UNIVERSIDAD TORCUATO DI TELLA
Departamento de Ciencia Política y Estudios Internacionales

LOS ATAQUES CIBERNÉTICOS Y SUS REPERCUSIONES POLÍTICOS GLOBALES

Alumna: Jessica Yancey
ID# 10W424
Tutor: Jorge Battaglino

Abril, 2017

TABLA DE CONTENIDOS

INTRODUCCIÓN

En el presente proyecto de tesis, discutiré los fenómenos actuales conocidos como WikiLeaks, Anonymous, y los "Ciberataques". Analizaré cada organización desde que fueron creadas hasta que lograron impactar en las relaciones internacionales, aunque haré hincapié en las repercusiones causadas en los Estados Unidos. He elegido este tema debido a que tengo gran interés sobre el papel que cumple la tecnología en nuestra sociedad; me interesa saber cómo se ha utilizado en los últimos años en contra de distintas organizaciones y estados, así marcando un nuevo paradigma mundial. También me ha resultado muy llamativo el rol que ha adoptado el Estado estadounidense a partir de los ataques sufridos, las diferentes posturas que tomó ante cada situación y las nuevas políticas que está aplicando actualmente ante posibles amenazas. Mi intención en este trabajo es demostrar que la aparición de dichas organizaciones cibernéticas ha impactado de manera negativa a las políticas internacionales y diplomáticas de los Estados Unidos. ¿Qué daños pueden producir los ciberataques?

Comprobaré, mediante la investigación de artículos académicos, documentos gubernamentales, informes de la NSA (Agencia de Seguridad Nacional) y otros informes de espionaje cibernético chino, cómo el desarrollo de estas organizaciones ha impactado negativamente a los Estados Unidos. En los últimos tiempos, los Estados Unidos también han sido testigos de los cambios sobre la seguridad cibernética empresarial y la piratería. Las grandes corporaciones han sufrido *hackeos* de sus bases de datos, y esto ha cambiado la forma en que las empresas ven su propia seguridad en la red.

En los últimos 10 años, la seguridad cibernética ha comenzado a cobrar relevancia en todo el mundo, en particular en los Estados Unidos. ¿Qué tan grande fue el impacto de las filtraciones de WikiLeaks en Estados Unidos, tanto política como económicamente? ¿Cuáles son las estructuras de WikiLeaks? ¿Quiénes son los principales actores en Anonymous? ¿Cómo afectan estos a la política estadounidense? ¿Cuáles son los principales Ciberataques que han sufrido los Estados Unidos en los últimos 10 años?

Estados Unidos mostró una serie de fallas e incongruencias graves en la lucha contra la seguridad cibernética en los últimos 10 años. ¿Cómo hacen para sobrevivir

frente a estos inconvenientes? ¿Cómo respondemos estas preguntas? En los últimos 10 años se han llevado a cabo ataques cada vez más graves al gobierno de Estados Unidos. Hoy, gracias a las advertencias de los legisladores de alto rango y de los funcionarios de la administración de Obama, los estadounidenses son cada vez más conscientes de las vulnerabilidades en Internet que podrían conducir a un ataque "ciber Pearl Harbor".[i] En 2007, el año de fundación de Twitter, US-CERT ha recibido casi 12.000 ciber-informes. Para el 2009, esa cifra aumentó más del doble, según las nuevas estadísticas de la Oficina de Responsabilidad del Gobierno de Estados Unidos, y para el 2012, se cuadruplicó. Los ciberataques son cada vez más frecuentes a nivel global. En cierta forma, estas son buenas noticias: un estado de alerta creciente lleva a una mejora en el desarrollo de medios de detección.[ii]

HISTORIA MUNDIAL DE LOS ATAQUES CIBERNÉTICOS

Un "ciberataque" se define como "un intento de dañar, interrumpir, u obtener acceso no autorizado a una computadora, sistema informático o red de comunicaciones electrónicas".[ii] En contraste con una guerra cibernética, el ciberterrorismo, y el espionaje cibernético; un ciberataque puede ir desde la instalación de spyware en una PC hasta intentos de destruir la infraestructura de naciones enteras. Los ciberataques se han vuelto cada vez más sofisticados y peligrosos, como ya muchos ejemplos han demostrado.

Un buen ejemplo, son los gusanos informáticos. Estos son programas maliciosos independientes que se replican a sí mismos para propagarse a otras computadoras.[iii] Uno de los primeros con el potencial de afectar la infraestructura cibernética del mundo fue el gusano Morris[iii] en 1988. El mismo fue obra de Robert Tapan Morris, quien afirmó haber estado tratando de calcular la dimensión y la magnitud de Internet. Posteriormente, se convirtió en la primera persona en ser condenada por fraude informático y violación de la Ley de los Estados Unidos, e irónicamente ahora trabaja como profesor en el Instituto Tecnológico de Massachusetts (MIT). La Ley de Fraude y Abuso fue promulgada por el Congreso en 1986 como una enmienda a la ley de fraude informático existente (18 USC § 1030), que había sido incluida en la Ley Integral de Control del Crimen de 1984[iv].

A raíz de este ataque, no fue hasta diciembre de 2006 que la NASA (National Aeronautics and Space Administration) se vio obligada a bloquear mensajes de correo electrónico con archivos adjuntos antes de los lanzamientos espaciales por temor a que sean *hackeados*. Ese año los planes para el lanzamiento espacial habían sido obtenidos por intrusos extranjeros desconocidos. A partir de entonces, cada año siguiente, y casi todos los meses, los ciberataques se convirtieron en una amenaza común en todo el mundo. En abril de 2007, el gobierno de Estonia fue acosado y hubo rebeliones cibernéticas. En junio de 2007, la cuenta de correo electrónico no clasificado de la Secretaría de Defensa del Estado fue *hackeada* por intrusos extranjeros desconocidos como parte de una serie más amplia de ataques al acceso a las redes del Pentágono.

En octubre de 2007, el Ministro de Seguridad de la República Popular China fue

hackeado por Taiwán y los Estados Unidos. A partir de 2008-2009, los Estados Unidos, Georgia, e Israel habían todos sido atacados. Los *hackers* atacaron la infraestructura de Internet de Israel durante la ofensiva militar en la Franja de Gaza, lo cual afectó al menos 5.000.000 de computadoras.

En enero de 2010, el mundo reunió al primer grupo de *hackers* que se hizo conocer como el "Ejército Cibernético Iraní". Los mismos desestabilizaron el servicio del popular motor de búsqueda chino Baidu. Los usuarios eran redirigidos a una página que mostraba un mensaje político iraní.

En 2011, el gobierno canadiense informó sobre un ataque cibernético importante contra sus agencias. Dicho ataque obligó al Departamento de Finanzas y al Consejo del Tesoro, principales organismos económicos de Canadá, a suspender sus conexiones a Internet. Además, el subsecretario de Defensa de Estados Unidos mencionó que un contratista de defensa fue *hackeado* y 24.000 archivos del Departamento de Defensa fueron robados.

En octubre de 2012, los rusos declararon sufrir un ataque de ciber-espionaje en base a un programa de malware, y en enero de 2013 fue llamado "Octubre Rojo" por la firma rusa Kaspersky Lab. Los *hackers* reunieron información a través de las vulnerabilidades en los programas Word y Excel de Microsoft. [v]

Al año siguiente, en 2013, Corea del Sur sufrió ataques cibernéticos, y el 4 de junio de 2013 la OTAN (Organización del Tratado del Atlántico Norte) decidió que era momento de actuar. La OTAN, en su primera reunión dedicada a la defensa cibernética, acordó que la capacidad de defensa de la Alianza debía ser plenamente operativa en otoño, y que debían extender dicha protección a todas las redes propietarias y operadas por la Alianza. La "ciberdelincuencia" le cuesta a la economía estadounidense hasta $ 140 mil millones de dólares por año. Las amenazas cibernéticas que más rápido han crecido incluyen ataques a los estados nacionales, a los competidores y al crimen organizado, aunque éstos siguen siendo mucho menos frecuentes. Según los resultados de los investigadores, los ataques de los estados nacionales se incrementaron un 86% en 2014, y la actividad se centra principalmente en los sectores de telecomunicaciones de

petróleo y gas, en la industria aeroespacial y de defensa, y en la tecnología. Los informes de incidentes de seguridad atribuidos a competidores aumentaron un 64% en comparación al año anterior. Los niveles de robos por crimen organizado ultimamnte han sido particularmente altos en Malasia, India y Brasil.

Los delincuentes están intensificando su juego y la violación de la privacidad de datos es cada vez más común y devastadora. Según un estudio de Arbor Networks, el número de ataques DDoS superó 20Gbps en el primer semestre de 2014, lo cual fue el doble que en 2013. Se registraron más de 100 ataques de más de 100 Gbps en el primer semestre del año 2015.[vi]

HISTORIA DE LOS ATAQUES CIBERNÉTICOS VINCULADA A LOS ESTADOS UNIDOS

"Nada es más importante en la guerra que la unidad en el mando."

Napoleon Bonaparte[vii]

Como base para comprender los problemas de seguridad cibernética, se analizarán los estudios de casos de la Tormenta del Desierto (1990), la Operación Fuerza Aliada (1999), la Operación Protector Unificado (2011) y la Guerra Global contra el Terror (2001-presente).

En la historia de los ataques cibernéticos contra los Estados Unidos, los incidentes que se produjeron en 1990 en relación a la campaña Tormenta del Desierto se destacan como especialmente dramáticos y severos. El caso tiene todas las características de poder haber sido un ataque muy exitoso; si Saddam Hussein hubiera sido ligeramente más inteligente, cibernéticamente hablando, él bien podría haber alterado el resultado del conflicto Tormenta del Desierto / Escudo del Desierto. Para apreciar plenamente la naturaleza del ataque cibernético de 1990, es necesario colocar los eventos específicos del ataque en el contexto más amplio de los avances cibernéticos de aquel momento.

Uno de los principales retos de la era temprana de internet en la década de los 80 era la compatibilidad entre los elementos de la red. En ese momento, la industria estaba considerando la viabilidad económica de la creación de redes variadas, y por extensión, también lo hicieron las aplicaciones prácticas. Varias empresas y universidades construyeron computadoras y redes simultáneamente, y cada organización tenía su propio protocolo para la interconexión de los elementos en una red.

Los *hackers* aprendieron a acceder al control por fuera de sus computadoras individuales bastante temprano; al comenzar a conectar dichas computadoras individuales a través de redes y otros equipos como puerta de enlace, éstos encontraron maneras de aprovechar su conocimiento. Cuatro errores de seguridad, que en base a los estándares de

hoy en día se consideran relativamente arcaicos, se explotaron en 1988 con el primer gusano en toda la internet el maligno gusano Morris, un programa escrito por un estudiante de la Universidad de Cornell, Robert Tappan Morris. Los mismos incluían debilidades en Sendmail, el protocolo *finger*, los privilegios de usuarios, así también como el uso de contraseñas débiles[viii]. El gusano Morris usaba estas simples falencias de seguridad para obtener el control de una computadora central y luego enviarse a sí mismo a otros equipos de la misma red. Los equipos de puerta de enlace tenían medidas de seguridad para evitar que alguien pudiera acceder de manera no autorizada; sin embargo, no necesariamente se regulaba la información que pasaba a través de los mismos. Por lo tanto, si un gusano controlaba un *host* en una red, simplemente podría "saltar" a la siguiente red sin tener que superar posibles medidas de defensa en los equipos de puerta de enlace.

Estos acontecimientos históricos nos llevan directamente al estudio de caso Tormenta del Desierto y los incidentes que tuvieron lugar en 1990. Dos años luego del incidente con el gusano Morris, los mismos agujeros de seguridad aún existían, con muy pocos cambios en los mecanismos de defensa, por lo cual los nuevos atacantes cibernéticos explotaron precisamente las mismas vulnerabilidades. Organizar y ejecutar una estrategia eficaz para hacer frente a las violaciones de seguridad cibernética era una operación relativamente nueva.

Un artículo publicado en 1991 en el *New York Times* citó a varios expertos en informática que reconstruyeron los ataques de 1990 siguiendo las líneas principales de las actividades de los hackers, y se llegó a esta conclusión: "Las tácticas del grupo son de particular interés para los expertos en seguridad informática, porque los miembros han utilizado fallas de seguridad en varias ocasiones demostradas por un programa escrito por Robert Tappan Morris, un estudiante de la Universidad de Cornell, hace más de dos años"[ix]. Los ataques reconstruidos proporcionan amplia evidencia de la correlación entre el ataque del gusano Morris de 1988 y los ataques cibernéticos durante la Tormenta del Desierto en 1990.

"El ejército convencional pierde si no gana. La guerrilla gana si no pierde".

Henry A. Kissinger[x]

En 1999, Slobodan Milosevic entró en una batalla política astuta contra la OTAN, y en particular contra los Estados Unidos. Dos facciones en guerra competían por el dominio del campo de Kosovo: los albaneses y los serbios. Milošević lideró la facción serbia, e intentó llevar a cabo un programa de limpieza étnica brutal para eliminar a todos los albaneses de Kosovo. Pronto fue presionado por la indignación internacional para detener dichos terribles actos. La OTAN amenazó con acciones drásticas si no retiraba sus tropas de Kosovo, pero Milosevic no tenía la intención de cumplirlo.

Como parte del esfuerzo, los serbios iniciaron varios ataques cibernéticos en Occidente durante el conflicto de Kosovo. Estos ataques fueron relativamente leves en comparación a los eventos de Tormenta del Desierto. Aunque los ataques se extendieron por varios sitios dentro de la OTAN, los EE.UU. y el Reino Unido, el impacto de los ataques era relativamente insignificante. En los EE.UU. el sitio web de la Casa Blanca fue desconfigurado, y el Reino Unido reconoció haber perdido al menos un poco de información de su base de datos[xi]. El incidente de Kosovo ilustra varias lecciones importantes en materia de seguridad cibernética. En primer lugar, los componentes cibernéticos necesarios para tal conflicto alcanzaron una madurez significativa a mediados de la década de 1980; desde entonces, siguiendo con un patrón emergente, casi todos los conflictos informáticos ha tenido un elemento cibernético asociado a ellos.[xii]

"A menos que y hasta que nuestra sociedad reconozca el acoso cibernético como lo que es, el sufrimiento de miles de víctimas silenciosas continuará."

Anna Maria Chavez

ANONYMOUS

Anonymous es el grupo de *hacktivistas* más famoso del mundo. El carácter informal del grupo hace que su mecánica sea difícil de definir. Además, sin una jerarquía formal en su organización, es difícil de explicarle qué es Anonymous al público en general y a los medios de comunicación.

Hacktivista es una combinación de los términos "hackers" y "activistas". Cuando las personas tienen habilidades técnicas, tienen acceso a Internet, y entienden cómo funciona la infraestructura de distintas organizaciones y los servidores de red, puede ser tentador poner ese conocimiento en práctica para cambiar algún aspecto del mundo. La parte "activista" de "hacktivistas" significa que ellos no realizan *hackeos* ni otras acciones sin una causa particular. Las diversas personas detrás de Anonymous en todo el mundo se unen por la creencia de que las empresas y organizaciones que consideran que son corruptas deben ser atacadas. Es decir que si uno es administrador de una red que tiene pocas razones para ser objetivo de los activistas sociales, es poco probable que su red y servidores se conviertan en un blanco de Anonymous.

No todas las actividades de Anonymous implican atacar redes o sitios web. Anonymous también ha participado activamente en la iniciación de protestas públicas. Sin embargo, los canales web y de IRC son el alma del grupo. Si no fuera por Internet, Anonymous nunca hubiera existido.

En 2003, Christopher Poole, un joven de quince años de edad de la ciudad de Nueva York, lanzó "4chan", un foro de discusión donde los fans del anime podían publicar fotografías y comentarios de manera libre y anónima. El enfoque se amplió rápidamente para incluir muchos de los primeros memes de Internet: "LOLcats", "Chocolate Rain", "RickRolls". Los usuarios que no ingresaban un nombre para mostrar en pantalla fueron llamados por defecto Anonymous (Anónimos en inglés). Poole esperaba que el anonimato fuera para mantener conversaciones irreverentes. "No tenemos ninguna intención de participar en discusiones inteligentes en relación a asuntos exteriores"[xiii], escribió en el sitio. Uno de los términos más altamente buscados dentro de la comunidad 4chan fueron los "lulz", un término derivado del acrónimo LOL. *Lulz* se

refiere a lo que se produce generalmente mediante el intercambio de bromas o imágenes, muchas de ellas pornográficas o escatológicas. Lo más impactante de estos fue publicado en una parte del sitio con la etiqueta "/b/", y cuyos usuarios se llamaban a sí mismos "/b/tards".

Doyon era consciente de la magnitud de 4chan, pero consideró que sus usuarios eran "un montón de pequeños bromistas estúpidos." Aproximadamente en 2004, algunas personas en /b/ comenzaron a referirse a "Anónimo" como una entidad independiente. Era un nueva especie de *hackers* colectivos. "No es un grupo", Mikko Hypponen, un destacado investigador de seguridad informática, informó. Más bien, podría considerarse como una subcultura que cambia de forma.

Barrett Brown, periodista de Texas y un campeón bien conocido de Anonymous, lo ha descrito como "una serie de relaciones". No existe ninguna cuota de afiliación o de iniciación. Cualquier persona que quiera ser parte de Anonymous -una "lealtad Anon"- puede simplemente unirse y reclamar. En 2007, una filial local de noticias en Los Ángeles llamó a Anonymous "una máquina de odio en Internet".

El 5 de febrero de 2011, el Financial Times informó que Aaron Barr, CEO de una empresa de seguridad cibernética llamada HBGary Federal, había identificado los "más altos" miembros de Anonymous. La investigación de Barr sugirió que uno de los tres primeros había sido Comandante X, un pirata informático con sede en California, que podía "gestionar algunos poderes de fuego significativos". Barr se contactó con el FBI y se ofreció a compartir su trabajo con ellos.

Assange continuó como tal, hasta que en 2012, la Associated Press llamó a Anonymous "un grupo de hackers expertos"; Quinn Norton, en Wired, escribió que "Anonymous había descubierto la manera de infiltrarse en cualquier cosa", lo que resulta en "una cadena salvaje de *hacks* brillantes". De hecho, algunos Anon son programadores talentosos, pero la gran mayoría poseen poca habilidad técnica.

Doyon se encuentra todavía en la clandestinidad. Incluso Jay Leiderman, su

abogado, no sabe dónde está. Leiderman dice que, además de los cargos en Santa Cruz, Doyon podría enfrentar acusaciones por su papel en los atentados de PayPal y Orlando. Si es arrestado y declarado culpable de todos los cargos, podría pasar el resto de su vida en prisión, siguiendo el ejemplo de Edward Snowden, quien espera solicitar asilo de parte de los rusos.

WIKILEAKS 2006

A todo esto, es necesario continuar con la siguiente pregunta: ¿qué es exactamente WikiLeaks? Se trata de "una organización internacional sin fines de lucro que publica informes y documentos de carácter privado, secreto y clasificado, preservando el anonimato de sus fuentes". ¿Quiénes están detrás de los ataques cibernéticos? ¿Cuál es su objetivo? ¿Los de Anonymous pudieron tener un impacto global? ¿Cuáles son las principales diferencias entre Anonymous y WikiLeaks? ¿Se puede considerar *hackers* a los dos?

El propósito original de la organización WikiLeaks era someter a la exposición a regímenes opresores, así también como proteger a quienes hacían posible esta revelación de información. Mediante la publicación de los documentos en el sitio web, las fuentes de aquel material quedan protegidas tanto de contraer cargos criminales como de causarle algún perjuicio a quien suministró la información. Internet está plagado de "enlaces rotos" cuyo contenido revela asuntos de la CIA y aporta datos inverosímiles que han sido publicados por WikiLeaks, como por ejemplo el caso de los War Logs (registros de guerra). Los documentos publicados por la organización fundada por Julian Assange proporcionan un interesante conocimiento de la realidad diplomática.

Desde el lanzamiento en 2006 del sitio web, WikiLeaks, el mismo ha sido el centro de debate; este sitio web no está asociado a Wikipedia ni a la Fundación WikiMedia. Con excepción del australiano Julian Assange, no se ha podido identificar aún al resto de los fundadores de WikiLeaks. Julian Assange, es un hombre brillante, de carácter particular y excéntrico, sin embargo, existe un estereotipo de él formado por los medios con el que el mismo Assange no coincide. A pesar de encontrarse bajo arresto domiciliario y de haberse ganado como enemigos a muchas de las personas más ponderosas del mundo, él defiende su punto de vista. El argumenta que WikiLeaks no es una mera parte de su vida, sino un estilo de vida en general. Assange, quien es considerado periodista y editor, opera un sitio de internet y publica material. Muchos se refieren a él como un *hacker*, debido a que ha ayudado a desestabilizar a las más importantes instituciones con sus publicaciones.

WikiLeaks, sembró la duda desde su creación. Por ejemplo, los medios se preguntan quién fue el responsable de revelar en internet 250.000 documentos sin redactor que contenían información clasificada del Pentágono. Por consiguiente, la batalla entre la libertad de prensa y los secretos del gobierno continúa, complicando de esta manera el panorama para el fundador, a quienes algunos se refieren como a un héroe y otros como a un terrorista.

Existe material sobre la supuesta intención de ejecutar a Assange y a su equipo por parte del gobierno estadounidense, incluso en base a declaraciones hechas por el vice presidente del país. Los WikiLeaks secretos están almacenados en servidores que se encuentran en distintas partes del mundo y desde allí son publicados con un alcance global. El fundador asegura que Estados Unidos aún no cuenta con la tecnología necesaria para desactivar este sitio web tan controversial.[xiv] Aun no se sabe de qué manera va solucionar esto los Estados Unidos, y por esta razón se estudian las posibilidades y consecuencias de los resultados de los ataques.

Definido de distintas maneras, el grupo conocido como Anonymous, "en un comienzo un movimiento por diversión, desde 2008 se manifiesta en acciones de protesta a favor de la libertad de expresión, de la independencia de Internet y en contra de diversas organizaciones, entre ellas la Cienciología, los servicios públicos, las corporaciones con presencia global y las sociedades de derechos de autor."[xv] Los que influyen son los diarios, los periodistas y la sociedad en contra del gobierno. Todo esto tiene un resultado negativo sobre la política Estadounidense.

Los ciberataques le agregan una nueva realidad a los Estados Unidos. En una nota de un diario se publicó esta información: "los ataques cibernéticos podrían costarle a la economía estadounidense la suma de US$ 140 mil millones y también medio millón de puestos de trabajo cada año, de acuerdo a un nuevo estudio que reemplaza un cálculo previo que estimaba pérdidas anuales de más de US$ 1 billón."[xvi]

Aquí se puede notar cómo los ciberataques afectan no solo política sino económicamente.

Definitivamente, hay una gran posibilidad de obtener beneficios mediante WikiLeaks, aunque también ha quedado claro que la organización puede provocar más problemas de los que puede llegar a resolver. Los fundamentos legales y éticos de este sitio web son por demás cuestionables, ya que afecta los procesos políticos de las naciones del mundo, y genera un caos inmanejable. Sin embargo, no se puede dejar de reconocer que, al mismo tiempo, les da la posibilidad a los habitantes de gozar de su derecho a conocer qué está ocurriendo a puertas cerradas en sus gobiernos.

En este proyecto de tesis exploraré los fenómenos conocidos como los delitos cibernéticos y los WikiLeaks y cómo éstos afectaron la diplomacia de Estados Unidos de Norteamérica en los últimos 10 años. Los WikiLeaks son un movimiento negativo para el gobierno de los Estados Unidos y bajan la calidad del país drásticamente, los ciberataques también, y por esta razón los Estados Unidos trata de luchar contra estos fenómenos.

JULIAN ASSANGE, SU HISTORIA

Nacido el 3 de julio de 1971 en Townsville, Australia, Julian Assange usó su gran IQ para *hackear* las bases de datos de muchas organizaciones de alto perfil. En 2006, Assange comenzó a trabajar en Wikileaks, un sitio web destinado a recopilar y compartir información confidencial a escala internacional. La información que su organización lanzó le valió fuertes partidarios y poderosos enemigos. Por sus esfuerzos, el activista de Internet ganó el título de "Persona del Año" en la revista Time. Tras llegar a la Embajada de Ecuador en Londres en junio de 2012, tratando de evitar la extradición a Suecia, Assange recibió asilo político del gobierno ecuatoriano en agosto de 2012.

El periodista, programador y activista Julian Assange nació el 3 de julio de 1971, en Townsville, Queensland, Australia. Assange tuvo una infancia inusual, ya que pasó parte de sus primeros años viajando con su madre, Christine, y su padrastro, Brett Assange. La pareja trabajó para poner en acción distintas producciones teatrales.

Brett y Christine luego se distanciaron, pero Assange y su madre siguieron viviendo un estilo de vida transitorio. Con tanto movimiento, Assange terminó asistiendo a aproximadamente 37 escuelas diferentes mientras crecía, y a menudo era educado en casa.

La Fundación De Wikileaks

Assange descubrió su pasión por las computadoras cuando era adolescente. A la edad de 16 años, obtuvo su primera computadora como un regalo de su madre. En poco tiempo, desarrolló un talento para *hackear* sistemas informáticos. Su entrada en 1991 en la terminal maestra de Nortel, una compañía de telecomunicaciones, le causó problemas. Assange fue acusado de más de 30 cargos de *hacking* en Australia, pero interrumpió sus actividades con sólo una multa por daños.

Assange continuó con su carrera como programador de computadoras y desarrollador de software. Con una mente inteligente, estudió matemáticas en la Universidad de Melbourne. Abandonó sin terminar la carrera, aunque más tarde afirmó que había dejado la universidad por razones morales; Assange cuestionó a otros

estudiantes que trabajaban en proyectos informáticos para los militares.

En 2006, Assange comenzó a trabajar en Wikileaks, un sitio web destinado a recopilar y compartir información confidencial a escala internacional. El sitio se lanzó oficialmente en 2007 y fue trabajado fuera de Suecia en ese entonces debido a las fuertes leyes del país que protegían el anonimato de una persona. Más tarde ese año, Wikileaks publicó un manual militar estadounidense que proporcionaba información detallada sobre el centro de detención de Guantánamo. En septiembre de 2008 Wikileaks también compartió correos electrónicos que recibió de una fuente anónima de la entonces candidata presidencial Sarah Palin.

Wikileaks ¿Cuál Es La Situación Actual En 2017?

La asombrosa transformación de Julian Assange hasta hoy es increíble. Las opiniones del fundador de WikiLeaks han cambiado a medida que los partidarios estadounidenses van proyectando sus propias prioridades sobre él. No es tan inusual que una figura pública cambie de ser considerado un héroe a un villano. Sin embargo, ¿que cambie de la villanía al heroísmo? Ese es un camino más difícil de recorrer.

Hace seis años, cuando WikiLeaks estalló públicamente con su liberación masiva de documentos estadounidenses, Donald Trump estaba desconcertado. “Creo que es una vergüenza, creo que debería haber pena de muerte o algo así”, dijo Trump en un intercambio recientemente desenterrado por CNN.[xvii]

“¿Por qué Obama no puede hacer algo con WikiLeaks?”[xviii] Sarah Palin comparó WikiLeaks con la revista Inspire de Al Qaeda y llamó a Assange “un agente anti-estadounidense con sangre en sus manos”.

Pero Assange ganó algunos admiradores de la izquierda estadounidense; personas que aplaudieron su voluntad de decir la verdad sobre el poder; por ejemplo, al exponer la brutalidad de la guerra de Irak, que se mostró como un conflicto innecesario lanzado por la administración Bush.

El presidente Donald Trump prometió una revelación sobre los *hackeos* en 2017,

y ese momento llegó y se fue sin ninguna noticia, aunque en el programa de Hannity, Assange repitió lo que dijo antes: que Rusia no era la fuente de WikiLeaks. Sin embargo, Trump publicó un *tweet* agradeciendo la entrevista, sólo para criticar al día siguiente que "a los medios de comunicación deshonestos les gusta decir que estoy de acuerdo con Julian Assange – están muy equivocados. Simplemente declaro lo que dice. Es para que el pueblo tome una decisión en cuanto a la verdad", como si fuera un simple "agregador" de noticias, en vez de que el presidente electo de los Estados Unidos citara con la aprobación de Assange.

Assange, en los últimos tiempos, dijo que su organización compartirá información con empresas de tecnología sobre las vulnerabilidades del producto de los datos de la CIA: "Vault 7".

WikiLeaks les permitirá a las empresas de tecnología acceder a información mucho más detallada sobre las técnicas de *hackeo* de la CIA para que se puedan "desarrollar arreglos" antes de que la información sea ampliamente publicada.

Dos días después de que WikiLeaks publicara miles de documentos, Assange habló dos días después de que reveló herramientas de *hackeo* que la CIA desarrolló para convertirlas en servidores, teléfonos inteligentes, computadoras y televisores. La conferencia de prensa tuvo lugar en la Embajada de Ecuador en Londres, donde Assange se ha escondido desde que solicitó asilo en 2012.

"La Agencia Central de Inteligencia (CIA) perdió el control de todo su arsenal de armas cibernéticas", dijo Assange. "Este es un acto histórico de la devastadora incompetencia de haber creado tal arsenal y almacenado todo en un solo lugar y no haberlo asegurado".

Assange dijo que algunas empresas de tecnología han estado buscando más detalles sobre las herramientas de la CIA. Afirmó también que WikiLeaks no ha publicado los detalles porque no quiere que "los periodistas y personas del mundo, nuestras fuentes, sean *hackeados* usando estas armas". La mejor manera de evitar eso, dijo, es darle acceso a empresas como Apple, Google y Samsung.

¿Qué Es Vault 7?

El martes 7 de marzo de 2017, WikiLeaks comenzó su nueva serie de filtraciones de la Agencia Central de Inteligencia de Estados Unidos. El nombre en clave "Vault 7" de WikiLeaks, es la mayor publicación de documentos confidenciales de la agencia.

La primera parte completa de la serie, "Year Zero", incluye 8.761 documentos y archivos de una red aislada y de alta seguridad ubicada dentro del Centro de Ciberesferencia de la CIA en Langley, Virgina. Es la continuación de una revelación inicial de la CIA el mes pasado, dirigida a los partidos políticos franceses y a los candidatos en la víspera de las elecciones presidenciales de 2012.

Recientemente, la CIA perdió el control de la mayoría de su arsenal de *hackers*, incluyendo malware, virus, troyanos, *exploits* de "día cero" armados, sistemas de control remoto de malware y documentación asociada. Esta colección extraordinaria, que asciende a más de varios cientos de millones de líneas de código, le da a su poseedor toda la capacidad de *hackear* a la CIA. El archivo parece haber sido distribuido entre antiguos *hackers* y contratistas del gobierno estadounidense de una manera no autorizada, uno de los cuales le ha proporcionado partes del archivo a WikiLeaks.

"Year Zero" presenta el alcance y la dirección del programa global de piratería de la CIA, su arsenal de malware y decenas de *exploits* armados de "día cero" contra una amplia gama de productos de compañías estadounidenses y europeas, incluyendo el iPhone de Apple, e incluso los televisores Samsung, que funcionarían como micrófonos encubiertos.

Desde el 2001, la CIA ha ganado preeminencia política y presupuestaria sobre la Agencia Nacional de Seguridad de los Estados Unidos (NSA). La CIA se encontró construyendo no sólo su infame flota de aviones no tripulados, sino un tipo muy diferente de fuerza encubierta, que abarca todo el mundo: su propio equipo de *hackers*. La división de piratería de la agencia se liberó de tener que revelar sus operaciones –a menudo polémicas– a la NSA (su principal rival burocrático) con el fin de aprovechar las capacidades de *hackeo* de la NSA.

A finales de 2016, la división de piratería de la CIA que forma parte del Centro para la Inteligencia Cibernética (CCI) de la agencia tenía más de 5000 usuarios registrados y había producido más de mil sistemas de *hackeo*, troyanos, virus y otros programas maliciosos "armados". Tal es la escala del compromiso de la CIA, que para el año 2016 sus hackers habían utilizado más código que el utilizado para ejecutar Facebook. La CIA había creado, en efecto, su "propia NSA" con menos responsabilidad y sin responder públicamente a la cuestión de si tal gasto presupuestario masivo para duplicar las capacidades de una agencia rival es justificable.

EL IMPACTO DE EDWARD SNOWDEN

Genio de la computación. Estratega cibernético. Activista. Campeón de la privacidad de los datos y la libertad en Internet. Patriota autoproclamado. Se busca en los Estados Unidos por espionaje: su nombre es Edward Snowden.

Primeros Años

Edward Joseph Snowden nació en 1983 en Elizabeth City, Carolina del Norte, en una familia en la cual todos habían trabajado para el gobierno federal en cierta forma. En el décimo grado, Snowden dejó de asistir a la escuela secundaria cuando se le diagnosticó con mononucleosis.

En lugar de volver a la escuela para terminarla, comenzó a tomar clases en el colegio comunitario local y se dedicó a las computadoras, la tecnología, Internet y la cultura del anime japonés. En 2004, se unió a la Reserva del Ejército de los Estados Unidos, pero pronto fue dado de baja después de quebrarse las dos piernas durante cinco meses en entrenamiento de fuerzas especiales.

La carrera de Snowden como especialista en seguridad comenzó en 2005, cuando trabajó como guardia de seguridad en el Centro de Estudios Avanzados de la Universidad de Maryland. En 2006, fue contratado por la CIA en Langley, Virginia.[xix] Un año más tarde, la CIA lo envió a Geneva para mantener la seguridad de la red informática.

En 2009, renunció a la CIA para trabajar como contratista privado: primero para Dell, y luego para Booz Allen Hamilton. Como contratista, Snowden trabajó en Tokio, Maryland, y finalmente en Hawái, donde comenzó el trabajo que lo convertiría en una de las figuras más controversiales de Estados Unidos.

Mientras trabajaba en la oficina de la NSA en Hawái en 2013, Snowden comenzó a preocuparse cada vez más por cómo la NSA estaba espiando a los ciudadanos comunes a través de sus datos de teléfono e Internet. Comenzó a compilar un dossier lleno de información sobre las prácticas de vigilancia masiva de la NSA. Luego se puso en contacto con la documentalista Laura Poitras, así como con los periodistas Glenn

Greenwald, Ewen MacAskill y Barton Gellman, pidiéndoles que vieran los documentos que había recogido.

En mayo de 2013, Snowden les informó a sus jefes que necesitaba un permiso médico para hacerle frente a la epilepsia que le había sido diagnosticada recientemente. El 20 de mayo de 2013, Snowden voló a Hong Kong y se preparó para lo que estaba por venir.

El 5 de junio de 2013, *The Guardian* filtró documentos que demostraban que Verizon estaba compartiendo todos sus datos de usuario con la NSA. Al día siguiente, *The Guardian* y *The Washington Times* publicaron la historia de PRISM, un programa de vigilancia de la NSA que le permite a la NSA recopilar datos de Internet de sus ciudadanos a través de su actividad en línea sobre productos y aplicaciones de Microsoft, Yahoo, Google y Apple, solo para mencionar unos ejemplos.

David Drummond, el director jurídico de Google, expresó su enojo por dichas revelaciones. Dijo que Google estaba preocupado por la posibilidad de otros husmeen información de sus usuarios y que la empresa ha extendido el cifrado en más y más plataformas de servicios de Google y sus enlaces. Drummond declaró que no proporcionó ningún acceso gubernamental a sus sistemas y que está indignado en base a los esfuerzos del gobierno de Estados Unidos para interceptar datos desde las redes privadas de Google.[xx]

Yahoo declaró que tienen controles estrictos para la protección de sus centros de seguridad y datos y que no le han permitido el acceso a estos centros de datos a la NSA ni a cualquier otra agencia gubernamental.

Éstas fueron sólo las primeras de una serie de filtraciones incriminatorias de los medios de comunicación mundiales que revelaron los numerosos programas de vigilancia masiva no sólo de la NSA, sino también de sus socios globales.

Repercusiones

El 9 de junio de 2013, Snowden reveló su identidad a través de *The Guardian*, afirmando: "No tengo intención de ocultar quién soy porque sé que no he hecho nada malo".[xxi]

Varios días más tarde, los fiscales federales estadounidenses acusaron a Snowden de robo de propiedad del gobierno, además de dos cargos por violar la Ley de Espionaje de los Estados Unidos: había comunicado sobre información de defensa nacional de forma no autorizada y sobre inteligencia secreta con una persona no autorizada de manera voluntaria.

Snowden permaneció en Hong Kong durante un mes, hasta que, con la ayuda de WikiLeaks, se dispuso a huir a Ecuador por medio de Rusia y Cuba. Cuando su vuelo llegó a Rusia, sin embargo, los funcionarios estadounidenses revocaron su pasaporte, lo que le impidió continuar su viaje. Snowden ha permanecido desde entonces en Rusia, donde se le concedió inicialmente asilo temporal, y luego, en agosto de 2014, un permiso de residencia de tres años. Él vive allí actualmente.

Los Efectos De Snowden En Los Estados Unidos Y La Política

Aunque el expresidente de los Estados Unidos Barack Obama criticó los métodos de Snowden, en agosto de 2013 anunció la creación de un panel independiente para examinar las prácticas de vigilancia del gobierno de los Estados Unidos. Las conclusiones de ese grupo, publicadas en diciembre de 2013, recomendaban que se suspendiera la recopilación en masa de registros telefónicos y se aconsejaba una mayor supervisión de programas sensibles, como los enfocados a dirigentes extranjeros amigos. Obama actuó sobre varias de estas sugerencias y recomendó la revisión de otros por parte del Congreso, pero el papel de la NSA y sus esfuerzos de recopilación de datos seguían siendo un punto de discusión entre la comunidad de inteligencia y los defensores de la privacidad. En abril de 2014, *The Guardian US* y *The Washington Post* recibieron el Premio Puliere por el servicio público de sus funciones en informar sobre las filtraciones de la NSA. Snowden caracterizó el premio como una "reivindicación" de sus esfuerzos

para poner en evidencia los programas secretos de vigilancia.

Después de que Edward Snowden se identificara como la fuente de *The Guardian* para los documentos filtrados secretos sobre la NSA y sus programas generales de vigilancia, la reacción del público fue mixta. Algunos aclamaron a Snowden como un activista y un héroe, mientras que otros lo consideraban un traidor.

¿En Dónde Se Encuentra Snowden Actualmente Y Qué Pasará?

En agosto de 2014, cuando el permiso de residencia temporal de Snowden expiró, el gobierno ruso le otorgó un permiso de residencia de tres años (efectivo el 1 de agosto), que le permitiría salir del país por hasta tres meses. También se le concedió la oportunidad de solicitar una prórroga de ese permiso y, después de cinco años de residencia, solicitar la ciudadanía rusa si así lo decidiera.

Las filtraciones influyeron directamente en las relaciones internacionales de EE.UU. de una manera negativa. Por ejemplo, Brasil canceló una visita de Estado y Ecuador renunció a los beneficios comerciales de EE.UU. Las filtraciones tuvieron un impacto financiero en algunas de las masivas empresas de tecnología de las comunicaciones con sede en Estados Unidos; Especialmente sobre aquellos que se especializaban en computación basada en la nube. Muchas personas, empresas y naciones se vieron afectadas por las filtraciones. Algunos proveedores de correo electrónico tuvieron que cerrar debido a la NSA y otras presiones del gobierno para revelar sus claves secretas.

La estimación actual es que los EEUU perderán entre $ 25 mil millones a $ 35 mil millones en la nube, lo cual computaba ingresos basados en las filtraciones de Snowden. La confianza en los profesionales de seguridad con sede en EE.UU. también se degradó después de que se reveló que la NSA había presionado por tener estándares de seguridad defectuosos. Esto afectará al estado y los profesionales de seguridad con sede en Estados Unidos en el futuro. Las consecuencias de estas revelaciones incluyen tensas relaciones extranjeras y el conocimiento de que existen programas de vigilancia masiva.

ESPIONAJE CIBERNÉTICO CHINO

Aunque la población de China está activa en el ciberespacio y tiene su propio comando cibernético ofensivo, el uso real de esto en ataques cibernéticos es muy mínimo y exhibe las dinámicas típicas de las interacciones de espionaje en lugar de una guerra cibernética corriente. En respuesta a los artículos negativos sobre el Primer Ministro de China, Wen Jiabao, lanzó una serie de ataques de denegación de servicio y ataques de fraude electrónico (*phishing*) contra el *New York Times* y el *Washington Post*. Todas las computadoras, las contraseñas y cuentas de correo electrónico "de los empleados del *New York Times* fueron infiltradas". El medio de comunicación había sido víctima de estos ataques durante al menos cuatro meses hasta que los expertos en seguridad pudieron finalmente cerrar estos intentos de fraude electrónico desde su comienzo.

Es interesante mencionar que al localizar las fuentes de los ataques procedentes de China, se encontró que los mismos habían sido obra de una operación del gobierno chino conocido como Ejército de Liberación del Pueblo Chino: una entidad que ha estado preocupando a muchas redes gubernamentales y privadas en los EE.UU. por años.[xxii] Aunque sean preocupantes, estos ataques no llegan al nivel de la exageración de la mayoría de los pronosticadores. En lugar de destruir las operaciones de los medios de comunicación estadounidenses que solo han tratado de alterar, sancionar y robar información de la que se sienten que son los agresores originales.

El espionaje cibernético tiene la intención de tratar de equilibrar la situación contra un rival. El equilibrio no es ni pacífico ni beneficioso;[xxiii] pero sucede y muchas veces será el objetivo de los estados que son parte de una rivalidad. En cierto modo, la idea es lograr ganancias a través de medios no convencionales porque el estado rival no puede aspirar a alcanzar a sus competidores a través de tácticas convencionales. Esta puede ser la motivación para las numerosas campañas de espionaje cibernéticas y las operaciones lanzadas por China contra el gobierno de Estados Unidos y el sector privado estadounidense. China no puede igualar a los estadounidenses en términos de medios militares convencionales, pero parece tener una ventaja sobre los EE.UU. en el ciberespacio, y ha utilizado estas habilidades para disgusto de EE.UU.

Los chinos han estado infiltrando redes de América Latina y trabajando en el robo de información en el ciberespacio desde hace más de una década. La pregunta que se debe plantear es por qué los estadounidenses han dejado que China se salga con la suya durante tanto tiempo. Deben mejorar sus defensas cibernéticas o dejarle en claro a China que este tipo de actividad no será tolerado. Hasta el momento, nadie lo ha hecho. Algunas teorías de terrorismo sugieren que la táctica se puede utilizar para afectar los patrones de voto o ser un atajo para una revolución.[xxiv] En términos de espionaje cibernético, el objetivo sería entonces provocar reacciones internas a través del miedo a la amenaza cibernética.

El mayor ataque de espionaje cibernético tuvo lugar cuando China se infiltró en el Pentágono y el establecimiento militar de la India y robó documentos confidenciales. Otro incidente de espionaje de la misma gravedad fue el robo de China de planes sobre los aviones F-35 de Lockheed-Martin. Los efectos de estas infiltraciones aún no se han visto, ya que China no ha producido tecnología militar estadounidense ni india. China está utilizando sus habilidades en el ciberespacio para acosar a su más poderoso competidor en los Estados Unidos y la competencia regional en la India.

Si las redes son inseguras, si las personas siguen respondiendo a los intentos de engaño cibernético y carecen del sentido común básico necesario para todas las interacciones cibernéticas, siempre habrá víctimas de ciberataques. Los ataques sólo hacen que el ciclo interminable de operaciones cibernéticas siga teniendo lugar. Se espera que haya espionaje cibernético. La industria del espionaje es una de las profesiones más antiguas de este mundo y no va a desaparecer. Todos unidos usarán cualquier táctica que puedan con fines políticos. Sin embargo, a lo largo de la historia, el impacto del espionaje ha tenido éxitos relativamente menores o mayores que en general pueden atribuirse a errores por parte de la persona que ha sido el objetivo en vez de la habilidad del propio agresor.

Lista De Ataques Chinos

Estos son algunos de los ataques más dañinos contra el gobierno de los Estados Unidos en los últimos años que se considera que han sido patrocinados o respaldados por el gobierno chino:

1) Titan Rain

En 2004, un analista llamado Shawn Carpenter en Sandia National Laboratories identificó los orígenes de un gran equipo de espionaje cibernético patrocinado por el gobierno de la provincia de Guangdong en China. Los hackers, codificados por el FBI como "Titan Rain", robaron cantidades masivas de información de laboratorios militares, la NASA, el Banco Mundial y otros. En lugar de ser recompensado, Carpenter fue despedido e investigado después de revelar sus hallazgos al FBI, porque *hackear* computadoras extranjeras es ilegal bajo la ley de los Estados Unidos. Él realizó una demanda también más adelante y fue concedido más de $ 3 millones. El FBI rebautizó a Titan Rain y el nuevo nombre es de carácter confidencial. Se supone que el grupo sigue funcionando.

2) State Department's East Asia Bureau

En julio de 2006, el Departamento de Estado admitió que se había convertido en una víctima de la piratería informática después de que un funcionario en "Asia Oriental" hubiera abierto accidentalmente un correo electrónico que no debería tener. Los atacantes trabajaron entrando ilegalmente a las computadoras en las embajadas de los EEUU en toda la región y finalmente penetrando los sistemas en Washington.

3) Offices of Rep. Frank Wolf

Wolf ha sido uno de los legisladores más prominentes en temas de derechos humanos en China, por lo que no ha sido sorpresa cuando anunció que en agosto de 2006 sus computadoras estaban comprometidas y que sospechaba del gobierno chino. Wolf también informó que unos ataques similares habían comprometido los sistemas de varios otros congresistas y la oficina de la Comisión de Asuntos Exteriores de la Cámara.

4) Commerce Department

La Oficina de Industria y Seguridad del Departamento de Comercio tuvo que desechar todas sus computadoras en octubre de 2006, paralizando así la oficina durante más de un mes debido a ataques procedentes de China dirigidos a ellos. Este Departamento es donde se emiten licencias de exportación de artículos tecnológicos a países como China.

5) Naval War College

En diciembre de 2006, el Naval War College en Rhode Island tuvo que desconectar todos sus sistemas informáticos durante semanas después de un gran ataque cibernético. Un profesor de la escuela les dijo a sus estudiantes que los chinos habían derribado el sistema. El Naval War College es donde se desarrolla mucha estrategia militar contra China.

6) El Secretario de Comercio Carlos Gutiérrez y el apagón de 2003

Un artículo de la revista National reveló que se encontró software de espionaje destinado a robar datos personales de forma clandestina en los dispositivos del entonces Secretario de Comercio Carlos Gutiérrez y varios otros funcionarios, tras una misión comercial a China en diciembre de 2007. En ese mismo artículo, se relaciona este evento con el masivo apagón del noreste de 2003 hacia el PLA, pero algunos analistas cuestionan dicha conexión.

7) Campañas presidenciales de McCain y Obama

Tanto las campañas de los entonces senadores Barack Obama y John McCain fueron totalmente invadidas por espías cibernéticos en agosto de 2008. El Servicio Secreto obligó a todo el personal de alto nivel de la campaña a reemplazar sus *Blackberries* y dispositivos portátiles. Los *hackers* buscaban datos como una forma de predecir las posiciones del futuro ganador. Los altos funcionarios de campaña han reconocido que el gobierno chino se puso en contacto con una campaña y utilizó la información que sólo se podía obtener del robo.

8) Office of Sen. Bill Nelson, D-FL

En una audiencia de marzo de 2009, Nelson reveló que las computadoras de su oficina habían sido *hackeadas* tres veces y su ayudante confirmó que los ataques tenían sus orígenes en China. Los objetivos de los ataques fueron el asesor de política exterior de Nelson, su director legislativo y un ex asesor de la NASA.

9) Ghostnet

En marzo de 2009, investigadores de Toronto concluyeron una investigación de 10 meses que reveló un enorme equipo de espionaje cibernético que llamaron Ghostnet, el cual había penetrado más de 1.200 sistemas en 103 países. Las víctimas fueron embajadas extranjeras, ONG, instituciones de prensa, ministerios de relaciones exteriores y organizaciones internacionales. Casi todas las organizaciones relacionadas con el Tíbet habían sido comprometidas, incluyendo las oficinas del Dalai Lama. Los ataques usaron malware chino y vinieron de Beijing.

10) Lockheed Martin's F-35 program

En abril de 2009, el Wall Street Journal reportó que se sospechaba que China estaba detrás de un robo importante de datos del programa del F-35 de Lockheed Martin, el avión más avanzado jamás diseñado. Las infiltraciones múltiples al programa F-35 aparentemente continuaron por años.

En muchos aspectos, el conflicto en Libia en 2011 reflejó los acontecimientos en Kosovo más de una docena de años antes. Una batalla cibernética se libraba dentro de Libia, entre Gadafi y sus propios ciudadanos. "El movimiento anti-Gaddafi había subido videos de ataques de aviones de combate del dictador contra su propio pueblo - no sólo para reunir a las multitudes en el país sino también para presionar a la comunidad internacional."[xxv] La lucha contra las guerras cibernéticas debe tener en cuenta la psicología del dominio y un actor político con experiencia encontrará una manera de robarle al guerrillero la legitimidad. Una estrategia militar eficaz siempre requiere más que solo medir los aspectos defensivos.

"El terrorismo cibernético también podría llegar a ser más atractivo, ya que el mundo real y el virtual se comienzan a superponer, con los automóviles, electrodomésticos y otros

dispositivos conectados a Internet.” - Dorothy Denning -

Aunque el FBI no puede confirmar que un grupo terrorista haya llevado a cabo un ataque cibernético contra los Estados Unidos, ha habido muchos incidentes cibernéticos de alto nivel desde el comienzo de la guerra global contra el terrorismo. Algunos de los ejemplos más ominosos incluyen la infección del gusano Slammer a una planta de energía nuclear de Ohio en 2004, y los ataques cibernéticos coordinados contra Estonia en 2007. El número extremadamente alto de ataques cibernéticos es un tema muy intenso.

LOS *HACKEOS* E INTERFERENCIAS POR PARTE DE RUSIA EN LOS ESTADOS UNIDOS

La injerencia de Rusia en las elecciones presidenciales de 2016 fue un ataque contra el pueblo estadounidense, amenazando la integridad y legitimidad del proceso democrático, así como el resultado de las elecciones. Sin embargo, la Evaluación de la Comunidad de Inteligencia sobre la actividad rusa en las elecciones descubrió que ésta era la expresión más reciente y agresiva hasta la fecha de un antiguo deseo ruso de sembrar el caos y la inestabilidad en los Estados Unidos. La intromisión de Rusia en las elecciones de 2016 debería ser una llamada de atención a todos los estadounidenses sobre las diversas formas en que la ciberactividad maligna rusa podría afectar a todos los aspectos de sus vidas.

La llamada campaña de guerra de información ordenada por el presidente ruso Vladimir Putin durante las elecciones forma parte de una estrategia de inteligencia rusa de múltiples facetas que "combina operaciones secretas de inteligencia –como la ciberactividad– con los esfuerzos manifiestos de las agencias gubernamentales rusas": los medios de comunicación financiados por el Estado, los intermediarios de terceros y los usuarios de medios sociales pagados –o también llamados "trolls"– para paralizar a sus adversarios. Las elecciones no fueron la primera vez que los "ciberactores" rusos han tenido éxito. Durante la última década, los grupos de hackers rusos –muchos de los cuales están respaldados por el gobierno– han desplegado con éxito una estrategia basada en tecnología para infiltrar, manipular y robar información confidencial en los sistemas gubernamentales, militares, bancarios y de comunicaciones de los Estados Unidos y Europa.

Estados Unidos sigue siendo seriamente vulnerable a una serie de amenazas cibernéticas de Rusia. Si no se controla la situación, las ciberoperaciones rusas seguirán probablemente siendo dirigidas a las instituciones, la infraestructura, los líderes y los ciudadanos estadounidenses. Según el ex director de la Agencia Nacional de Seguridad, Michael S. Rogers, los ataques de hackers, incluidos los de Rusia, le están costando a los Estados Unidos "cientos de miles de millones de dólares" y darán lugar a "problemáticas

verdaderamente significativas y posiblemente catastróficas si no se toman medidas".

Todos los estadounidenses deberían estar profundamente preocupados por los intentos de Rusia de interferir en las elecciones presidenciales de los Estados Unidos en 2016 y por el potencial de los actores rusos para interferir la vida diaria de otra nación. A continuación se muestra una muestra de las formas en las cuales grupos e individuos rusos ya han intentado tomar como objetivo a una variedad de instituciones estadounidenses y europeas, desde bancos y datos personales, hasta entidades gubernamentales.

Bancos Y Finanzas

Los estadounidenses confían en los bancos y las instituciones financieras para proteger sus ahorros universitarios, sus cuentas de jubilación y otros medios de subsistencia. Sin embargo, los bancos e instituciones financieras estadounidenses han sido objeto de numerosos ataques por parte de grupos de hackers de origen ruso durante la última década, y así mostrando importantes vulnerabilidades en la seguridad financiera de los estadounidenses de todos los días.

En mayo de 2015, hackers rusos usaron malware para atacar a varios bancos estadounidenses e internacionales, incluyendo Bank of América y TD Bank, y robaron hasta 900 millones de dólares en un solo año. Todavía se desconoce la medida en que estos maliciosos programas rusos se infiltraron en otras instituciones financieras.

Los mismos hackers rusos también construyeron el mejor sistema jamás descubierto que les permitiera robar información de acceso y credenciales de contraseña de decenas de millones de cuentas en línea, incluyendo cuentas bancarias, lo cual les ha costado a las víctimas cientos de millones de dólares.

Información Personal

Han surgido varios esquemas de *hackeo* que tienen como objetivo a dispositivos personales, incluyendo teléfonos y computadoras, en un intento por obtener datos

confidenciales y de seguridad de los usuarios. Los ejemplos a continuación ilustran las formas en que los hackers rusos explotan programas que la mayoría de los estadounidenses usan todos los días en un intento por acceder a sus archivos personales.

En febrero de 2015, los investigadores descubrieron que había *hackers* rusos que habían desarrollado malware para iOS diseñado para acceder a los datos personales de los usuarios en dispositivos con software iOS7, el cual operaba en ese momento en un cuarto de los dispositivos iOS. Apple vendió 130 millones de dispositivos iOS en 2014. Esto significa que es posible que millones de estos dispositivos podrían aún estar afectados. Además de poder iniciar grabaciones de audio en segundo plano sin el conocimiento de un usuario, este malware puede recopilar mensajes de texto, listas de contactos, imágenes, datos de localización geográfica, listas de aplicaciones instaladas, listas de procesos y el estado WiFi de un usuario.

En octubre de 2015 y 2016, los mismos hackers rusos también explotaron varias vulnerabilidades de "día cero" o defectos de software previamente desconocidos en Adobe Systems y Microsoft Windows en un intento por acceder a los datos personales de los usuarios, que luego utilizó para dirigirse a otras personas. Estos ataques se produjeron con la intención de acceder y controlar computadoras individuales de forma remota.

Gobierno Y Militares

Los grupos de hackers rusos han logrado tener acceso a una variedad de servidores gubernamentales y de empleados. Además de las amenazas a la seguridad nacional que plantean estos ataques, los miles de millones de dólares que el gobierno gasta para recuperarse de los ataques y proteger la información, particularmente la información confidencial, sale de los bolsillos de los contribuyentes estadounidenses.

Los ejemplos a continuación ilustran los peligros que plantea la campaña rusa de hackers:

En 2015, un grupo de hackers rusos tuvo como objetivo de ataque a los servidores de computadoras del Departamento de Estado de S., la Casa Blanca, y los Jefes de Estado Mayor Conjuntos. Como parte de los ataques contra el Departamento de Estado y la Casa

Blanca, los hackers obtuvieron acceso a información altamente confidencial, incluyendo detalles sobre el calendario del presidente Barack Obama. Además, en los ataques al sistema de correo electrónico utilizado por los Jefes de Estado Mayor Conjunto, los hackers pudieron tomar el control del sistema en una hora, lo que les permitió acceder a las credenciales informáticas del entonces Presidente del Jefe Conjunto Martin Dempsey, así como cientos de otros altos oficiales. El Pentágono sólo pudo detener el ataque al quitar toda la red. El objetivo del ataque no era espiar sino "causar daño y obligar al Pentágono a reemplazar tanto el hardware como el software, lo cual tomó alrededor de dos semanas".

Influencia Política

El gobierno ruso ha utilizado diferentes formas de campañas cibernéticas en un intento de influenciar no sólo las elecciones estadounidenses, sino también de provocar inestabilidad al crear sentimientos de miedo y desconfianza hacia las instituciones de gobierno estadounidenses. Los *hackers* rusos y los *trolls* han utilizado esquemas muy exitosos de piratería, propaganda y fugas de información oportunas para lograr su agenda, como se evidencia a continuación.

Elecciones Y Cortes Posteriores A Las Elecciones

En el verano de 2015, dos grupos de hackers rusos accedieron al Comité Nacional Demócrata (DNC) y expusieron información privada enviada a través de servidores DNC. La Oficina del Director de Inteligencia Nacional (DNI) ha confirmado que cree que estos ataques fueron diseñados para influir en el resultado de las elecciones de 2016. Los hackers luego filtraron información confidencial, que fue muchas veces malinterpretada por el público, en un intento de desacreditar a la candidata demócrata a la presidencia, Hillary Clinton, y ayudar al entonces candidato republicano a la presidencia, Donald Trump.

En marzo o abril de 2016, los *hackers* rusos también *hackearon* el Comité Democrático de la Campaña del Congreso (CCCC). Como resultado, los Demócratas cayeron presos de una operación de influencia rusa después de que los hackers publicaran

por primera vez la información personal de los legisladores y documentos internos del partido, incluyendo las evaluaciones de los candidatos.

A lo largo de 2016, unos hackers rusos, que la Oficina Federal de Investigación (FBI) creía que estaban trabajando para la inteligencia rusa, se infiltraron los sistemas estatales del registro de votantes en Illinois, Arizona y Florida. En Illinois, los funcionarios afirmaron que los datos de alrededor de 90.000 personas pueden haber sido afectados. En Arizona, los funcionarios estatales indicaron que los hackers no podían acceder a los datos en sus sistemas, aunque los funcionarios indicaron que los investigadores estaban trabajando sobre el supuesto de que los *hackers* hayan podido acceder a los datos. Y en Florida, los investigadores federales también indicaron que los datos personales de los votantes de la Florida podrían haber sido expuestos.

Después del éxito electoral de Donald Trump, los hackers rusos comenzaron a atacar a individuos asociados con grupos progresistas activistas y organizaciones no gubernamentales u ONGs en los Estados Unidos. La empresa de seguridad Voxity, la cual investigó los ataques, dijo que es probable que los atacantes estuvieran buscando un acceso a largo plazo que les diera información confidencial sobre la formulación de políticas de Estados Unidos. El informe de la Oficina del Director de la Inteligencia Nacional sugiere que la seguridad nacional y las organizaciones de política exterior son el objetivo principal y sostiene que la campaña de *hackeo* podría proporcionar inteligencia que permita la futura manipulación electoral.

Ataques Internacionales

Además de algunos de los ataques contra las instituciones estadounidenses aquí resaltados, Rusia ha llevado a cabo muchos más ataques y campañas de influencia en todo el mundo, a menudo con un efecto devastador, como se pone en evidencia en los siguientes ejemplos.

En 2007, después de la decisión de Estonia de retirar y trasladar una estatua conmemorativa de la Segunda Guerra Mundial, los *hackers* desataron una ola de tres semanas de ataques cibernéticos contra Estonia, desactivando los sitios web de los

ministerios gubernamentales, partidos políticos, periódicos, bancos y empresas. Los expertos en seguridad cibernética y funcionarios estonios identificaron que muchas de las direcciones de Internet para los ataques eran rusas, y algunas eran de instituciones estatales rusas.

En 2008, en la víspera de la invasión terrestre, marítima y aérea rusa de Georgia, los piratas informáticos rusos –quienes se cree que son respaldados por el Kremlin– llevaron a cabo ataques coordinados contra la red de Internet de Georgia, incluyendo ataques al sitio web del presidente, así también como la comunicación, las finanzas y otros sitios gubernamentales. Estos ataques bloquearon con eficacia las comunicaciones dentro del país, impidiendo que los ciudadanos accedieran a sitios web para obtener información e instrucciones mientras que el conflicto estaba en marcha.

En 2014, Rusia usó tácticas similares en Ucrania, apareando su invasión de Crimea con ciberasaltos a más de 100 organizaciones gubernamentales e industriales en Polonia y Ucrania, además de ataques contra la Comisión Europea y el Parlamento. Desde la anexión de Crimea, Rusia ha seguido lanzando ciberataques contra Ucrania, apuntando a las comunicaciones militares, los bancos, los ferrocarriles, la industria minera, y la red eléctrica. La firma de ciberseguridad LookingGlass ha apodado a estos ataques Operación Armagedón y ha encontrado una correlación entre los ataques de la Operación Armagedón y la actividad militar rusa en Ucrania.

Desafortunadamente, los europeos han sido durante mucho tiempo los blancos de las campañas rusas de *hackeo* y desinformación. Además de los informes anteriores, existe la preocupación de que los rusos estaban difundiendo la desinformación durante el reciente voto Brexit en el Reino Unido, además de trabajar en contra del gobierno del ex primer ministro italiano Matteo Renzi durante el reciente referéndum sobre la constitución italiana. Hay muchos otros ejemplos en los cuales los rusos intentan cambiar el rumbo de la política en Europa. Lo que es particularmente alarmante sobre estas tácticas cibernéticas rusas es el hecho de que Rusia es “el único país hasta la fecha que ha combinado ciberguerra con asaltos por cañones y tanques convencionales”. Además, como han tenido cierto éxito utilizando estas tácticas, no es probable que Rusia deje de

usarlas en un futuro cercano.

Teniendo en cuenta los ejemplos proporcionados aquí del *hackeo* ruso, tanto en los Estados Unidos y en el extranjero, es evidente que debe haber un enfoque más completo para comprender, prevenir y responder a los ciberataques en todos los sectores. Estados Unidos y Europa son claramente vulnerables a ataques cibernéticos, y como el mundo sigue dependiendo más de los sistemas electrónicos, dichas vulnerabilidades sólo seguirán creciendo.

Con el fin de comprender mejor los ataques específicos descritos aquí, debe haber una investigación más profunda de las habilidades cibernéticas de Rusia, específicamente con respecto a su participación en las elecciones presidenciales de 2016 en los Estados Unidos. Para prevenir y responder mejor a los ataques cibernéticos, las agencias gubernamentales estadounidenses, así como otras industrias como los bancos e instituciones financieras, deben desarrollar estrategias integrales para identificar, prevenir y responder a ataques cibernéticos. También es importante recordar que estos ataques no son sólo contra las instituciones; también se llevan a cabo contra ciudadanos comunes. Incluso cuando estos ataques afectan directamente al gobierno, hay un costo para todos los estadounidenses. El *hackeo* ruso es una amenaza para la democracia estadounidense y los derechos de privacidad. No puede quedar sin solucionarse.

LA VULNERABILIDAD DE ESTADOS UNIDOS FRENTE AL ATAQUE CIBERNÉTICO DE COREA DEL NORTE

Mientras que Corea del Norte se enfurece al lanzar ataques con misiles contra Estados Unidos y sus aliados, los expertos advierten que la acción agresiva de Corea del Norte es más probable que provenga del ciberespacio.

Mientras que Kim Jong-Un ha luchado para desarrollar un arsenal tradicional para competir frente a sus enemigos, ya que sanciones internacionales han bloqueado a Pyongyang del sistema financiero mundial, las fuerzas armadas de Corea del Norte ha cultivado un grupo cada vez más sofisticado de *hackers* capaces de atacar objetivos cibernéticos respaldados por Occidente.

John Carlin, ex asistente del fiscal general de seguridad nacional, dijo que el gobierno no ha hecho lo suficiente para proteger la infraestructura central del país frente a Corea del Norte y otras amenazas cibernéticas.

"Todavía somos vulnerables", dice Carlin. "La amenaza en este camino supera a nuestras defensas actuales. Tiene que ser una prioridad de esta administración y este Congreso arreglarlo... Usted ha visto todos los ataques que han ocurrido. No es un caso hipotético".

Cito dos ejemplos recientes de ataques cibernéticos en Estados Unidos que se sospecha que han sido llevados a cabo por Corea del Norte. En 2014, un grupo que se autodenominaba Guardianes de la Paz *hackeó* Sony Pictures Entertainment, retrasando el lanzamiento de *The Interview*, una comedia protagonizada por Seth Rogen y James Franco que describía un intento de asesinato ficticio contra Kim Jong-Un. En los días siguientes, los *hackers* publicaron información propietaria y correos electrónicos vergonzosos que le costaron millones de dólares al estudio.

En 2016, los piratas informáticos robaron $ 81 millones de fondos de Bangladesh del Banco de la Reserva Federal de Nueva York a través de la red SWIFT, un servicio de mensajería financiera utilizado por miles de bancos alrededor del mundo. Según *The New York Times*, funcionarios estadounidenses están investigando si Corea del Norte estaba

involucrado porque los hackers usaron un código que también apareció en el ataque cibernético contra Sony.

El gobierno norcoreano ha negado cualquier acusación sobre el *hackeo*, pero la firma rusa de seguridad cibernética Kaspersky publicó un informe a principios de este mes vinculando al grupo *hacker* "Lazarus" a los ataques de Sony y SWIFT y rastreando a "Lazarus" de vuelta a una dirección IP en Corea del Norte.

En enero, el presidente Donald Trump se comprometió a contratar a un equipo para crear un plan para abordar las vulnerabilidades de ciberseguridad en los Estados Unidos dentro de los 90 días de su toma de cargo, pero Carlin señaló que el plazo ha llegado sin un plan ni un equipo.

"No puedo pensar en un problema más urgente que afronte esta administración, pero aún no hemos escuchado cuál será su estrategia", dijo Carlin. "Espero que llegue a lo más alto de su agenda".

Un funcionario de alto rango de la administración se negó a comentar cuándo se haría público el plan de seguridad cibernética del presidente, pero dijo que, a pesar de los informes opuestos, ya existe un equipo de ciberseguridad "completamente funcional" liderado por el coordinador de ciberseguridad del Consejo de Seguridad Nacional de la Casa Blanca, Robert Joyce. Los esfuerzos relacionados a Jared Kushner y Rudy Giuliani también están en marcha, dijo el funcionario, pero es Joyce quien establecerá las prioridades de seguridad cibernética.

El funcionario reconoció, sin embargo, que el gobierno tiene "un largo camino por recorrer" cuando se trata de ciberseguridad, citando vulnerabilidades en algunas redes federales. "Hay más de 200 departamentos y agencias y no todos están preparados para trabajar la ciberseguridad", dijo el funcionario. Dichas vulnerabilidades podrían ser explotadas por *hackers* extranjeros. Una brigada cibernética es más fácil de desarrollar que una fuerza de combate tradicional, incluso para un país con una infraestructura de red extremadamente pobre. Según se conoce públicamente, Corea del Norte realizó su primera conexión a Internet en 2010, y este acceso sigue estando estrictamente

controlado por el gobierno y limitado a sólo un grupo seleccionado de ciudadanos. Como resultado, el uso de Internet en Corea del Norte es uno de los más bajos del mundo, con sólo 14.000 usuarios de Internet en el país en 2016, según la Unión Internacional de Telecomunicaciones (UIT) de las Naciones Unidas.

Un extenso informe sobre las capacidades cibernéticas de Corea del Norte, compilado en 2014 por la empresa de tecnología HP, determinó que la mala conectividad de Corea del Norte no ha impedido que su gobierno construya un equipo de "guerreros cibernéticos". Algunos opositores afirman que el régimen gubernamental identifica a los estudiantes prometedores en matemática en las escuelas, envía potenciales alumnos a academias de élite para un riguroso entrenamiento en informática y eventualmente recluta estudiantes exitosos en una rama de operaciones cibernéticas de los militares. Estos "guerreros cibernéticos", dice HP, son algunos de los únicos norcoreanos con acceso a Internet.

"Si se trata de una maniobra ofensiva, lo cibernético tiene mucho sentido para ellos", dijo Martyn Williams de 38 North, quien se especializa en seguir el tema de las capacidades tecnológicas de Corea del Norte. "Algunas de las cosas que se observan en los desfiles pueden asustar, pero no tienen los recursos para igualar el armamento de los Estados Unidos o Corea del Sur. Cuando se trata de recursos cibernéticos, es mucho más fácil convertirse en un oponente formidable, por lo que este es un campo de juego mucho más uniforme".

Se desconoce el tamaño exacto de esta fuerza que se distribuye entre varias unidades supervisadas por la Oficina General de Reconocimiento (RGB) dentro del Departamento de Estado Mayor del Ejército del Pueblo Coreano. Sin embargo, un análisis del gobierno surcoreano realizado en 2014 estimó que dicha fuerza podría incluir cerca de 6.000 soldados, muchos de los cuales operan en países extranjeros para ocultar su actividad. El informe de HP señaló la ubicación de un grupo, por ejemplo, llamado Unidad 121, el cual se cree que ha lanzado ataques contra "redes enemigas" tanto en Estados Unidos como en Corea del Sur desde China, no muy lejos de la frontera norcoreana.

John Bambenek, de Fidelis Cybersecurity, quien frecuentemente realiza consultas para agencias gubernamentales estadounidenses, dice que muchas instituciones estadounidenses, sobre todo los bancos, tampoco están preparadas para defenderse contra un servicio de inteligencia hostil.

"¿Serían capaces de comprometer a la CIA? No," dijo Bambenek. "Pero creo que sin duda podría suceder luego de un objetivo fácil".

Los robos cibernéticos de las instituciones financieras podrían poner en duda las preocupaciones de seguridad sobre Corea del Norte, planteando la cuestión de si Corea del Norte podría estar aplicando esos fondos presuntamente robados a su programa de misiles.

Anthony Ruggiero, un destacado especialista en Corea del Norte en la Fundación para la Defensa de la Democracia, expresa que estos presuntos ataques podrían ser parte de una nueva estrategia para eludir las sanciones internacionales diseñadas para paralizar el programa de misiles.

"Corea del Norte tiene una larga historia de actividades ilícitas para adquirir fondos para su programa de misiles nucleares, el cual consideran clave para la supervivencia del régimen", dijo Ruggiero. "A medida que se extienda más y tenga más éxito, podrían recurrir a más actividades ilícitas. Las iniciativas cibernéticas son unas de las opciones en su caja de herramientas".

UNA CONSECUENCIA DE LOS ATAQUES CIBERNÉTICOS A ESTADOS UNIDOS: MISILES NORCOREANOS

"Internet en Corea del Norte" es prácticamente un oxímoron. El acceso a Internet global en esta misteriosa nación está fuertemente restringido y está disponible solo para funcionarios gubernamentales selectos y otras élites. El resto de la nación tiene acceso a una red nacional cerrada llamada Kwangmyong, una intranet con información aprobada por el estado.

El régimen de Corea del Norte es efectivamente uno de los más agresivos del planeta en cuanto a su censura en línea. Además, al parecer, también funciona bastante bien para defenderse de ciberataques extranjeros, según un reporte reciente de Reuters.

Según Reuters, hace cinco años, Estados Unidos trató de sabotear el programa de armas nucleares de Corea del Norte con un virus informático. La campaña se basó en una variante de Stuxnet, el malware que inhabilitó las centrífugas iraníes, que –según lo reportado por *The Washington Post* y otros– fue un proyecto conjunto de los Estados Unidos e Israel. La idea era usar una versión del virus que se activara cuando se encontrase con la configuración en coreano, informó una fuente anónima a Reuters.

Pero la campaña flaqueó. Fue "bloqueada", informó Reuters, por el "secreto total de Corea del Norte, así como el aislamiento extremo de sus sistemas de comunicaciones".

Resulta que solo tener una infraestructura de Internet es una buena manera de evitar un "Pearl Harbor cibernético", según funcionarios de los EE.UU. han estado advirtiendo durante años.

Corea del Norte intentó disparar un misil recientemente, pero el mismo explotó en cuestión de segundos. Sucedió un día después del aniversario de la fundación del país. Aunque que el programa de misiles de Corea del Norte sea el más sombrío de la tierra, es posible que los guerreros cibernéticos de EE.UU. hayan sido la razón del fracaso del lanzamiento.

Un informe reciente del *New York Times* reveló una operación secreta para

descarrilar el programa de misiles nucleares de Corea del Norte durante al menos tres años. En síntesis, el informe le atribuye la alta tasa de fracaso de Corea del Norte con misiles de diseño ruso a la intromisión de Estados Unidos en el software y las redes de misiles del país.

Aunque la infraestructura de misiles de Corea del Norte carece de la competencia rusa, el misil de la era soviética en el que Corea del Norte basaba su misil presentaba un índice de fracaso del 13% y la versión norcoreana falló un gran 88% del tiempo.

Si bien el fracaso de los misiles recientes podría haberse debido a la falta de mano de obra, el Asesor Adjunto de Seguridad Nacional de EE.UU., K.T. McFarland, parecía dar lugar a la especulación sobre el espionaje, al informarle a Fox News: "no podemos hablar de inteligencia secreta, cosas que podrían haberse hecho, ni de operaciones encubiertas, así que realmente no tengo comentarios".

El vicepresidente Mike Pence visitó el lunes la zona desmilitarizada entre las Coreas, y afirmó que "todas las opciones están sobre la mesa para lograr los objetivos y asegurar la estabilidad de la gente de este país", y que "la era de la paciencia estratégica" con Corea del Norte "ha terminado".

Para los entendidos en el tema, la campaña contra Corea del Norte no ha sido una sorpresa. Ken Geers, un experto en seguridad cibernética de Comodo con experiencia en la Agencia de Seguridad Nacional, explicó que las operaciones cibernéticas como la de Corea del Norte eran lo esperado.

Mientras que para los EE.UU. *hackear* el programa de misiles de otro país pueda ser escandaloso para algunos, "dentro de los espacios de inteligencia militar, esto es lo que se hace", dijo Geers. "Si uno piensa que la guerra es posible con un estado dado, va a estar tratando de preparar el espacio de batalla para el conflicto. En la era de Internet, eso significa *hackear*".

Las redes internas de Corea del Norte están fuertemente aisladas y no están conectadas a Internet, lo que representa un desafío para los hackers en Estados Unidos. No obstante, Geers dijo que "absolutamente no es el caso", ya que *hackear* requiere computadoras

conectadas a Internet.

Un informe reciente en *The New Yorker* sobre la piratería rusa detalló un caso en el que Rusia obtuvo acceso a una red de ordenadores de la OTAN en 1996. Los operadores de la OTAN compraron las unidades de pulgar, las usaron en la red e igualmente los rusos entraron. “Es ahí donde la SIGINT (inteligencia de señales) o COMINT (inteligencia de comunicaciones) entra en colaboración con la HUMINT (inteligencia humana)”, dijo Geers. Describió el momento actual como la “edad de oro del espionaje”, ya que la guerra cibernética sigue siendo no letal, impagable y casi totalmente impune.

Sin embargo, un reciente lanzamiento de misiles de Corea del Norte sugiere que incluso un ciberataque prolongado y sofisticado no puede descarrilar completamente su programa de misiles nucleares.

“Imagina que eres el presidente, y Corea del Norte es un abusador de los derechos humanos y un exportador de tecnología peligrosa”, supuso Geers. “Los gobiernos responsables realmente necesitan pensar en maneras de manejar a Corea del Norte, y una de las opciones es el cambio de régimen”.

Además, según Geers, debido a la limitada cantidad de servidores y tan restringidos puntos de acceso a Internet en Corea del Norte, “si alguna vez llegara la ciberguerra entre Estados Unidos y Corea del Norte, sería una abrumadora victoria para Occidente”.

“Corea del Norte puede hacer atacar a Sony o a la Casa Blanca, pero eso sucede porque esa es la naturaleza del ciberespacio”, dijo Geers. “Pero si llegara la guerra, verías que el Comando Cibernético acabaría con la mayoría de los otros países con bastante rapidez”.

EVOLUCIÓN DE LAS RELACIONES INTERNACIONALES DE LOS ESTADOS UNIDOS DEBIDO A LOS ATAQUES CIBERNÉTICOS

Los Estados pueden utilizar la amenaza de un ataque cibernético para influir en el comportamiento de un Estado-nación opositor, casi de la misma forma en que la amenaza de las armas nucleares subyuga a otros estados. Algunos estiman que la amenaza cibernética es urgente e importante. El ex presidente estadounidense, Barack Obama, ha declarado que la "amenaza cibernética es uno de los más graves problemas de seguridad económica y nacional que enfrentamos como nación."[xxvi] Después de la investigación relacionada a extensos ataques cibernéticos, es evidente que tanto China como la política exterior de Estados Unidos se ven afectados.

Cuando China haga uso de un conflicto cibernético dirigido hacia los Estados Unidos, estos últimos responderán con la diplomacia y tratarán de mejorar las relaciones con el poder creciente. Estos resultados desafían la sabiduría convencional típica propuesta por los expertos y académicos que sugieren que las interacciones cibernéticas son una nueva y revolucionaria forma de llevar a cabo interacciones interestatales. Debido a la naturaleza de las interacciones internacionales entre los Estados y sus afiliados, hay una historia, origen y método para el análisis de estos eventos, los cuales se basan directamente en la naturaleza del conflicto cibernético entre competidores internacionales.

Es claro que el término "guerra cibernética" causa conmoción y describe un proceso que aún no ha sucedido. Las redes y conexiones correctamente señalan que la guerra cibernética no está ocurriendo, lo cual nos permite argumentar que los procesos en desarrollo en el ciberespacio son un poco diferentes a los de la guerra tradicional. Lo cibernético es una táctica, no una forma de guerra completa. Es una herramienta disponible en el arsenal de la diplomacia y las interacciones internacionales, al igual que otras formas de amenazas están en la caja de herramientas del arsenal del poder de un estado.

En 2011, el gobierno declaró que USS era un incidente cibernético similar a un acto de guerra, el cual se castiga por medios militares convencionales. Este es un paso

importante, ya que permite que la respuesta a un incidente malicioso no físico en el ciberespacio se realice de forma física, en movimiento. El conflicto se desplaza del ciberespacio a las formas convencionales. Las amenazas no físicas rara vez hemos visto que se convierten en la razón de amenazas físicas de respuesta.[xxvii] No se puede argumentar que las operaciones cibernéticas no estén causando un cambio en la forma en que se lleva a cabo la política exterior; nuestra opinión es que este cambio podría ser problemático a la luz de la evidencia.

La comprensión de otros usos anteriores y los actuales del poder cibernético y las reacciones a estas estrategias puede ayudar a explicar y predecir los usos y las futuras respuestas de las tácticas. Con un enfoque en operaciones cibernéticas ofensivas y la naturaleza exagerada de las amenazas cibernéticas míticas, parece que hemos dirigido la aplicación de la tecnología a la esfera política incorrectamente. En lugar de una revolución en los asuntos militares, las tácticas cibernéticas simplemente parecen haber reorientado el estado de las amenazas externas. Al centrarse en las amenazas externas y no a la reacción real a las acciones cibernéticas, como comunidad no somos capaces de proporcionar un análisis adecuado de la verdadera conducta de las interacciones de política exterior cibernéticas. La ciberseguridad es el marco para la defensa del Estado contra cualquier posible incidente cibernético malicioso que ingrese a sus fronteras y a las redes a través de canales digitales.

Las acciones cibernéticas son difíciles de realizar debido a que, por naturaleza, el arma es reproducible. Esto hace que sea poco probable que cualquier opción cibernética utilizada se dé a conocer públicamente, porque el arma estaría libre para cualquier persona que desee utilizarla. Debido a este factor, es muy probable que haya un retroceso con el mismo método utilizado al inicio. A esto se le añade el hecho de que las armas cibernéticas son costosas de desarrollar y para nada baratas o fáciles de usar como algunos parecen pensar. Estos tres factores, la reproducibilidad, el retraso, y la naturaleza costosa de las armas, hacen probable que los estados restrinjan el uso de opciones cibernéticas. Las operaciones cibernéticas suelen representar pruebas débiles para amenazar al enemigo y demostrar habilidades. Los Estados Unidos son capaces de mucho más en el ciberespacio; sin embargo, parecen estar conteniéndose de desencadenar sus

capacidades cibernéticas completamente. Las normas y los tabúes también refuerzan este proceso y son críticos porque las armas cibernéticas no son controlables y manejables. Las interacciones internacionales cibernéticas están determinadas por el tema que atrae a los estados en conflicto.

La mayoría de las interacciones rivales en el ciberespacio tendrán un contexto regional conectado a la cuestión de las consideraciones territoriales o los conflictos, ya que la mayoría de las rivalidades comienzan debido a preocupaciones territoriales. Un estado que sea centro de atención no puede permitirse el lujo de parecer débil y no responder a este tipo de acciones que tratan de hacer una demostración de la capacidad. Otras tácticas cibernéticas, como el espionaje y otros, son menos propensas a recibir reacciones, ya que se pueden ocultar y es poco probable que el estado objetivo busque reacciones intensificadas, dado el potencial de intensificación de lo cibernético.

Los incidentes cibernéticos son eventos individuales que se dirigen a un país en una cuestión de horas, días o semanas que se codifican fácilmente uno por semana. Los incidentes cibernéticos también están codificados de acuerdo a su método. Los métodos son las formas en que los iniciadores son capaces de acceder a las redes de sus rivales. El vandalismo es el proceso de inyección de código en un sitio web que desfigura ese sitio. La denegación de métodos de servicio es la inundación coordinada de sitios web o redes particulares mediante la activación de varios equipos controlados remotamente para derribar un blanco. Las intrusiones son métodos utilizados para acceder de forma remota y en silencio a una red y potencialmente robar información. Por último, las infiltraciones son métodos cibernéticos que pueden hacer el mayor daño potencial. Estos incluyen los virus, los gusanos, las bombas lógicas, y el registro de pulsaciones.[xxviii] Los incidentes cibernéticos son una manera de derribar al opositor usando "botnets" en lugar de balas.

Lo más interesante de los resultados de este análisis en grupo controlado son las respuestas estadísticamente significativas de los Estados Unidos después de que es víctima de un incidente cibernético. Con la excepción de China, Estados Unidos responde negativamente y coercitivamente a todos sus rivales si es la víctima del conflicto cibernético. Cuando Estados Unidos es víctima de conflictos cibernéticos procedentes de

China, esto evoca respuestas cooperativas hacia el régimen de política exterior de Estados Unidos. Debe tenerse en cuenta que éstas son reacciones públicas capturadas por las variables dependientes de los datos de los eventos. A puertas cerradas, por lo tanto, la reacción de Estados Unidos a las intrusiones por parte de China en sus redes seguras podría ser muy diferente. En cualquier caso, nuestro enfoque en los eventos públicos y los resultados parecen contrarios a la intuición, debido a todos los informes públicamente negativos de las empresas de seguridad cibernética sobre agresión china en el ciberespacio.

Los enemigos de los Estados Unidos también reaccionan negativamente a las incursiones estadounidenses en el ciberespacio. Siria, Corea del Norte e Irán, todos evocan respuestas de política exterior negativas y estadísticamente significativas cuando se infringen sus redes.

CONCLUSIÓN

La mayoría de los incidentes cibernéticos pueden ocurrir sin ninguna respuesta significativa por parte de la víctima. De hecho, los incidentes entre las grandes potencias como Estados Unidos y China en realidad resultan en relaciones positivas en vez de otras interacciones degenerativas. La razón de esto probablemente se deba a incidentes cibernéticos que caen por debajo del rango normal de las operaciones. Por lo general, estos métodos son silenciosos y están destinados a no alterar el delicado equilibrio de las relaciones entre estados rivales que compiten enfocados uno en el otro. Cuando China se infiltra en los Estados Unidos, estos últimos responden diplomáticamente sin más operaciones cibernéticas. El futuro podría ser diferente, pero por ahora, los poderes han aprendido a manejar las relaciones, incluso durante las operaciones cibernéticas constantes y perjudiciales. Los Estados Unidos se están restringiendo de reaccionar de manera negativa hacia China a fin de no empeorar el conflicto cibernético a niveles apocalípticos. Muchos expertos y académicos dicen que es inevitable.

En una sociedad conectada digitalmente, todo el mundo se ve y el estado puede entonces ser obligado a reaccionar. Lo bueno es que estas reacciones están a la altura del nivel de una guerra y esto es violencia pura y convencional. Si no se manejan estos tipos de incidentes cibernéticos en el futuro, los mismos podrían conducir a nuevos incidentes cibernéticos de contraataque devastadores. Por ahora, los estados parecen estar dispuestos a responder con protestas y luego poner la otra mejilla. Los únicos incidentes cibernéticos que constantemente evocan respuestas de política exterior negativas son los que tratan de cambiar el comportamiento del Estado.

Las políticas exteriores son mucho más positivas en cuanto a la posibilidad de la cooperación y la paz cibernéticas que lo que cree la mayoría de los especialistas. La mayoría de los estados parecen tener restricciones en sus acciones en el ciberespacio. Estos hallazgos son un buen augurio para el futuro de las interacciones internacionales cibernéticas y cuestionan la naturaleza del cambio de las doctrinas en las organizaciones militares.

[i] We're headed for a 'cyber Pearl Harbor,' says Adm James Stavridis, *CNBC,* http://www.cnbc.com/2016/12/15/were-headed-at-a-cyber-pearl-harbor-says-adm-james-stavridis.html (15 Dec 2016)
[ii] Cyberattack, *Dictionary.com* < http://dictionary.reference.com/browse/cyber-attack>
[iii]Gusano informático https://es.wikipedia.org/wiki/Gusano_inform%C3%A1tico
[iv] Computer Fraud and Abuse Act, *Wikipedia,* <http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act>
[v] "Red October" Diplomatic Cyber Attacks Investigation, *SecureList, https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/ (*Enero 2013)
[vi] Cyber Incidents, *Arbor Networks* < http://www.arbornetworks.com/>
[vii] Napoleon Bonaparte Quotes <http://www.rodneyohebsion.com/napoleon-bonaparte-quotes.htm>
[viii] John Markoff, "Dutch Computer Rogues Infiltrate American Systems With Impunity," New York Times (abril 21 1991).
[ix] The Robert Morris Internet Worm, *MIT.edu* < http://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html>
[x] Henry Kissinger, "The Vietnam Negotiations," *Foreign Affairs*, (enero 1969).
[xi] [x] Kenneth Greers, "Cyberspace and the Changing Nature of Warfare" (junio 4 2012).
[xii] Jason Healey and Karl Grindal, "Lessons from the First Cyber Commanders," *New Atlanticist*,(junio 4 2012).
[xiii] The World Conservation Strategy, *Positive Habit Creation* <http://positivehabitcreation.com/order-now/the-world-conservation-strategy/>
[xiv] "WikiLeaks' Julian Assange," *60 Minutes,* <http://www.cbsnews.com/video/watch/?id=7379648n> (4 septiembre 2011).
[xv] Wikipedia, "Anonymous," *Wikipedia,* <http://es.wikipedia.org/wiki/Anonymous> (29 mayo 2013).
[xvi] Paresh Dave, "Cybercrime costs U.S. economy up to $140 billion annually, report says," *Los Angeles Times,* <http://www.latimes.com/business/technology/la-fi-tn-cybercrime-140-billion-dollars-economy-20130722,0,308705.story> (22 julio 2013).

[xvii] Trump in 2010: WikiLeaks 'disgraceful,' there 'should be like death penalty or something' , *CNNPolitics,* http://www.cnn.com/2017/01/04/politics/kfile-trump-wikileaks/
[xviii] From Hero to Zero: wikileaks founder reveals the dirt on the wrong people, *WhaleOil,* https://www.whaleoil.co.nz/2017/01/hero-zero-wikileaks-founder-reveals-dirt-wrong-people/

[xix] Edward Snowden, *American intelligence contractor,* https://www.britannica.com/biography/Edward-Snowden (mayo 2017)
[xx] David Drummond on Snowden, the NSA and Google, < The Daily DoseFEB 26 2014> http://www.ozy.com/pov/david-drummond-on-snowden-the-nsa-and-google/30081
[xxi] Edward Snowden Quotes https://www.brainyquote.com/quotes/quotes/e/edwardsnow523846.html
[xxii] Perlroth, Nicole, "Hackers in China Attacked the Times for Last 4 Months." The New York Times (30 enero 2013).
[xxiii] Morgenthau, Hans. "Another 'Great Debate': The National Interest of the United States." *The American Political Science Review*, 46 (4): 961-988. (1952).
[xxiv] Conrad, Justin. "Interstate Rivalry and Terrorism: An Unprobed Look." Journal of Conflict Resolution 55 (4): 529-555. (2011).
[xxv] Tobias Franke, "Social media: the frontline of cyberdefence?" *NATO Review*, (junio 4 2012).
[xxvi] The White House, ''Foreign Policy: Cybersecurity,'' The White House, agosto 5, 2014, <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity. >
[xxvii] Brandon Valeriano and Ryan C. Maness, Cyber Hype Versus Cyber Reality: Restraint and Norms in Cyber Conflict (Oxford, UK: Oxford University Press, in press).
[xxviii] Clarke and Knake, Cyber War, capitulo 3.