un retraso, que, evidentemente beneficiaría a un Estados Unidos temeroso por su estabilidad.

Stuxnet, Duqu y Flame son tres ciberarmas producto de esta operación con capacidades ofensivas sumamente altas, si no hubiera sido por el error que nadie calculó y que hizo que Stuxnet saliera a la luz, tal vez hoy en día no se sabría de estos tres malwares, debido a que son muy difíciles de detectar.

Otro de los factores que evita la captura de los responsables es que los ciberataques son anónimos, la autoría de es difusa, ya que los hackers o ciberguerreros están parapetados en servidores falsos y crean programas y softwares capaces de difuminar su ubicación.

Posterior a la Operación Juegos Olímpicos y ya con Obama en el poder, el tema de la ciberseguridad se vuelve prioritario para Estados Unidos, el Quadriennial Defense de 2010 incluye de manera significativa el tema, y el de 2014 ya lo reconoce como una de las principales amenazas para el país.

El departamento de defensa de este país a través del USCYBERCOM comienza a vigilar detalladamente el ciberespacio, a través del encriptamiento de redes de información. Por primera vez este país reconoce que se están fabricando ciberarmas para defenderse ante un ciberataque, pero no reconoce ningún ataque previo.

Asimismo, Estados Unidos utiliza su influencia en organismos internacionales como en la OTAN para crear un mecanismo legal que ayude a la solución de los cibercrimenes, me refiero al Manual de Tallin que en 2013 llegaría a ser considerado como el primer intento de regulación jurídica internacional ante ciberataques, pero no es así, este Manual es meramente una recomendación sobre el cómo hacerle frente a un cibercrimen, no es coercitivo y si llegará a adoptarse no sería internacional debido a que solo lo adoptarían los países miembros de la OTAN.

A través de 95 reglas, este manual sugiere diversos mecanismos para combatir el cibercrimen, pero es rescatable y a la vez polémico es la actuación de las autoridades. Este manual justifica el hecho de matar a un hacker civil que haya participado en un incidente de ciberguerra, ciberespionaje o ciberterrorismo.

Ejemplos como el anterior evidencian que la ciberguerra ya no es un conflicto del futuro, ni suceso de ciencia ficción, es necesario prepararse para este conflicto, el incremento de gasto militar en materia de ciberseguridad aumenta en los países desarrollados. Gobiernos y empresas buscan, actualmente, a programadores o hackers, que tengan las habilidades para crear nuevos softwares, esto nos da a entender que Stuxnet solo fue el principio de una producción masiva de ciberarmas que veremos en el futuro. Dentro de este conflicto, las estrategias clásicas, deben ser replanteadas para adaptarlas a este nuevo escenario internacional.

La prevención es prioritaria, pero no por ello el mecanismo que garantice una mejor seguridad, el manejo de los riesgos y amenazas debe ser efectivo, pero también se debe dar pie a crear acciones o medidas para que un agente que ha sido atacado pueda reponerse por sí mismo a los ciberataques, es decir, hacer que exista dentro del Estado la ciberresiliencia.

Crear un mecanismo internacional que sea capaz de contener a las ciberamenazas y a los actores, no es tarea sencilla. Países como España, Alemania, Francia, Brasil y Estonia, han seguido el ejemplo estadounidense y lograron poner en marcha mecanismos que castiguen o, al menos, minimicen los daños de un ciberataque. Pero, desafortunadamente, estos siguen siendo esfuerzos nacionales, ya que ningún país estaría dispuesto a ceder parte de su soberanía para lograr una legislación internacional, ya que, el ciberespacio no tiene un lugar fijo.

Mientras no exista una regulación a nivel internacional, ataques como el de Stuxnet seguirán pasando con mayor frecuencia y las infraestructuras críticas serán los objetivos, ya que son infraestructuras vitales para el funcionamiento y desarrollo del país.

Irán es una potencia media que está aprovechando los recursos con los que cuenta, y su posición geográfica privilegiada. Convirtiéndose en un pivote geopolítico en el área de Medio Oriente.

El Programa Nuclear Iraní representa un gran riesgo internacional, pero sobretodo representa un riesgo para Estados Unidos, quien no permitirá que un país tenga mayor armamento nuclear. Los intereses estadounidenses por la suspensión del PNI no son por la defensa de valores altruistas en vistas de amenazas a la paz y seguridad internacionales. El desarrollo de armas nucleares por parte de Irán haría que un país tan fuerte como lo es Estados Unidos, reduzca su fuerza militar. El desarmamiento nuclear debe ser por todos y no solo de un país como Irán, el apoyo que ha buscado Estados Unidos ha sido una cortina.

La Operación Juegos Olímpicos demostró la capacidad de un Estado para idear nuevas formas de ataque y aprovechar los recursos con los que cuenta. Esta acción representa la extensión del poder estadounidense a nuevos medios, con la finalidad de defender al país ante posibles amenazas que pongan en riesgo su seguridad y estabilidad. La visión de occidente (y en particular de Estados Unidos) es clara, Irán representa una amenaza que debe ser contenida, y la ciberguerra es una opción.

El argumento central de esta investigación se comprueba ya que las acciones llevadas a cabo por parte del presidente Barack Obama hacen especial énfasis en protegerse ante diversos ciberataques de los que puedan ser objeto, el ataque al PNI confirmó que tan preparado estaba EE.UU. para un ataque hacia una infraestructura crítica, pero también dejó ver que debían tomarse las medidas necesarias para responder ante una posible respuesta. Es por ello que Barack Obama lleva a cabo diversas acciones involucrando a todos los sectores de la población estadounidense, con las empresas crea el Decreto de ciberseguridad de 2013, además de la creación del USCYBERCOM y el Cybersecurity National Action Plan, ahora el reto será saber si estas acciones son suficientes para la respuesta ante los inminentes ciberataques que se presentan en un mundo cada vez más digitalizado y menos protegido en este ámbito.

Fuentes de consulta

Bibliografía

- Aron, Raymond, “La república imperial”, Editorial Emecé, Buenos Aires, Argentina, 1974. 388 págs.
- Boureston, Jack and Ferguson, Charles D.: «Schooling Iran’s atom squad», Bulletin of the Atomic Scientists, volumen 60, número 3, pp. 31-35, mayo-junio de 2004, citado en Núñez García- Sauco, “Irán como pivote geopolítico”.
- Cano M. Jeimy, “Inseguridad de la información: una visión estratégica”, Editorial Alfaomega, Bogotá, 2013, 198 págs.
- Capitán de Fragata Ponce de León y Marcos Enrique Carlos, “Las redes sociales en el ciberespacio como herramienta de la política”, en Seguridad y Defensa del Ciberespacio, Secretaria de Marina, México, 2015, pág. 439 págs.
- Clarke A. Richard, Knake K. Robert (traducción de Noriega Luis Alfonso), “Guerra en la red: Los nuevos campos de batalla”, Editorial Ariel, Barcelona, 2011, 368 págs.
- Clausewitz, Karl Von. “De la Guerra”, Ed. Terramar Ediciones, 2008, 308 págs.
- David Gallo Facundo, “Inseguridad informática”, S/E, Madrid, 2012, 280 págs.
- Denning, Dorothy E. “Activism, Hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy”, en Arquilla, J. y Ronfeldt, D. F. 2011, (Ed.), Networks and Netwars: The Future of Terror, Crime, and Militancy, Santa Monica, Rand, pp. 239-288.
- Díaz Viana Luis, “El regreso de los lobos: la respuesta de las culturas populares a la era de la globalización”, Consejo Superior de Investigaciones Científicas. Departamento de Antropología de España y América, Madrid, 2003, pág. 97

- Diccionario Enciclopédico Usual Larousse (2012), México D.F., México Larousse
- Eric Hobsbawm, Guerra y paz en el siglo XXI, Editorial Crítica, España, 2007, 180 págs.
- Gendron Bernard, 1977, Technology and the Human Condition, Technology and Culture Vol. 18, No. 3, 568 págs.
- Gómez Vieites Álvaro, *“Enciclopedia de la seguridad informática”*, 2ª Edición, Editorial Alfaomega, Madrid, España, 2011, 828 págs.
- Held David and Mc Grew Anthony, “The global transformations reader: An introduction of Globalization debate”, Ed. Great Britian Polity Press, Gran Bretaña, 2003, 624 págs.
- Hobbes, Tomas, *“El Leviatán”*, Madrid, Editora Nacional, 1979, 576 págs.
- Jordan, T Y Taylor, P. “Hacktivism and Cyberwars: rebels with a cause?”, Routledge, 2004, 185 págs.
- Lujan Mora Sergio, “Programación de aplicaciones web: historia, principios básicos y clientes web”, Editorial Club Universitario, Alicante, 2002, 354 págs.
- Marco Galindo María de Jesús, *“Escaneando la Informática”*, Editorial UOC (Universitat Oberta De Catalunya), 2010, 256 págs.
- Margaix Arnal, Dídac. “Conceptos de web 2.0 y biblioteca 2.0: origen, definiciones y retos para las bibliotecas actuales”. En: El profesional de la información, 2007, marzo-abril, v. 16, n. 2, pp. 95-106.
- Marroquín Néstor, “Tras los pasos de un... Hacker”, Editorial Independiente, Quito, 2010, 720 págs.
- Mary Kaldor, “Las nuevas guerras: violencia organizada en la era global”, España, Editorial Tusquets, 2001, 248 págs
- Mesa del Monte Luis, “Las políticas de Bush y Obama hacia la República Islámica de Irán. La centralidad del factor nuclear”, El Colegio de México, A.C., Foro Internacional, vol. XLIX, núm. 4, octubre-diciembre, 2009, pág. 832

- Morales, Isidro, “Globalización y regionalización. Hacia la construcción y gestión de un nuevo orden económico internacional”, en Zidane Ziraoui, “Política Internacional Contemporánea” Ed. Trillas, México, 2000, 387 págs.
- Nye, Joseph. “La naturaleza cambiante del poder norteamericano”. Buenos Aires. GEL. 1991. 304 págs.
- Orozco Alcántar José Luis, Filosofía norteamericana del poder, México, Cd. Juárez, Universidad Autónoma de Ciudad Juárez, 1995, 166 págs
- Robert Jervis, “*Cooperation under the Security Dilemma*”, World Politics , Vol. 30, No. 2, 1978, p.58
- Sábada Chalezquer Charo, Domingo Prieto Víctor, et al. “La protección y seguridad de la persona en internet: Aspectos sociales y Jurídicos”, Editorial REUS, Madrid, España, 2014, 208 págs
- Trigo Aranda Vicente, “Ciencia Divulgativa: Del Abaco A Internet”, Editorial Creaciones Copyright, S/L, 2010, 154 págs
- Waever, O. “Securitization and Desecuritization” en Lipschutz, R.(Ed.), On Security, Nueva York: Columbia University Press, 1995, 233 págs.

Cibergrafía

- 20 minutos.es “Estados Unidos potencia la ciberseguridad por miedo a un Pearl Harbor informático” 31 de enero del 2013 , en línea, dirección URL: <http://bit.ly/1Slolgc>, consultado el 6 de noviembre del 2015
- Acuña Calviño Daniel, “Ciberterrorismo, un reto para los próximos años”, en línea, Madrid, España, Revista electrónica DINLET (Difusión de las Ingenierías informática y telecomunicaciones), marzo 2010, p.88, Dirección URL: <http://bit.ly/2djkmEC>, consultado el 04 de junio del 2016.
- Administración Nacional de la Aeronáutica y del Espacio, conocida como NASA (National Aeronautics and Space Administration), “*Sputnik and The Dawn of the Space Age*”, EE.UU., NASA Main Page Multimedia Interactive Feature on 50th Anniversary of the Space Age, en línea, 10 de octubre del 2007, consultado: 06 de noviembre de 2015.

- Alandente David, “Obama ordenó un ataque cibernético contra Irán del que perdió el control”, junio del 2012, en línea, dirección URL: <http://bit.ly/2eU16wk>, consultado el 17 de octubre del 2016
- Amador José, “Guerra informática: el lado desconocido del acuerdo de Irán sobre su programa nuclear”, julio 2015, en línea, dirección URL: <http://bit.ly/2etAwKs>, consultado el 10 de septiembre del 2016..ly/2eD8GvD, consultado el 23 de octubre del 2016.
- BBC, “El virus que tomó control de mil máquinas y les ordenó autodestruirse”, julio 2015, en línea, dirección URL: <http://bbc.in/1GDvzCY>, consultado el 18 de octubre del 2016.
- BBCL, “Cronología de los sucesos más importantes de Internet”, Marzo 2014, en línea, dirección URL: <http://bit.ly/2do6y8z>, consultado el 25 de junio del 2016
- CCN Expansión, “5 ‘fails’ de las empresas en ciberseguridad”, 18 de noviembre del 2014, en línea, dirección URL: <http://bit.ly/1xNlcsj>, consultado el 13 de noviembre del 2015.
- Centro Criptológico Nacional, “Ciberseguridad. Una prioridad nacional”, en línea, enero 2013, Madrid, España, Dirección URL: <http://bit.ly/2dsSexl>, consultado el 04 de junio del 2016.
- CNN, Joy Oliver, “Mandiant: China is sponsoring cyber-espionage”, Febrero 2013, en línea, dirección URL: <http://cnn.it/2dozxJ7>, consultado el 13 de julio del 2016
- Collin Barry, “The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge”, en línea, Estados Unidos, Dirección URL: <http://bit.ly/2dfVXiQ>, consultado el 4 de junio del 2016
- Como Hacer para, “Diferencias entre un Hacker y un Cracker”, 10 de abril del 2014, en línea, dirección URL: <http://bit.ly/1zWjHy4>, consultado el 3 de diciembre del 2015.
- Cory Janssen, “Cyberspyng”, en línea, Techopedia, Dirección URL: <http://bit.ly/2cMrcgT>, consultado el 04 de junio del 2016

- DCAF, Democratic Governance Challenges of Cyber Security, en línea, Génova, DCAF, 2009, Dirección URL: <http://bit.ly/2cx8Apa>
- Delicia Zurita, María, “La guerra Fría desde la óptica de las Relaciones Internacionales”, Universidad Nacional de La Plata (Argentina), 2007, artículo consultado en línea; <http://bit.ly/1QVKtyu>, consultado el 29 de agosto del 2014
- Departamento del Homeland Security de los Estados Unidos, “What Is Critical Infrastructure?”, 2015, en línea, dirección URL: <http://bit.ly/2fbhgQ3>, consultado el 04 de octubre del 2016.
- Discurso emitido por el presidente de los Estados Unidos, Barack Obama, durante la firma del “Decreto de ciberseguridad para enfrentar los ciberataques en los Estados Unidos” el 13 de febrero del 2014, obtenido en línea; <http://bit.ly/1QtYqS4>, consultado el 23 de agosto del 2014.
- E. Sanger David, NYTimes, “Obama Order Sped Up Wave of Cyberattacks Against Iran”, junio del 2012, en línea, dirección URL: <http://nyti.ms/1EhRr87>, consultado el 17 de octubre del 2016.
- EL MUNDO ES, “Estonia es el primer país que realiza sus votaciones parlamentarias por Internet”, Marzo 2007, en línea, dirección URL: <http://bit.ly/2dJ0c6O>, consultado el 13 de julio del 2016
- El mundo.es, “EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán”, junio 2012, en línea, dirección URL: <http://bit.ly/2epmARh>, consultado el 18 de octubre del 2016.
- El país “Lista de empresas afectadas por el ciberataque”, octubre del 2016, en línea, dirección URL: <http://bit.ly/2dLfzJY>, consultado el 23 de octubre del 2016.
- El país, “El virus Duqu aprovecha un agujero de Windows para infiltrarse”, noviembre 2011, en línea, dirección URL: <http://bit.ly/2fcJuw4>, consultado el 18 de octubre del 2016.
- EL PAIS, Fuentes Julio, “Guerra informática en Serbia”, en línea, Abril 1999, España, dirección URL: <http://bit.ly/2di65Fu>, consultado el 26 de junio del 2016.

- Fayer Wayer, “A Sony le costará USD \$15 millones arreglar el ataque a Sony Pictures”, 4 de febrero del 2015, en línea, dirección URL: <http://bit.ly/21Kdyi9>, consultado el 17 de noviembre del 2015
- Fayer Wayer, “Texto cifrado en el logo del USCYBERCOM (Actualizado)”, 7 de julio del 2010, en línea, dirección URL: <http://bit.ly/1QuEwCZ>, consultado el 25 de julio del 2016.
- FBI, “Los delitos cibernéticos más recientes”, septiembre 2015, en línea, dirección URL: <https://www.fbi.gov/espanol/historias/los-delitos-ciberneticos-mas-recientes>, consultado el 12 de noviembre del 2015.
- FBI, “Terrorism”, en línea, Estados Unidos, Dirección URL: <http://bit.ly/1nsbpT8>, consultado el 04 de junio del 2016.
- Foro Económico Mundial, “Tech utopia or cybergeddon?”, enero 2013, en línea, dirección URL: <http://bit.ly/2cVif6S>, consultado el 17 de junio del 2016.
- Fragmento encontrado en: Orozco Gabriel, “*El concepto de la seguridad en la Teoría de las Relaciones Internacionales*”, en línea, Barcelona Revista CIDOB d’Afers Internacionals, núm. 72, p. 161-180, Dirección URL: <http://bit.ly/1QOwkW5>, consultado el 27 de agosto del 2014.
- Gijón Anastasio, “Hallados los Responsables del Ataque a Sony Pictures”, 31 de diciembre del 2014, en línea, dirección URL: <http://bit.ly/21Kdyi9>, consultado el 2015
- González Veiguela Lino “Los ciberataques (conocidos) más importantes” en línea, Julio 2013, dirección URL: <http://bit.ly/2cUte0W>, consultado el 26 de junio del 2016
- IEEE, Ureña Centeno Francisco, “Ciberataques, la mayor amenaza actual”, en línea, Enero 2015, España, Dirección URL: <http://bit.ly/1yj9NFt>, consultado el 26 de junio del 2016.
- ISACA, “Ciberataques. ¿Estamos preparados?”, en línea, Buenos Aires, dirección URL: <http://bit.ly/2cE5RIN>, consultado el 20 de junio del 2016.

- Jot Down.com “La guerra de las galaxias de Ronald Reagan”, 2013, en línea, dirección URL: <http://bit.ly/1PwJ0eb> consultado el 01 de octubre del 2014
- Kaspersky Lab, “What is Flame Malware?”, 2012, en línea, dirección URL: <http://bit.ly/2fj1ilG>, consultado el 18 de octubre del 2016.
- Kaspersky Lab, “Los ataques DDoS en el primer trimestre de 2016”, Abril 2016, en línea, dirección URL: <http://bit.ly/2jO51O2>, consultado 20 de diciembre del 2016.
- Kaspersky Lab, “Los ataques DDoS en el tercer trimestre de 2016”, Octubre 2016, en línea, dirección URL: <http://bit.ly/2keig7x>, consultado 20 de diciembre del 2016.
- Kjellen Rudolf, El Estado como forma de vida, Citado por Rosales Ariza Gustavo, “geopolítica geoestrategia, liderazgo y poder”, 2005, Universidad Militar de Nueva Granada, Colombia, pág. 17, en línea, dirección URL: <http://bit.ly/1hqzvdF>, consultado el 10 de septiembre del 2016.
- La nación, “¿Hackers rusos y chinos, autores del ciberataque?”, octubre del 2016, en línea, dirección URL: <http://bit.ly/2ejZVbA>, consultado el 23 de octubre del 2016.
- López C. Orlando, “Hackers & Crackers& phreakers: una perspectiva ética” en Revista Tecnológica Volumen 2 de la Universidad del Bosque, julio-diciembre 2003, documento pdf, en línea, dirección URL: <http://bit.ly/24DNSGg>, pág. 60, consultado el 5 de diciembre del 2015
- López Michelone Manuel, “Hace 25 años salió el primer virus en Internet”, 3 de noviembre del 2013, en línea, dirección URL: <http://bit.ly/21Kde2K>, consultado el 7 de noviembre del 2015.
- María Cristina Rosas, “De la ciberguerra a la ciberpaz”, en línea, revista Etcétera, 2011, dirección URL: <http://bit.ly/2cPIY6p>, consulta: 13 de febrero de 2013.
- Ministerio de Defensa de España, “Disposiciones generales. Definiciones”, emitido el 26 de febrero del 2013, en línea, dirección URL: <http://bit.ly/2bA6Afb>, consultado el 23 de junio del 2016

- Ministerio de Defensa Español, “Monografía 137: Necesidad de una conciencia nacional de ciberseguridad”, septiembre del 2013, en línea, dirección URL: <http://bit.ly/1Rsfllel>, documento pdf, pág. 80-81
- Ministerio de Defensa Español, “Orden Ministerial 10/2013: Guerra Cibernética: Aspectos Organizativos”, 19 de febrero del 2013, en línea, dirección URL: <http://bit.ly/2cPIY6p>, consultado el 15/04/2016, pág. 4.
- NATO, “Cyber definitions”, 2010, en línea, dirección URL: <http://bit.ly/2iYNPG7>, consultado el 12 de enero de 2016.
- Núñez García- Sauco, Antonio, “Irán como pivote geopolítico”, Junio 2010, en línea, dirección URL: <http://bit.ly/1dBNrTB>, consultado el 10 de septiembre del 2016.
- Ortega García Julián, Instituto Español de Estudios Estratégicos, “Programa Nuclear Iraní: Una Visión Técnica”, septiembre 2012, en línea, dirección URL: <http://bit.ly/2f8ChNC>, consultado el 07 de octubre del 2016, pág. 2
- Panda Security, “Phishing”, Agosto 2009, en línea, dirección URL: <http://bit.ly/1QuDx5R>, consultado el 12 de noviembre del 2015
- Para Libros, “Internet y la World Wide Web”, 2008, en línea, dirección URL: <http://bit.ly/2dC98XE>, consultado el 25 de junio del 2016.
- Plan Nacional de Protección de Infraestructuras Críticas, “Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas”, abril 2011, en línea, dirección URL: <http://bit.ly/2ffQpBg>, consultado el 04 de octubre del 2016.
- Procuraduría Federal del Consumidor (PROFECO), “Comercio electrónico”, enero 2012, en línea, dirección URL: <http://bit.ly/1dziHh7>, consultado el 13 de noviembre del 2015
- R. Suarez Héctor, D. Peláez Álvarez Juan, “Ciber- resiliencia: Aproximación a un marco de medición”, INTECO (Instituto Nacional de Tecnologías de la Comunicación), España, S/A, pág. 19, en línea, dirección URL: [http://bit EL PAIS, Belinchon Gregorio, “La ciberguerra, la nueva arma de destrucción masiva”, Febrero 2016, en línea, dirección URL: <http://bit.ly/2dUTU2e>, consultado el 10 de septiembre del 2016.](http://bit.ly/2dUTU2e)

- Radio Radica.le “Ninguna nación puede solucionar sus problemas por sí solo”, en línea, Italia, 2005, dirección URL: <http://bit.ly/1QuCZNe>, consultado el 1 de septiembre del 2014
- Revista soluciones, “Qué es y Cómo Funciona el Virus Flame”, mayo 2012, en línea, dirección URL: <http://bit.ly/2f2h8C2>, consultado el 18 de octubre del 2016.
- Reyes E. Giovanni, “Teoría de la Globalización: Bases Fundamentales”, en Nómadas, núm. 3, enero-junio, 2001, Universidad Complutense de Madrid, España, en línea, dirección URL: <http://bit.ly/21GRw31>, consultado el 20 de octubre del 2014
- Rodríguez Bernal Antonio, “Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia”, 5 de septiembre del 2006, en línea, dirección URL: <http://bit.ly/2cyZyVv>, consultado el 17 de abril del 2016.
- Rosas González María Cristina, “Ciberespacio, Crimen Organizado y Seguridad Nacional” en Revista del Centro de Estudios Superiores Navales, julio- septiembre del 2011, documento pdf, en línea, dirección URL: <http://bit.ly/1p1UJji>, pág.13.
- S/A “Internet y la World Wide Web”, 1998, en línea, dirección URL: <http://bit.ly/1p1U36S>, consultado el 6 de noviembre del 2015.
- S/A, “Todo sobre el ataque norcoreano a Sony”, 19 de diciembre del 2014, en línea, dirección URL: <http://bit.ly/1oSethR>, consultado el 17 de noviembre del 2015.
- S/A, RTVE, “Cronología de la crisis nuclear iraní”, enero 2016, en línea, dirección URL: <http://bit.ly/2f9reE6>, consultado el 14 de octubre del 2016
- S/A, RTVE, “Irán crea un cibercomando especializado en la lucha contra los ataques informáticos”, octubre 2011, en línea, dirección URL: <http://bit.ly/2fgxk1T>, consultado el 14 de octubre del 2016.
- Sánchez Manuel, “Infraestructuras Críticas y Ciberseguridad”, julio 2011, en línea, dirección URL: <http://bit.ly/2elSGNB>, consultado el 04 de octubre del 2016.

- Sánchez Medero Gema, “La ciberguerra: los casos de Stuxnet y Anonymous”, en línea, Revista Derecom No. 11. Nueva Época. Septiembre- Noviembre, 2012, Dirección URL: <http://bit.ly/2dxTsUA>, consultado el 26 de junio del 2016.
- Secretaría de Estado de Comercio de España, “Irán, la importancia de la geopolítica y su vuelta a la comunidad internacional”, Boletín electrónico, Mayo 2015, en línea, dirección URL: <http://bit.ly/2eS8AxD>, consultado el 24 de septiembre del 2016.
- Symantec, “Ciber- resiliencia”, febrero 2013, en línea, dirección URL: <http://symc.ly/2dzv4BI>, consultado el 23 de octubre del 2016.
- Symantec, “El gusano Stuxnet”, 2010, en línea, dirección URL: <http://symc.ly/2fcaOLg>, consultado el 18 de octubre del 2016.
- Tecnología 21, Paredes Meylin, “Obama firma decreto ley sobre ciberseguridad”, Febrero 2013, en línea, dirección URL: <http://bit.ly/2dR4shc>, consultado el 28 de agosto del 2016.
- The White house, Daniel Michael, Scott Tony, “Presidents national cybersecurity plan what you need know”, Febrero 2016, en línea, dirección URL: <http://bit.ly/20LUYZG>, consultado el 28 de agosto del 2016.
- Thierse, Wolfgang, “Globalización y capacidad de estructuración de la política”, Materiales de Trabajo No. 10, Facultad Latinoamericana de Ciencias Sociales (FLACSO), México, 1999, Fundación Friederich Ebert, en línea; dirección URL:<http://bit.ly/1TbiGKs> pág. 8, consultado el 22 de octubre del 2014
- TIME RIME, “ARPANET deja de existir”, 2015, en línea, dirección URL: <http://bit.ly/2dkHUqY>, consultado el 25 de junio del 2016
- U.S. Department State, “Terrorism” ”, en línea, Estados Unidos, Dirección URL: <http://bit.ly/1efkxtF>, consultado el 4 de junio del 2016. Traducción propia.
- UIT-ONU, “Decisiones destacadas de Guadalajara: Resolución 181: Definición de Ciberseguridad”, en línea, dirección URL: <http://bit.ly/1PCGgzp>, consultado el 26 de marzo del 2016.

- UNODC, “Comprehensive Study on Cybercrime”, 2013, en línea, dirección URL: <http://bit.ly/1ppgOOs>, consultado el 17 de abril de 2016.
- Vargas Vargas, Edison. (2014). Ciberseguridad y Ciberdefensa: ¿Qué implicaciones tiene para la Seguridad Nacional?. Especialista en Alta Gerencia de la Defensa Nacional. Universidad Militar Nueva Granada, Facultad de Relaciones Internacionales, Estrategia y Seguridad, en línea, dirección URL: <http://bit.ly/2cWcsAM>, consultado el 20 de abril del 2016