TÉCNICAS DE CIBERATAQUE Y SU RELACIÓN CON EL ESPIONAJE INDUSTRIAL Y ECONÓMICO

JUAN MIGUEL RUBIO SILVERA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTA MARTA DISTRITO TURÍSTICO Y CULTURAL
2019

TÉCNICAS DE CIBERATAQUE Y SU RELACIÓN CON EL ESPIONAJE INDUSTRIAL Y ECONÓMICO

JUAN MIGUEL RUBIO SILVERA

Monografía presentada como requisito para optar al título de Especialista en Seguridad Informática

Ing. CRISTIAN ANGULO RIVERA
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTA MARTA DISTRITO TURÍSTICO Y CULTURAL
2018

AGRADECIMIENTOS.

Al finalizar este trabajo quiero agradecer a Dios por toda la bendición que me dio durante este tiempo y a mi señora madre Edith Silvera de Rubio por haber estado ahí apoyándome todo el tiempo.

LISTA DE FIGURAS

CONTENIDO

GLOSARIO

Amenaza: se refiere a cualquier cosa que puede pasar o no pasar y tiene el potencial de causar serio daño a un sistema de cómputo.

Ciber-ataque: es una deliberada explotación de sistemas de cómputo de empresas y redes computacionales.

Ciber-espacio: es otra forma de llamar al internet.

Cifrado: transformar alguna información dada por signos como: letras, números y caracteres especiales con el fin de esconder y asegurar la confidencialidad y autenticidad de la información ante personas extrañas.

Confidencialidad: es cuando solo los usuarios autorizados pueden ver la información y no otros usuarios no autorizados.

DoS (denegación de servicio): es cualquier tipo de ataque donde los atacantes envían muchos mensajes en masa para interrumpir algún servicio de un servidor dando así la interrupción del servicio a usuarios legítimos.

Hacker: es una persona con conocimientos avanzados en seguridad informática, los cuales los utilizan para cometer ataques a personas, empresas u organizaciones con diferentes fines.

Inflación: es una medida o porcentaje que muestra la subida en precio de los bienes y servicios en un país o región.

Integridad: es una de las tres características de la seguridad en los sistemas de información, la integridad se refiere a la validez y precisión de los datos e información, y que solo puede ser cambiado por personal autorizado.

LAN (red de área local): es una red de computadoras que se limita a un área no muy grande, por ejemplo la red de una empresa.

Marketing: son actividades relacionadas con el mercadeo de bienes y servicios de una empresa.

Networking: se llaman así a las actividades hechas por usuarios con sus dispositivos de cómputo en la red internet.

Riesgo: es el impacto a una organización o empresa cuando una vulnerabilidad es explotada por una amenaza.

RESUMEN

Esta es una monografía que se enfoca en hacer una investigación detallada del espionaje económico e industrial, para luego relacionarlo con las diferentes técnicas de ciber-ataques en todo el mundo. El objetivo principal de este trabajo es ver la importancia de estos tipos de espionaje en el mundo en los cuales se basan en ataques a través de la red internet y de las técnicas utilizadas por estos delincuentes en contra de empresas, organizaciones y gobiernos, para finalmente poder relacionarlo en el escenario colombiano.

Entre las temáticas a desarrollar se tiene en cuenta:

- La historia de estos ataques a nivel mundial.
- La evolución de este problema a través de los tiempos.
- La descripción de las técnicas de estos ataques que emplean los hackers y atacantes en la red.
- Se analiza este problema en el panorama nacional colombiano.

Esta investigación es muy importante realizarla debido a la necesidad de conocer y entender la gran amenaza que representa este problema de seguridad a nivel mundial como local para muchos países en sus organizaciones y empresas.

Es muy importante conocer la forma actual de espionaje que se basa en la tecnología y el uso de ordenadores, las cuales muchos países han utilizado, utilizan y seguirán utilizando. De esta manera siempre van a mejorar las técnicas de ciberataques y esto depende da la capacidad en relación a la economía y a su musculo financiero, por esto los atacantes de países desarrollados tienen más posibilidades que en otros países menos desarrollados. A pesar de esto hay países no tan desarrollados como India y Cuba los cuales invierten en ciberseguridad y son apoyados por otros países en su mayoría, las potencias mundiales, como en el caso de Cuba que es apoyado por Rusia.

En general, los ciberataques de espionaje económico se dan en todo el mundo siempre con fines lucrativos y para ser mejor que el otro en materia de tecnología, armamento e innovación. Los ataques de espionaje corporativo se dan con la intención de poder ganar terreno en esa área empresarial con respecto a la competencia en el mercado, tomando ventaja en materia de mercado mejorando sus productos en base al espionaje hecho hacia las empresas de la competencia.

De este modo, en los países de Latinoamérica hay más vulnerabilidad de espionaje corporativo y económico, que los otros países del mundo, debido a que los países de la región no tienen todavía políticas de protección y control de la seguridad en su infraestructura de redes y comunicaciones. Pocos países de la región de América han comenzado a implantar sus primeros controles en materia de seguridad en internet.

INTRODUCCIÓN

El espionaje siempre ha sido una actividad del ser humano. Todos los pueblos de la humanidad la han practicado durante toda su existencia, y que le han traído beneficios de una y otra forma. Estos reinos, estados y pueblos han usado el espionaje para mejorar en algunas áreas tales como:

- El estándar de vida
- La economía
- La milicia y las armas
- El avance tecnológico, entre otros

El espionaje ha tomado dos (2) nombres específicos, dependiendo a quien se le espié:

- Espionaje económico
- Espionaje industrial o corporativo (entre empresas)

El espionaje económico se realiza cuando un país espía a otro y el espionaje industrial o corporativo lo hacen las empresas entre ellas, también puede haber combinación de estos 2 tipos de espionaje, por ejemplo que un país utilice sus empresas para espiar otras empresas de otros países. A través del desarrollo de esta monografía se ira describiendo los diferentes tipos de espionaje, ya sean individuales o combinados.

Esta monografía se desarrolla en cuatro (4) capítulos, la cual comienza en el primer capítulo con el origen y la evolución del espionaje en todo el mundo, en el segundo capítulo se describen las principales técnicas de los ciberataques, en el siguiente capítulo se describen las técnicas y personas que utilizan los gobiernos para hacer espionaje económico y finalmente se describe el problema en Colombia y su enfoque en un futuro.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

En la actualidad muchas organizaciones en el mundo, como muchos gobiernos están enfrentados a muchos riesgos y amenazas en sus sistemas de información. Estos riesgos y amenazas están relacionados con la pérdida de información relevante en las empresas y/o gobiernos, la mayoría de veces adquirida a través de sus redes de información (redes de datos).

El proceso de perdida de información relevante en las empresas y/o gobiernos son realizados por los hackers y piratas informáticos a través de las redes de computadoras, utilizando herramientas avanzadas de hacking para alcanzar sus objetivos destructivos, ya sean contra personas, organizaciones privadas o del gobierno.

Estos delitos informáticos o ciberataques los realizan de una manera anónima y escondida dentro de la red. Estos robos de información silenciosa y expiatoria son los llamados espionaje económico y espionaje industrial, donde el primero se refiere a espionaje entre naciones o países, y el segundo entre empresas que también es llamado espionaje corporativo. En esta investigación se hará énfasis en las técnicas de ciberataques relacionados con el espionaje económico e industrial o corporativo.

Colombia es un país que todavía está en pañales en estos tipos de amenazas espiatórias en las redes de datos. En contraste los países desarrollados o de primer mundo se ven muy afectados por estos crímenes de espionaje, tales como EE.UU, Alemania, Francia entre otros.

1.3 JUSTIFICACIÓN

Teniendo en cuenta el posible impacto que puede generar y ha generado el espionaje económico y el espionaje industrial en las empresas y gobiernos a través de los tiempos, es muy importante conocer sus orígenes como consecuencias que estos pueden traer a las organizaciones como al país.

Este problema del espionaje económico ha ocurrido desde mucho tiempo atrás en países de todo el mundo, en especial a países desarrollados en todas las épocas y de diferentes formas. Les ha ocurrido más a los países desarrollados debido a que éstos producen y crean nuevos avances en tecnología como en otras áreas, las cuales muchos países se interesan en estos inventos e invenciones.

Es muy importante conocer las técnicas de ciberataques que los atacantes utilizan

para conseguir sus objetivos, esto debido a que en Colombia, prácticamente es casi nula esta actividad para fines de espionaje económico como espionaje industrial. Colombia necesita conocer en más detalle estos riesgos y amenazas en las cuales pueden verse afectadas sus organizaciones, empresas, y el mismo gobierno en un futuro no muy lejano.

En Colombia solo ha habido casos aislados de espionaje industrial (entre empresas), esto por intereses comerciales y de mercadeo principalmente, como fue el caso que ocurrió con la empresa sur coreana HYUNDAY en el año 2016. En Colombia ha habido otros casos de espionaje corporativo, pero el problema está en que estos ataques no se divulgan públicamente por el miedo de que estas empresas atacadas creen mostrarse vulnerables y por tanto temen de volver ser atacadas, ya sean por los mismos delincuentes o por otros.

En resumen es muy importante conocer la actual forma de espionaje que se basa en la tecnología y el uso de ordenadores, las cuales muchos países han utilizado, utilizan y seguirán utilizando mejorando las técnicas de ciberataques.

1.4 OBJETIVOS

1.4.1 Objetivo general.

Analizar, describir y mostrar los orígenes del espionaje económico e industrial a nivel mundial para luego relacionarlo en Colombia y sus organizaciones privadas o públicas.

1.4.2 Objetivos específicos

1. Investigar las causas, orígenes, y evolución del espionaje industrial y económico en diferentes países del mundo.

2. Describir en profundad las diferentes técnicas de ciberataques que los atacantes utilizan para realizar ataques corporativos en Colombia y el mundo.

3. Conocer las distintas técnicas de ciberataques y las fórmulas que los gobiernos utilizan para cometer espionaje económico e industrial.

4. Enfocar el problema del espionaje económico e industrial en un futuro en Colombia

2. MARCO REFERENCIAL

2.1 MARCO TEÓRICO

2.1.1 Diferencia entre espionaje económico y espionaje industrial.

La diferencia clave entre espionaje económico y espionaje industrial, es que el primero envuelve los esfuerzos de un gobierno para conseguir información de otro gobierno, el cambio el espionaje industrial ocurre entre empresas que es el llamado espionaje corporativo. Espiar es irresistible para los líderes, eso es ocasionalmente de gran valor, particularmente en tiempo de guerra. Los lados opuestos en la primera guerra mundial hicieron espionaje y la finalidad era por encontrar armas secretas. Los espías ganaron información en cómo crear armas tales como: gas venenoso y otras armas usadas en la época.

Estos países espiando, ganaron tiempo y recursos financieros que ellos podrían haber gastado más si hubieran desarrollado por ellos mismos este gas venenoso.
La práctica comúnmente conocida hoy: como espionaje industrial, incluyendo el espionaje patrocinado por el estado o gobierno, se ha llevado por varios siglos.

Actualmente y siempre ha sido así, de que las naciones extranjeras dedican significantes recursos económicos para reunir inteligencia acerca de otros gobiernos o elementos de allí, y conseguir información de contra-inteligencia para protegerse en contra de actividades de inteligencia de otras naciones.
El problema del espionaje económico extranjero ha crecido significativamente desde el fin de la guerra fría.

2.1.2 Espionaje económico e industrial.

El espionaje económico ha sido definido como la acción de una nación de colectar información económica de otra nación, simplemente el espionaje económico es robar información privada sin derecho alguno de otro país. El espionaje industrial o corporativo, es una forma de ataque por parte de los empleados dentro de una empresa, dirigido hacia su propia empresa donde trabajan, robando información relevante para poder infiltrarla de esa empresa hacia la competencia principalmente.

Con la competencia entre empresas y gobiernos entre sí, se busca proteger y expandir sus economías. Datos e información colectada puede incluir información como: el producto bruto de un país o (PNB) y graficas estadísticas de tasas de inflación, las cuales pueden ser obtenidas de recursos publicados.

2.1.3 Transición a una sociedad de información que incrementa las interconexiones e interdependencia.

La sociedad moderna está incrementando la dependencia a los sistemas computacionales en redes. El desarrollo de la tecnología de la información en el cyber-espacio ha cambiado la sociedad, comercio y estilos de vida. Estas redes de información han dejado numerosos avances en la calidad de vida, mejorando la provisión de servicios vitales como: medicina y seguridad pública.

La era de la información está habilitada por la tecnología de la computación y tecnologías de las comunicaciones, conocidas como "tecnologías de la información" o TI, cuya evolución ha sido rápida en los últimos años. La computación y los sistemas de comunicaciones aparecen "virtualmente" en cada sector de la economía, incrementándose cada día más en hogares y otras localidades.

2.1.4 El rápido crecimiento de la tecnología computacional.

Como la mayoría de los países avanzados del mundo entran en lo que ha sido determinado como la era de la información, ésta nueva época es definida por el uso de computadoras, particularmente computadoras que se agrupan dentro de redes (redes LAN y WAN) y usadas para facilitar las interacciones de los usuarios.

Los 80´s vieron el rápido desarrollo de la tecnología del computador, y con eso la digitalización de la mayoría de las formas de información. En los años 90´s esta computarización permitió la expansión del internet la cual hace el transporte de la información a cualquier lugar simplemente haciendo solo clíck.

2.1.5 Nuevos crímenes de la era de la información.

El crecimiento de la era de la información y la globalización de la comunicación por internet y el comercio electrónico significativamente ha impactado en la manera en el cual los crímenes económicos son cometidos, la frecuencia con que los cometen y la dificultad de poder coger los atacantes.
La tecnología ha contribuido a incrementar los siguientes aspectos:

- Anonimidad
- Seguridad o inseguridad
- Privacidad o carencia de ella
- Globalización

Además, la tecnología ha provisto el medio o la oportunidad para que se realicen crímenes tradicionales. Los criminales en un mundo electrónico, pueden ignorar

fronteras internacionales, porque ellos pueden: enviar información y ejecutar comandos por las redes de computadoras desde cualquier parte del mundo. No requiriendo presencia física y facilitada por el internet.

2.1.6 Internet está haciendo "eso" fácil.

La popularidad del internet como una forma de comunicación ha colocado un enfoque en la necesidad de proteger las ideas originales por el uso impropio de estas. Irónicamente, la tecnología de la computación ha hecho que la información sea más fácilmente robada. En el caso de crímenes en los computadores o cibercrimen, la necesidad de la legislación para prevenir el acceso no autorizado a datos e información es más importante que nunca.

2.1.7 Los Cibercrimenes son reales.

La mayoría de los crímenes económicos tienen una ciber-versión. Con redes de computadoras o de datos, ahora estos crímenes se extienden a todo el globo, las leyes deben direccionarse a dimensiones internacionales en el tema de crímenes en el ciber-espacio. Estos cibercrimenes ofrecen más oportunidades a los criminales con más grandes posibilidades de éxito y pocos riesgos.

Esto además permite a compañías o empresas que compiten en el mercado en diferentes productos la posibilidad de identificar y descubrir debilidades de seguridad de la competencia colectando información valiosa.

2.1.8 La situación en Colombia.

El espionaje industrial y el robo de datos dentro de las compañías o empresas está cada día incrementándose más en el país. En Colombia donde la tecnología de punta está limitada tan solo en algunos pocos campos, los espías corren detrás de las víctimas donde estas no se relacionan con la investigación y el desarrollo de nuevos productos, sino el problema que es mínimo radica en el espionaje industrial o espionaje corporativo pero a pequeña escala, entre las empresas y su competencia.

2.1.9 Espionaje económico electrónico.

"The anonymity and ease of use of the internet makes it incredibly simple for industrial spies or terrorist alike to obtain open-source data"[1]

Hoy en día se ve el gran desarrollo del internet como también de su expansión en todo el planeta, y se ha convertido en una herramienta muy usada por muchas

[1] FINK, Steven. Managing the global risk of economic espionage. Dearborn trade. 2002. P 119

empresas y firmas en varios países en todo el mundo, para poder obtener información y datos importantes de otras empresas y organizaciones de una manera muy fácil.

2.1.10 Espionaje en la red.

"*Some hackers are out for revenge or retaliation. In the first week in May 2001, in retaliation for an incident involving a U.S. reconnaissance plane, Chinese hackers attacked and defaced more than 650 Web sites of U.S. businesses and the U.S. government* "[2]

Hoy en día es tan fácil hacer espionaje en la red o NET-ESPIONAJE y algunos individuos llamados hackers que son individuos con grandes conocimientos de seguridad informática, pueden fácilmente irrumpir e intervenir en las páginas web de organizaciones y empresas de una manera tan fácil y sencilla y poder así hacer estragos, dejando la mayoría de estos sitios web con fallas o caídos.

Estos ataques han ido en crecimiento debido a la facilidad con que se pueden cometer estos delitos y la tecnología hace cada vez más sencilla el poder cometer estos ciber delitos a empresas, organizaciones o personas en todo el mundo.

"*Over half of 600 companies responding to a survey conducted in 2001 by the Computer Security Institute said they felt their competitors were a likely source of cyber attack, claiming more than $60 million in losses to cyberespionage. The survey is conducted annually by CSI and the Computer Intrusion Squad of the FBI in San Francisco*[3]

"El espionaje en la red envuelve a aquellos quienes se ganan la vida trabajando para empresas o compañías no éticas, el trabajo de estos es violar la red de la competencia y robar y sustraer secretos de comercio, mercadeo a través de la internet, causando grandes pérdidas a todas estas empresas que son víctimas de estos ciberataques por estos ciberespias.

2.1.11 Lidiar con el cibercrimen es muy difícil.

"The more obstacles the government and security experts put inthe hackers' paths—in effect saying, "I dare you to break in, now!"—the more determined the hackers and netspionagers are to showthat they're smarter than the business or government agency thatthinks it has built a better firewall."[4]

El hacking es en algunas instancias es un juego de adolescentes que muchas veces estos ataques en la red o ciberataques son inspirados en un juego de desafiar al otro, el poder ganarle al otro el cual los lleva a cometer estos ciberataques.

Lidiar con los ataques en internet es muy difícil porque no muchas veces se

[2] Ibid. p 123
[3] Ibid.p. 123
[4] Ibid.p. 126.

desconoce el motivo y/o las razones porque estos ciber-delincuentes hacen ataques a empresas como a personas, los motivos son muchos, pueden ser jóvenes hackers, como también hackers especializados con intenciones monetarias o financieras, o simplemente el hecho de hacer daño.

2.1.12 Ingeniería social electrónica.

Microsoft sufrió un ataque en el año 2000 que fue un caso de alta publicidad en ese entonces, fue un intruso que gano acceso a sus redes, sistemas e información muy importante. Microsoft es de las más "importantes y preferidas" empresas a hackear, es el sueño de cualquier hacker, es el poder hackear a la empresa Microsoft Corporation.

Microsoft states that this successful penetration was at the hands of someone specifically seeking the company's commercial and trade secrets. "We are very confident in describing this as an act of industrial espionage," said Microsoft spokesman Dan Leach"[5]

Pero a pesar de todo lo que se dijo y habló en los medios de comunicación, Microsoft se pronunció y anunció que al parecer fue un ataque de espionaje corporativo (industrial), solo con fines de encontrar secretos de marketing, comercio y otra información y datos relevantes a la competencia.

2.1.13 Información robada y crímenes computacionales.

"*Cyberattacks are cheap, easy to launch, difficult to trace, and hard to prosecute"*[6]
Cada año se están viendo más y más ciberataques, doblándose el número de ataques por año. La forma en el cual los crímenes son cometidos son difícil de descubrir y difícil poder penalizarlos y castigar a los autores de estos ciberataques.

"*Reported attacks against Internet systems are almost doubling each year and attack technology will evolve to support attacks that are even more virulent and damaging".*[7]
Los ciberataques están usando la conectividad al internet para explotar vulnerabilidades a los sistemas para conducir actividades criminales, información comprometida y lanzar ataques de negación de servicio (denial of service) como otros tipos de ciberataques que interrumpen seriamente las actividades y operaciones en la red de organizaciones, empresas y personas.

2.1.14 Preparándonos para una nueva cyber-guerra

---

[5] FINK, Steven. Managing the global risk of economic espionage. Dearborn trade. 2002. P 131.
[6] NASHERI, Hadieh. Economic Espionage and Industrial spying. Cambridge University Press. 2005 p 101
[7] Ibid. p. 131

"Although there has never been accurate nationwide reporting of computer crime, it is clear from the reports which do exist . . . that computer crime is on the rise "[8]

Con la expansión de la infraestructura de las redes de datos, de donde están conectados todos los computadores y dispositivos computacionales, se ha venido incrementando la severidad de los ciberataques, cada vez más fuertes y con mayor frecuencia. Haciendo una comparación con hace 15 años se veía que los computadores estaban relativamente aislados y ejecutaban tareas domésticas y básicas.

"*Purely domestic solutions are inadequate because cyberspace has no geographic or political boundaries. Many computer systems can be easily and surreptitiously accessed through the global telecommunications network from anywhere in the world. "*[9]

Hoy en día es difícil controlar estos ciberataques debido a que las redes de datos son extensas y estos ciberataques pueden ser realizados bien encubiertos, desde cualquier parte del mundo y en cualquier momento, y además los recursos tecnológicos que estos ciberatacantes utilizan muchas veces son muy avanzados, y por lo tanto casi siempre no se puede dar solución con sencillas políticas o dar soluciones rápidas a estos ciberataques.

"merchants conducting business in the online environment must face not only the emerging technological attacks such as hacking and infrastructure failures, but also the traditional fraud schemes that have plagued the industry since the inception of credit card transactions" [10]

Debido al rápido desarrollo de las tecnologías computacionales y de las telecomunicaciones, es muy importante que toda la empresa o compañía de negocios en todos sus niveles jerárquicos, desde el jefe ejecutivo hasta el más simple empleado tengan un conocimiento y un entendimiento de los temas de seguridad asociado con actividades de networking y sus implicaciones en el no cumplimiento de las políticas de la seguridad de la empresa.

"The cellular telephone industry is a primary example of an industry that was faced with a significant information security vulnerability, in the form of cellular cloning activity, which threatened to reduce the integrity of the wireless system…." [11] Como las empresas continúan expandiéndose a través de "sus complejos sistemas de redes de datos", la identificación de puntos de vulnerabilidad como sus posibles debilidades en la red son puntos difíciles para las empresas de poder ocultar. Estas vulnerabilidades son completamente difíciles de "tapar o esconder" ante los ojos de los ciberdelincuentes por tanto la empresa esta propensa a estos ciberataques muy fácilmente.

If companies lose valuable secrets to industrial espionage, they cannot profit by using their competitive advantage" [12] Algo importante en relación al espionaje industrial o corporativo es que las empresas o compañías tienen que estar actualizándose

[8] Ibid. p.108
[9] NASHERI, Hadieh. Economic Espionage and Industrial spying. Cambridge University Press. 2005 p 107
[10] Ibid, p 50
[11] Ibid, p 50
[12] Ibid, p 55

constantemente en sus productos y/o servicios y muchas veces sienten la necesidad de espiar a la competencia para así ser más competitivos en el mercado y "no dejarse" ganar de la competencia.

"*In turn, if they are unable to recoup their investments in research and development, they lose their motivation to innovate and bring new products or services to consumers. The consequences include higher prices charged to consumers as well as a decrease in new technologies, creative inventions, and improvements"* [13]

Por tanto, estas empresas si no son capaces de recuperar sus inversiones en investigación y desarrollo, ellos pierden su motivación para innovar y sacar nuevos productos y/o servicios a los consumidores. Esto muchas veces conlleva a graves problemas como son: altos precios en sus productos, y decrecimiento en nuevas tecnologías y de mejoras en sus productos.

Hoy en día es tan fácil poder robar y/o copiar "secretos de empresas" a través de la tecnología, robar tipos de información como:

- Código fuente de programas de computación
- Fórmulas químicas
- Esquemas y diseños técnicos en ingeniería

"*Computers now make it extremely easy to surreptitiously copy and transfer this valuable trade secret information. An employee can now download trade secret information from the company's computer on a diskette, take it home and scan the information on the hard drive of a home computer, and then upload it to the Internet where it can be transmitted within minutes to any part of the world….*" [14]

Y ahora los computadores hacen mucho más fácil que antes estos posibles robos de "información y datos" importantes de las empresas, simplemente usando un computador donde posiblemente puede estar esa información vulnerable y útil para otros como la competencia.

2.1.15 Algo de estadísticas en relación a los ciberataques corporativos.

Los robos de datos de tarjetas de crédito, así como el espionaje corporativo o industrial son los más frecuentes delitos cometidos en Internet. Un informe del año 2012 realizado por la empresa norteamericana INCAPSULA muestra que el 31% de todo el flujo de internet tiene fines malintencionados, que proceden de espías corporativos.

Después de haber analizado los datos de un millar de páginas en internet que contaban entre 50000 y 100000 visitas en un periodo de un mes, se llegó a la conclusión de que un 19% de estas visitas estaban conformadas por un grupo de espías corporativos llamados "espías cookies".

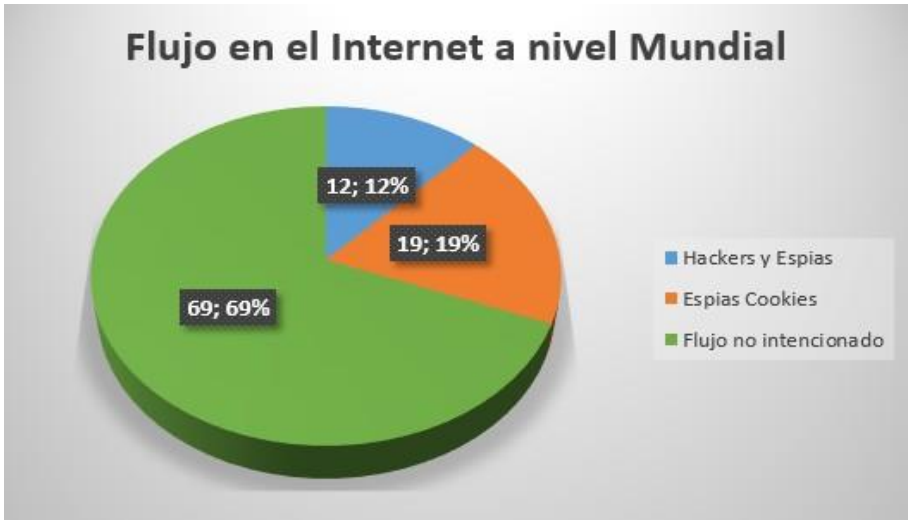
---

[13] Ibid, p 55

[14] NASHERI, Hadieh. Economic Espionage and Industrial spying. Cambridge University Press. 2005 p 56.

La tarea de estos delincuentes consiste en robar información vital para luego ser utilizada con fines de mercadeo para las empresas para la cual le trabajan estos ciberdelincuentes.

Figura 1 Flujo en el internet a nivel mundial.

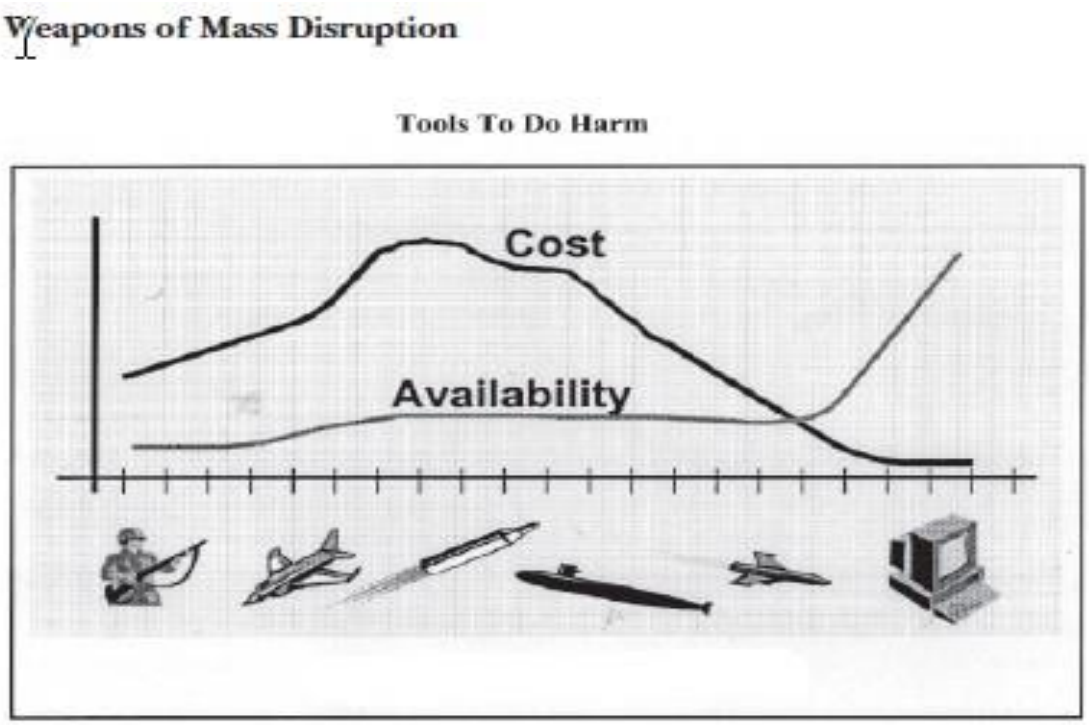


Fuente: UNIVERSIA. Delitos en internet: robo de datos y espionaje corporativo son los más frecuentes. [consultado: 13 Octubre 2018] Disponible en internet: http://noticias.universia.com.ar/en-portada/noticia/2012/03/21/918784/delitos-internet-robo-datos-espionaje-corporativo-son-mas-frecuentes.html

En américa latina, los ciberataques tienen un grado grande de penetración, entre los años 2009 y 2011 los ataques crecieron aproximadamente un 490% según un estudio de la empresa Incapsula, esto debido principalmente a los pocos controles y formas de seguridad que no se implantan en Latinoamérica, debido a los gobiernos por falta de interés de preocuparse por darle más seguridad al internet en los países de américa latina, muchos no miran este problema como importante.

En la siguiente grafica comparativa, se ve la comparación de "armas que hacen daño", esta grafica compara las distintas armas o herramientas que pueden hacer daños a las diferentes naciones, organizaciones y personas, y se puede observar en relación al mal uso de los sistemas de cómputo que tiene una gran disponibilidad y a bajo costo, la cual hace una herramienta muy dañina al ser mal usada por manos criminales o ciberdelincuentes.

Figura 2 Weapons of Mass Disruption.



Fuente**:** NASHERI, Hadieh. Economic Espionage and Industrial spying. [consultado: 29 de Agosto de 2018] Cambridge University Press. 2005. p 110

2.1.16 Esfuerzos por aplicación de las leyes.

"*The government catches about 10% of those who break into government-controlled computers and far fewer of those who break into computers of private companies….*" [15] Debido a la gran ocurrencia de casos de cibercrímenes en la internet, la aplicación de la ley en todos los niveles se está siendo muy difusa y muy difícil de aplicar sobre estos delitos que ocurren en la internet cometidos por ciberdelincuentes.

Hay varias razones por que ocurre esto, debido al gran aumento en crímenes computacionales, la no aplicación de la ley simplemente es debido a que no se tienen los recursos disponibles y también el soporte técnico para poder frenar cualquier cantidad de ciberdelincuentes.

"*Also, the rise in the number of networked computers makes it much easier for hackers to penetrate*

[15] NASHERI, Hadieh. Economic Espionage and Industrial spying. Cambridge University Press. 2005 p 117

and control vast numbers of computers with one breaking, rather than being forced to break in to each computer individually…" [16]
Debido a que los sistemas de cómputo actualmente están formando redes en redes o sub redes en redes de datos, es decir todas estas redes están conectadas entre sí, formando redes LAN, WAN y GAN básicamente. Y esto hace más fácil para los ciberdelincuentes poder atacar a varios sistemas de cómputo al mismo tiempo que atacar una en particular, el cual hace mucho más daño.

2.1.17 Tipos comunes de espionaje industrial o corporativo.

No solamente los estados y gobiernos realizan espionaje entre ellos mismos como a sus propios ciudadanos, sino también lo hacen a las empresas y organizaciones. Estos gobiernos utilizan "espías corporativos" y su efecto genera grandísimas pérdidas y daños a estas empresas espiadas, debido al robo de información tecnológica valiosa, este es el llamado espionaje industrial o corporativo.
Es muy importante tener en cuenta dentro de la misma empresa lo siguiente:

- La segmentación
- Transmisión y
- destrucción de la información y datos para evitar así el hurto de la información importante que podría terminar o acabar con una empresa.
- Sabotaje
- Robo de propiedad intelectual
- Robo de información de los clientes
- Impactos de reputación
- Pérdidas financieras directas

Existen 3 clases de espionaje corporativo:
• Espionaje tecnológico
• Espionaje estratégico
• Espionaje comercial.

2.1.18 Espionaje tecnológico.

Esta forma de espionaje tiene como finalidad poseer las ventajas técnicas que otras compañías tienen. Aquí se puede ver que mientras algunas compañías invierten cientos de millones en investigación y desarrollo de invenciones, otras simplemente se dedican a espiar a su competencia alcanzando así un óptimo nivel de desarrollo tecnológico en base a su accionar expiatorio.

Uno de los casos más conocidos a nivel mundial, fue un caso de espionaje en la fórmula 1, en el cual un ingeniero de la compañía Ferrari, paso una información

[16] Ibid p 117

técnica importante a la escudería británica McLaren en el año 2007.

2.1.19 Espionaje estratégico.

El espionaje estratégico consiste en espiar y robar información de las tomas de decisiones internas de otras empresas principalmente de la competencia de dicha empresa, para así poder tomar ventaja sobre la competencia en aspectos estratégicos y de mercado.

2.1.20 Espionaje comercial.

Este tal vez es el tipo de espionaje menos visible a simple vista. Es el tipo de espionaje que más afecta a las Pymes (pequeñas y medianas empresas), las cuales muchas veces tienen que cerrar sus negocios cada año debido a este tipo de espionaje.

Se podrían mostrar y enunciar innumerables casos que ocurren a diario dentro de las empresas, por ejemplo en los casos cuando empleados de algunas empresas salen con algún pen drive o memoria USB con la base de datos de dicha empresa, para luego establecer su propia empresa y con los años ver quebrar a su anterior compañía. Esto ocurre muy a menudo en el mundo de los negocios y ocurren principalmente a empresas pequeñas que no tienen casi presencia en el mercado.

2.2 MARCO CONCEPTUAL

1. ANONIMIDAD
2. AVANCES TECNOLOGICOS
3. CIBER-CRIMENES
4. COMERCIO ELECTRONICO
5. COMPETENCIA
6. COMPUTADORAS
7. ESPIAS INFORMATICOS
8. ESPIONAJE
9. GLOBALIZACION DE LAS COMUNICACIONES
10. HACKERS
11. INFORMACION
12. INGENIERIA SOCIAL
13. INTERESES DE LAS EMPRESAS
14. INTERESES DE LOS GOBIERNOS
15. INTERNET
16. MALWARE
17. REDES DE DATOS
18. SITIOS WEB
19. TECNOLOGIA

3. DESARROLLO DE LOS OBJETIVOS ESPECÍFICOS

- Investigar las causas, orígenes, y evolución del espionaje industrial y económico en diferentes países del mundo.

- Describir y analizar en profundidad las diferentes técnicas de ciberataques que los atacantes utilizan para realizar ataques corporativos en todas partes del mundo, como en Colombia.

- Conocer y describir las distintas técnicas de ciberataques que los gobiernos utilizan para cometer espionaje económico e industrial.

- Enfocar el problema del espionaje económico e industrial en un futuro en Colombia

3.1 CAUSAS ORÍGENES Y EVOLUCIÓN DEL ESPIONAJE INDUSTRIAL Y ECONÓMICO EN DIFERENTES PARTES DEL MUNDO

3.1.1 Definición del espionaje industrial.

Este tipo de espionaje que hacen las empresas ya sean industriales o comerciales hacia otras empresas consideradas como competencias, lo hacen de muchas formas, utilizando diferentes técnicas de espionaje, técnicas de ciberataques e ingeniería social disponiendo de infiltrados en algunas empresas objetivos, que casi siempre es la competencia inmediata.

3.1.2 Definición de espionaje económico.

Es aquel tipo de espionaje que realizan las naciones o países del mundo con el objetivo de conocer y obtener información acerca de otros países, muchas veces rivales, esta información está enfocada a la economía, finanzas, comercio, producción y tecnología principalmente. Casi todos los países cometen espionaje económico, siendo los más espiados los países más desarrollados como: Estados Unidos y Gran Bretaña. A manera de conclusión entre espionaje económico y espionaje industrial hay 2 puntos importantes:

1. Ambas utilizan técnicas computacionales como los ciberataques.
2. El espionaje económico algunas veces es también industrial, porque estos países que espían, muchas veces lo hacen a industrias que pertenecen a los países que estos espían.

El desarrollo del espionaje industrial como económico en el mundo estuvo relacionado directamente con el desarrollo de los pueblos, reinos, y más tarde con el desarrollo de los estados independientes. El espionaje en la mayoría de casos

ha sido fundamental para la guerra y el advenimiento de las guerras ha marcado la historia mundial.

3.1.3 En el mundo Antiguo:

3.000 años antes de Cristo (A.C.), ya se veían los primeros indicios de haber utilizado el espionaje por pueblos antiguos. En la cultura Mesopotámica donde el rey soberano Sargon I de Acad manejaba y controlaba un importante y vasto territorio entre el Golfo Pérsico y el Mar Mediterráneo. Este creó una red para espionaje de (espías) a través de mercaderes el cual le informaban acerca de las características de los territorios, de los reinos y las posibles utilizaciones que deseaba dominar y controlar.

En la civilización china se encontró el primer tratado militar donde aparecen y se palpan acciones de espionaje, este espionaje se ve reflejado en el arte de la guerra de Sun Tzu, en este tratado se trata algunos pasajes acerca de la importancia que tiene la información y el conocimiento antes de estar presente en una batalla.

Corriendo a través del tiempo, y analizando la histografía de Grecia, esta enseña y muestra como los griegos usaban el espionaje, como además también lo usaba el imperio Persa. Es en este período de tiempo cuando comienzan a desarrollarse sistemas "fuertes" en el cifrado de los mensajes. Por lo tanto, se daba de esta forma un gran avance en los métodos empleados hasta ese momento, que nada más consistía en infiltrar a exploradores en las zonas enemigas.

Según Víctor Ruiz de almirón[17] "uno de los iniciales ejemplos de "codificación criptográfica" que se recuerda es la famosa: de Escala Espartana. En el texto de Juan Carlos Herrera Hermosilla llamado "La breve historia del espionaje" él explica en qué consistía la técnica con la escala espartana: se cortaban 2 pedazos de madera con el mismo radio y grueso, de tal manera que ambos cortes coincidan muy aproximadamente entre sí. Después, con una cinta de cuero se escribía el correspondiente mensaje de forma longitudinal. Este mensaje solo sería legible si estaba enroscado en el trozo de madera. Al correspondiente mensajero de le entregaba la cinta de cuero, que normalmente se utilizaba como cinturón. Luego, al llegar al destino, este mensajero entregaba el cinturón y este mensaje, al poder enrollarse en una escala de las dimensiones, entonces el mensaje recibido podía leerse. Y en caso de que el mensajero fuera interceptado durante su recorrido no habría manera de descifrar o leer el contenido del mensaje.

[17] ABC Internacional. La evolución del espionaje en la Historia: la profesión más Antigua del mundo.[en línea]. https Madrid. (11 de abril de 2013). [Consultado: 15 de noviembre de 2018]. Disponible en internet://www.abc.es/internacional/20131104/abci-evolucion-espionaje-historia-201310311329.html

3.1.4 En el Imperio Romano:

El imperio romano no se quedó atrás con la utilización del espionaje, para poner la balanza de la guerra hacia su lado y así poder ganar las guerras. En la segunda guerra púnica llevada por Aníbal, Roma se vio en peligro, el cual después Aníbal se volvería el gran enemigo de Roma de todos los tiempos. Solo un militar pudo derrotarlo, el principal general Publio Cornelio Escipión, llamado comúnmente como el africano.

Figura 3 Una gran red de espionaje no salvó a Julio Cesar de su asesinato.

Fuente: ZURCHER, Anthony. Del Imperio Romano a la NSA: la historia del espionaje internacional. [consultado: 10 Septiembre 2018] Disponible en internet: https://www.bbc.com/mundo/noticias/2013/11/131101_finde_historia_del_espionaje_amv

En este punto Víctor Ruiz de almirón[18] , aquí en Roma los más importantes políticos poseían sus propias redes de vigilancia, las cuales daban información básica acerca de las posibles intrigas en los diferentes niveles jerárquicos del poder en el imperio. El gran Cicerón se quejaba a cada momento que su correspondencia era interceptada, “todavía no he encontrado un mensajero leal”, le comentó a un amigo íntimo, “son pocos aquellos mensajeros que lleven una carta sin dejar de leerla”. El emperador romano Julio César también diseñó una red de espías que lo tenía bien informado de complots y conspiraciones en su contra. De hecho, es muy probable que él tuviera conocimiento de la conspiración que ocurrió en el senado la cual terminó con su propia vida.

[18] ABC Internacional. La evolución del espionaje en la Historia: la profesión más Antigua del mundo.[en línea]. https Madrid. (11 de abril de 2013). [Consultado: 15 de noviembre de 2018]. Disponible en internet://www.abc.es/internacional/20131104/abci-evolucion-espionaje-historia-201310311329.html

3.1.5 En la edad media

Con el aparecimiento de la edad media, se volvió muy común y general las funciones de los agentes en las cortes de los imperios, que en la mayoría de las veces lo conformaban el embajador y su séquito. Además, ya se podría hablar que en el imperio real de España ya tenía una organización de espionaje bien organizado y centralizado. El primer espía principal o el llamado “espía mayor de la corte” y el encargado de la inteligencia del estado fue: Juan Velásquez en el año 1598.

Figura 4 Justiniano I recibe de los monjes los gusanos de seda. Grabado de P. Galle (1537-1612)

Fuente: HINOCINTE, Espías Medievales en Oriente. [Consultado: 25 Agosto 2018].Disponible en internet: https://hinocinte.blogspot.com/2015/05/espias-medievales-en-oriente.html

El caso de los gusanos de seda fue uno de los primeros casos de Espionaje Industrial en el mundo, fue dado entre China y Europa, cuando una princesa desde china llevo los gusanos que producen la seda a Europa.

3.1.6 En el Siglo XVI

En el entorno de La corte de la reina Isabel primera fue un ambiente de muchas intrigas y la función de Francis Walsingham fue el de tener a su reina más delante de sus contrincantes. En mayo de 1583, Walsingham interceptó unas cartas del embajador de España en Inglaterra, Bernardino de Mendoza, en la que se anunciaba una complot de una invasión a la isla y nombrar en el trono a María, la reina de actual de Escocia. Aquí se veían ya los primeros rasgos de conspiraciones e interceptaciones de mensajes de correo entre reinos.

3.1.7 En el siglo XIX

Otto Von Bismarck finalizando el siglo XIX, realizo varias alianzas que impusieron el dominio de Europa, que con la caída de las piezas claves, dio lugar a los grupos

de países enfrentados en la I Guerra Mundial. El escenario antes de la guerra y en la guerra misma, el espionaje internacional fue parte fundamental en la guerra como en la actuación política de un país.

Víctor Ruiz[19] con las confrontaciones de los años anteriores, se globaliza el uso y la utilización de los servicios de espionaje. Tales como: la fotografía, el radiotelégrafo y el teléfono, empiezan a estar en el objetivo. Sin embargo, la interceptación de las telecomunicaciones es tan ancestral como la misma existencia de las tecnologías más desarrolladas. De hecho, en el año 1862, en el mismo momento de la Guerra Civil, Abraham Lincoln autorizó el control sobre la infraestructura del telégrafo en América.

Víctor Ruiz[20] "es en el siglo XIX donde comienza a globalizarse el sistema de los agentes dobles, que alcanzaría su punto máximo en tiempos de la Guerra Fría entre la URSS y los EE. UU. A finales del siglo XIX Rusia creó una de las agencias de inteligencia más productivas y eficaces del mundo que se llamó: "La Okhrana" que se creó en agosto 14 de 1881, después del asesinato del Zar ruso Alejandro II.

Aunque al principio, la Okhrana se creó como un servicio para la completa seguridad de la familia real, esta lentamente se fue convirtiendo en una clase de "policía secreta" que se dedicaba a desenmascarar a bandidos y desbaratar movimientos revolucionarios.

3.1.8 En el Siglo XX

Durante la segunda Guerra Mundial (1939-1945), los nazis alemanes comenzaron a utilizar (desde comienzos de la década de los 30) un encriptador llamado y conocido como "La máquina enigma", consistía con una tecnología de momento cifrado rotatorio, tanto para cifrar y/o descifrar mensajes. Era una máquina muy liviana y no pesaba más de 12 kilogramos, la cual se podía transportar libremente y sin problemas de un lugar a otro, como también a áreas y zonas de combate, mejorando así las comunicaciones en tiempos de guerra principalmente.

[19] ABC Internacional. La evolución del espionaje en la Historia: la profesión más Antigua del mundo.[en línea]. https Madrid. (11 de abril de 2013). [Consultado: 15 de noviembre de 2018]. Disponible en internet:://www.abc.es/internacional/20131104/abci-evolucion-espionaje-historia-201310311329.html

[20] ABC Internacional. La evolución del espionaje en la Historia: la profesión más Antigua del mundo.[en línea]. https Madrid. (11 de abril de 2013). [Consultado: 15 de noviembre de 2018]. Disponible en internet:://www.abc.es/internacional/20131104/abci-evolucion-espionaje-historia-201310311329.html

3.1.9 Maquina Enigma

La máquina Enigma fue inventado por un ingeniero alemán, Arthur Scherbius, que era muy conocedor de la electromecánica, que tras la primera Guerra Mundial, trató de aplicar la tecnología del momento para tratar de mejorar los sistemas criptográficos de los ejércitos. La idea de Scherbius fue patentada en febrero de 1918, que consistía en la aplicación del cifrado VIGENERE, que en realidad, era aplicar un algoritmo que sustituía unas letras por otras.

La máquina Enigma era un aparato electromecánico, es decir, estaba compuesto por una parte mecánica y otra eléctrica. El mecanismo estaba constituido por una serie de teclas con todas las letras alfabéticas, era muy parecido a una máquina de escribir, al presionar las teclas estas activaban unos cilindros que daban vuelta, para el usuario era muy fácil manejarla y utilizarla, después de escribir las letras de las palabras introducidas la maquina generaba unas letras las cuales el que la utilizaba tenía que anotarlas, y que era finalmente el mensaje codificado.

Figura 5 Maquina Enigma

Fuente: MANSO, Alfonso. La Máquina Enigma. [consultado: 28 de Septiembre de 2018].Disponible en internet: http://www.u-historia.com/uhistoria/tecnico/articulos/enigma/enigma.htm

En este campo de las comunicaciones la armada estadounidense carecía de un sistema funcional como lo era la máquina enigma. Los sistemas tradicionales eran fácilmente interceptados por los ejércitos enemigos, como en el caso de los japoneses, durante las batallas en el pacífico en la segunda Guerra Mundial, así se presentó la utilización de lenguas nativas de indígenas nativos norteamericanos ya que los japoneses no conocían esas lenguas.

Figura 6 Criptógrafos de E. U interceptaron conversaciones diplomáticas en 1922.

Fuente : ZURCHER, Anthony. Del Imperio Romano a la NSA: la historia del espionaje internacional. [consultado: 10 Octubre 2018] Disponible en internet: https://www.bbc.com/mundo/noticias/2013/11/131101_finde_historia_del_espionaje_amv

3.1.10 En la guerra fría

En todo período de la Guerra Fría, la inteligencia y la contra-inteligencia se enfocó en objetivos puramente militares y políticos. Víctor Ruiz[21] de almirón: La Guerra Fría, se caracterizó como un periodo donde hubo una presión y tensión política constante entre la desaparecida Unión Soviética (URSS) y los Estados Unidos de América, la que estimuló el terreno para la época dorada del espionaje.

En este punto Víctor Ruiz[22] de Almirón, en 1947 el presidente norteamericano Truman presentó la nueva Ley para la seguridad nacional para todo el territorio. Esta Ley establecía la posible creación del organismo de seguridad CIA (Agencia Central de inteligencia). Esto debido principalmente a las fallas de inteligencia cometidas en relación al ataque japonés a Pearl Harbor en 1941. Las primeras actividades de la CIA en conjunción con el organismo británico de seguridad llamado MI-6, para interceptar las comunicaciones telefónicas en las oficinas de la URSS en la capital alemana Berlín.

En este punto Víctor Ruiz[23] "algunos agentes de la URSS infiltrados dañaron en muchas ocasiones los planes que los estadounidenses tenían. La más significante

[21]ABC Internacional. La evolución del espionaje en la Historia: la profesión más Antigua del mundo.[en línea]. https Madrid. (11 de abril de 2013). [Consultado: 15 de noviembre de 2018]. Disponible en internet://www.abc.es/internacional/20131104/abci-evolucion-espionaje-historia-201310311329.html

[22] . ABC Internacional. La evolución del espionaje en la Historia: la profesión más Antigua del mundo.[en línea]. https Madrid. (11 de abril de 2013). [Consultado: 15 de noviembre de 2018]. Disponible en internet://www.abc.es/internacional/20131104/abci-evolucion-espionaje-historia-201310311329.html

[23] ABC Internacional. La evolución del espionaje en la Historia: la profesión más Antigua del mundo.[en línea]. https Madrid. (11 de abril de 2013). [Consultado: 15 de noviembre de 2018].

infiltración de los soviéticos sobre los norteamericanos fue en las oficinas que la CIA tenía en el país centroamericano de Guatemala, desde donde se organizó el ataque a la Bahía de Cochinos, con lo que se provocaba incidir en un levantamiento del pueblo cubano contra el régimen del dictador Fidel Castro.

Figura 7 Un agente del FBI está usando luz ultravioleta para leer un escrito de un posible espía.

Fuente: LERNER, Lee. Encyclopedia of Espionage, Intelligence, and Security. volume 1. [consultado: 2 de Octubre de 2018].Gale 2004. p 124

3.1.11 La KGB y la CIA

El contraespionaje fue una de las labores más realizadas durante la Guerra Fría, esto fue lo que enfrentaron algunos países, que estuvo presente durante el siglo XX, desde 1945 hasta la terminación de la URSS y la caída del comunismo que fue entre 1989 (derrumbe del muro de Berlín) y 1991 (el golpe de estado en la Unión Soviética), entre los dos bloques: Oriental y Comunista liderado por la URSS y Occidental- capitalista, liderado por EE.UU.
Este conflicto estuvo presente en los niveles: ideológico, político, económico, tecnológico, militar principalmente.

Más tarde del derrumbe del muro de Berlín en noviembre de 1989, en Estados Unidos se tenía la esperanza de descubrir el secreto de la eficiencia de la Unión Soviética para “descubrir” a sus propios agentes. La pregunta era el cómo lograba

---

Disponible en internet:://www.abc.es/internacional/20131104/abci-evolucion-espionaje-historia-201310311329.html

la KGB ubicar a los agentes de la CIA que realizaban sus acciones diplomáticamente de estas detecciones, los operativos encubiertos de Estados Unidos fueron abortados y cancelados una y otra vez.

Figura 8 Emblemas de la KGB y la CIA

Fuente: SANTOS, Sandra. Descubre ideas sobre Guerra Fría. [consultado 12 de septiembre de 2018].Disponible en internet: https://co.pinterest.com/pin/320248223479844320/

3.1.12 Finales del siglo XX y comienzos del XXI

En la década de los 70, todos los logros y avances en el tema del espionaje partiendo de los pequeños micrófonos escondidos hasta teléfonos alterados se colocaron al servicio del espionaje político en el escándalo más hablado en el mundo hasta ese momento que fue el caso Watergate. Un caso que rodeó al presidente Richard Nixon, acusando y señalando a 7 colaboradores muy cercanos a él en el tema de espionaje telefónico. En esta década se comienza la utilización de satélites espías por ambas potencias los EE.UU. y la URSS, en la figura 9 se puede ver uno de los primeros satélites espías de la ex Unión Soviética, la serie de satélites Yantar.

Figura 9 Satélite Ruso yantar 4K2M

Fuente: MIRANDA, Eladio. Lanzamiento del satélite Yantar-4K2M (Kobalt-M)Cosmos 2450.[consultado 30 de Octubre de 2018].Disponible en internet: https://lanzamientos.wordpress.com/2009/05/07/lanzamiento-del-satelite-yantar-4k2m-kobalt-mcosmos-2450/

Edward snowden: Fue un ex-empleado de la Agencia de Seguridad Nacional (NSA), esta organización de Estados Unidos fue creada en la mitad de la década de los 50´s; la NSA es una organización de inteligencia que tiene como misión analizar a fondo como obtener información acerca de lo que transmiten los mandos de trasmisión y comunicación y además, tiene la función de proteger y darle seguridad a las comunicaciones que el Gobierno de Estados Unidos mantiene con otros países amigos y aliados.

Figura 10 Edward Snowden

Fuente: HISPANTV. Edward Snowden reaparece en Twitter con más de 150.000 seguidores en menos de una hora. [consultado el 3 de Agosto de 2018]. Disponible en internet: https://www.hispantv.com/noticias/sociedad/59058/edward-snowden-twitter-tuit-150000-seguidores

Por lo tanto, la NSA es muy importante en el círculo de inteligencia de los Estados Unidos. Snowden además de consultor en Tecnología, también trabajó para la CIA estadounidense por largo tiempo y así también para la NSA. El problema con Edward Snowden ocurrió cuando en Junio del 2013, divulgó, reveló y dio a conocer a través de los periódicos estadounidenses:

- The Guardian
- The Washington Post

Unos documentos muy secretos del organismo NSA, y más especialmente sobre un programa llamado PRISMA lo que impactó al público en general y de todo el mundo y especialmente a los Estados Unidos, tiene que ver con el programa PRISMA es supuestamente un ***ente de espionaje*** o un organismo expiatorio, que rastrea y sigue detenidamente a aquellos individuos estadounidenses que viven fuera de Estados Unidos o bien ciudadanos que se contactan con otros individuos que viven fuera del país, por medio de la lectura de sus correos electrónicos, de los videos que suben a Internet, de sus conversaciones, de sus direcciones IP, el movimiento de archivos que realizan, ya sea enviar o recibir archivos y además también de sus perfiles en las redes sociales donde tienen algún tipo de cuenta personal.

Este conocimiento y tal vez "***secreto de estado***" que divulgó, causó gran estupor a nivel mundial por la intromisión del programa prisma sobre la vida personal de los ciudadanos. Actualmente, nadie sabe dónde se encuentra Edward Snowden, huyó a Hong-Kong, y aunque se sabe que el Departamento de Justicia de Estados Unidos piensa en que su accionar fue un acto criminal, así que se especula con su detención y una dura sanción. Víctor Ruiz[24] de almirón "pero el gran invento propio del espionaje mundial es ECHELON, un sistema desarrollado por los países de habla inglesa".

3.1.13 Echelon

Echelon es un sistema global para espionaje el cual fue creado por los siguientes países:

- EE.UU.
- Australia
- Gran Bretaña
- Nueva Zelanda
- Canadá

Echelon es básicamente un sistema automatizado para interceptar y monitorear comunicaciones electrónicas, además puede monitorear hasta más de 3.100 millones de comunicaciones por día, incluyendo en estas comunicaciones:

- Llamadas por teléfono
- Transmisiones satelitales
- Correos electrónicos
- Faxes
- Descargas (downloads) desde internet.

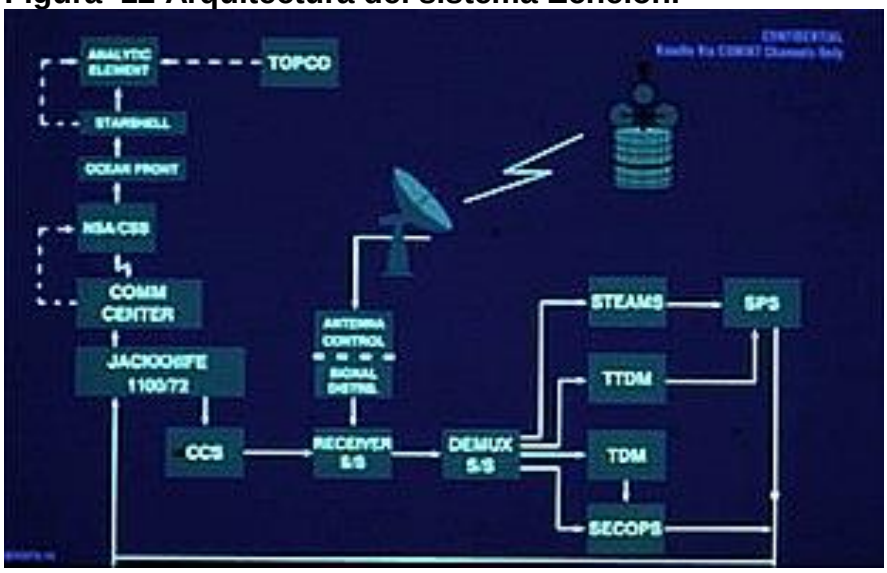
Echelon recoge información a través de un sistema amplio y extenso de antenas de radio y satélites en órbita sobre la tierra, que monitorean las comunicaciones entre satélites y "husmean" a todos los dispositivos que navegan en internet en tiempo real, a partir de los paquetes de datos o "frames". Echelon se ha utilizado muchas veces como medio para tareas de espionaje corporativo y espionaje económico, y no solamente para tareas y/o ejercicios militares

[24] ABC Internacional. La evolución del espionaje en la Historia: la profesión más Antigua del mundo.[en línea]. https Madrid. (11 de abril de 2013). [Consultado: 15 de noviembre de 2018]. Disponible en internet:://www.abc.es/internacional/20131104/abci-evolucion-espionaje-historia-201310311329.html

Figura 11 Sistema de vigilancia global Echelon

Fuente LA ESENCIA MISMA DEL MISTERIO. Conspiraciones: Echelon. [consultado: 3 de Noviembre de 2018]. Disponible en internet: https://revistavocesdelmisterio.wordpress.com/2018/03/08/conspiraciones-echelon/

Figura 12 Arquitectura del sistema Echelon.



Fuente: ECHELON. Echelon [consultado: 28 de Septiembre de 2018]. Disponible en internet: https://en.wikipedia.org/wiki/ECHELON

Este es un diagrama del sistema de interceptación de satelital en la estación NSA en la estación de investigación en Yakima (EE.UU.).

Estas son sus partes:

TOPCO: terminal de control de operaciones (Terminal Operations Control)

CCS: Subsistema de control computarizado. (Computer Control Subsystem)

STEAMS: Sistema de prueba, evaluación, análisis, y subsistema de monitoreo.

SPS: Subsistema de procesamiento de señal.

TTDM: Demodulador teletipo

3.2 DESCRIBIR Y ANALIZAR EN PROFUNDIDAD LAS DIFERENTES TÉCNICAS DE CIBERATAQUE.

En este punto se desarrollarán los siguientes subtemas: el cambio en las tendencias del espionaje, que hace referencia a la nueva forma de espionaje de las naciones como también los temas a espiar. También se describirá sobre la evolución a una sociedad de información incrementando las interconexiones e interdependencias. Se hablará del cambio que ha producido el Internet en la vida de los seres humanos en este siglo XXI. En el rápido crecimiento de la tecnología computacional, se habla un poco también de la expansión y aumento de la tecnología de los computadores, y otros dispositivos.

También se tratarán los nuevos crímenes en la era de la información. Se expondrá la aparición de nuevos delitos y la forma como los cometen los atacantes o criminales modernos.

3.2.1 Cambio en las tendencias del espionaje.

Con la caída del comunismo, la comunidad de inteligencia de EE.UU., fue forzada a redefinir su misión y rol en orden para encontrar nuevas realidades después de la guerra fría, los EE.UU. comenzó a buscar nuevas metas en carácter de espionaje y no solo se limitó a espiar a la ex unión soviética y sus movimientos, sino que su espionaje se enfocó en otros temas y en otros países.

Diferentes formas de espionaje involucrado. Ahora, las actividades del espionaje han cambiado para concentrarse en tecnología, procesos de manufactura, y otros secretos del comercio que algunas veces tienen dos (2) usos (uso dual).

Servicios de inteligencia extranjera ha incrementado sus recursos para robar tecnología de EE.UU., comenzando con el oficial de la CIA ALDRICH AMES que comenzó a enviar secretos a la KGB de la Unión Soviética en 1985, también un científico llamado RONALD HOFFMAN comenzó a vender información clasificada.

AMES, el último conocido espía de la guerra fría recibió $4.6 millones de dólares por nombres de informantes de la CIA antes que él fuera cogido a comienzos de 1994. HOFFMAN, un supervisor de un proyecto para una compañía llamada SCIENCIE APPLICATIONS, INC, consiguió $760.000 dólares vendiendo complejos programas de Software desarrollados bajo un contrato secreto para la iniciativa de defensa estratégica. HOFFMAN, quien fue atrapado en 1992, vendió su software a multinacionales japonesas las cuales fueron: La compañías NISSAN MOTOR, MITSUBISHI ELECTRIC, industrias MITSUBISHI NEAVY, e industrias ISHILLJAWAJIMA tomando esta información para programas Aero-espaciales.

3.2.2 Evolución a una sociedad de información incrementando las interconexiones e interdependencias.

La sociedad moderna está incrementando la dependencia a los sistemas de redes de computadoras. El desarrollo de la tecnología de la información en el ciberespacio ha cambiado la sociedad, comercio y estilos de vida. Estas redes de información han permitido numerosos avances en la calidad de vida mejorando la provisión de servicios importantes como: medicina y la seguridad. La era de la información está habilitada por la computación y la tecnología de la comunicación, conocida como las tecnologías de la información, cuya rápida evolución es casi dada por hecho.

La computación en cada sector de la economía ha producido un crecimiento en hogares y otros lugares. Estos sistemas enfocan la economía y la actividad social en la recolección de información; analizando, avasallando, almacenando, presentando y diseminando información en texto; numéros, en audio, en imágenes y formatos de video como un producto de eso mismo o un complemento a productos físicos.

La ciencia y la tecnología han revolucionado más la estrategia geopolítica, internacionalizando mercados y creó nuevas publicidades para una destrucción nuclear, gobiernos totalitarios, y a cambió la conducta de la guerra y las bases del poder público y económico.

3.2.3 El rápido crecimiento de la tecnología computacional.

Casi todos los países del mundo han entrado a la era de la información, esta nueva época es definida por el uso de computadores, particularmente computadores agrupados en forma de red y que fue usado para facilitar las interacciones de los humanos en los años 80´s.

En los 80´s se vio el rápido desarrollo de la tecnología computacional y con eso la organización a todas las formas de la información. En los años 90´s, esta computación permitió la expansión del Internet, que permite el transporte de la información rápidamente a cualquier parte del mundo con un solo clic.

La habilidad para digitalizar la información y su transporte en el mundo con un clic de un ratón creó un "**terreno fértil**" para el movimiento de información protegida por leyes de propiedad intelectual, por ejemplo: INTEL el fabricante de chips, ha revolucionado la industria computacional a través de un sencillo producto: el **microprocesador.**

INTEL desarrolló este producto a través de años de investigación, desarrolló y modificación. Sin embargo, a través de actos inescrupulosos de una persona, los competidores de la compañía pudieron obtener la información necesaria para producir un producto idéntico por menos costo, esfuerzo, y tiempo, dejando a INTEL fuera del negocio.

3.2.4 Nuevos crímenes en la era de la información.

El crecimiento de la era de la información y la globalización de las comunicaciones del Internet y el comercio ha impactado significativamente la manera en la cual los crímenes económicos son cometidos, la frecuencia con que se cometen y la dificultad para atrapar y penalizar a los **cibercriminales.**

La tecnología ha contribuido a incrementar en cuatro (4) grandes aspectos:

- Anonimidad
- Seguridad o inseguridad
- Privacidad o carencia de ella
- Globalización.

La tecnología ha provisto el medio y oportunidad para cometer crímenes tradicionales. Criminales en el mundo electrónico pueden ignorar leyes internacionales porque ellos pueden enviar información y ejecutar comandos a distancia a través de las redes de datos en el mundo. No requiriendo acceso físico y facilitado por la presencia del Internet.

Aunque el Hackeo de computadoras es un buen ejemplo de crimen internacional en el ciberespacio, hay otros crímenes que son facilitados por las redes de datos como: falsificación, transmisión de amenazas, fraude, infracción de derechos de autor, robo de secretos de negocios, transmisión de pornografía infantil, interceptación de comunicaciones y transmisión de comunicaciones de acoso.

Los casos de Hacking de computadoras han incrementado la cantidad de "temas" de los crímenes electrónicos internacionales. Además, la inhabilidad para prevenir estos ataques basados en: la fuerza de la Ley y sector privado carecen de herramientas efectivas y de soluciones para poder llevar a los criminales ante la justicia.

Antes de hablar de las técnicas de ciber-espionaje, se debe tener en cuenta que hay dos (2) tipos de amenazas para las organizaciones y estas se presentan en dos (2) formas:

- Criminales comunes (técnicas comunes)
- Empleados de confianza (insiders)

3.2.5 Definición de las técnicas más utilizadas y criminales comunes

De acuerdo al gobierno de EE.UU., más del 25% de la población ha sido golpeada por ladrones de identidad en una forma y otra. Estos ladrones de identidad cometen crímenes bajo el nombre de otra persona.

Para los ataques corporativos se utilizan las siguientes técnicas:

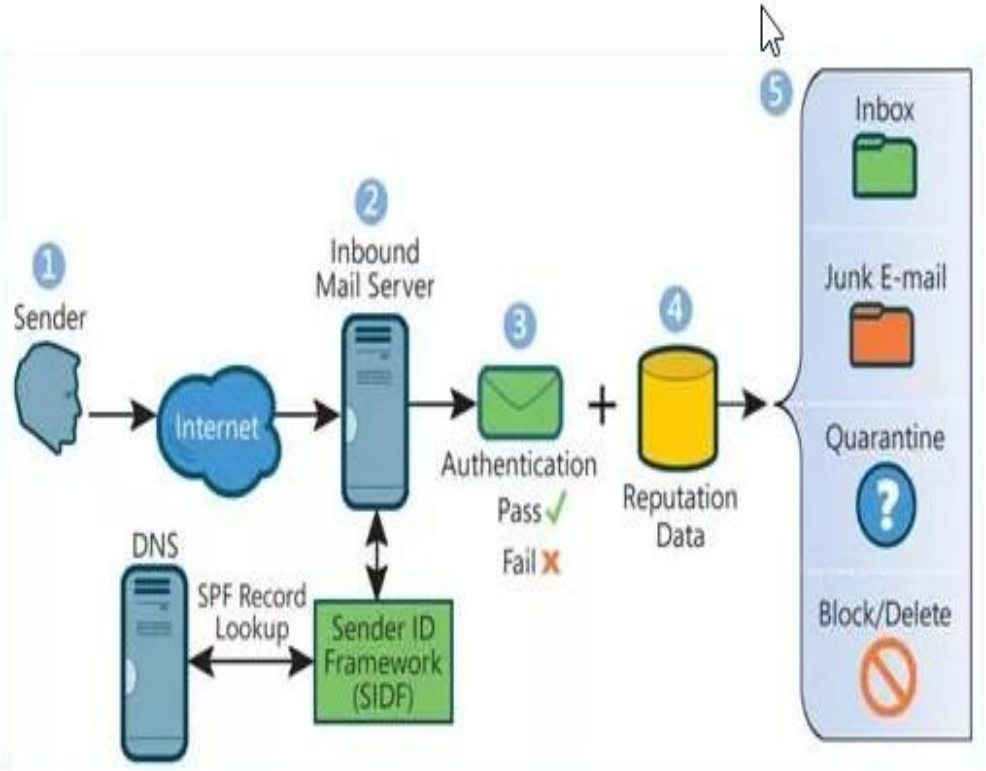
- Spammers (envían Spam).
- Phishing
- Virus y gusanos
- Spyware
- Vishing

3.2.5.1 Spammers (envían Spam)

El promedio de usuarios de Internet reciben docenas de mensajes de Spam todos los días. En un nivel básico, el problema de estos correos spam es que afecta la productividad de las empresas, y se toma mucho tiempo de ir a través de todos los correos electrónicos para verificar cuales son spam y cuáles no.

Figura 13 Spammers.

En este esquema se ve el proceso de entrada de correos electrónicos ya sean correos spam o normales, se ve el proceso de identificación y almacenado.



Fuente: POGOSYAN, Andrey. Virtualize my datacenter. [consultado 2 de Octubre de 2018].Disponible en internet: https://virtualizemydc.ca/why-do-we-need-an-spf-txt-record/

Los controles de Spam además causan que los mensajes válidos sean borrados y eso le cuesta a las compañías millones de dólares por año; para lidiar con este problema que en promedio es el 70% o más son mensajes de correo electrónico son Spam.

El propósito del Spam, es robar información de claves y credenciales de tarjetas de crédito y otra información relevante. El Spam está siendo combinado con más ataques dañinos; los Spams muchas veces liberan virus, ellos son además usados para esparcir Spywares los cuales monitorean las acciones de las computadoras de las compañías, roban información a estas y algunas veces toman el control completo de los computadores.

En figura 13 se muestra el proceso de un correo electrónico que comienza con el que lo envía (Sender) y llega hasta el punto 3, donde se analiza el E-mail punto 4 y luego se clasifica ya sea:

- ✓ Normal (vía inbox del usuario), junk (SPAM), va a cuarentena o se elimina.

3.2.5.2 Phishing.

Se ha convertido en uno de los más comunes crímenes informáticos de hoy en día, resultando en grandes pérdidas en fraudes, una cifra que excede los $2.400.000.000 de dólares anuales según el libro “Espías entre nosotros” de la autora IRA WINKLER. Phishing es básicamente un tipo de Spam que combina otras formas de ataque. Alguien hackea un servidor WEB y entonces crea un sitio WEB que luce como una página Web legitima de alguna compañía seria como: EBAY, PAYPAL, CITIBANK, O US BANK. La página requiere ahora personas que entren información personal como: número de cuentas, números de pines, credenciales de tarjetas de crédito.

El criminal entonces, crea “un mensaje SPAM” que aparentemente viene de una compañía suplantada. El mensaje podría decir que la cuenta del usuario en la compañía ha sido sujeta a fraude y requiere que el usuario verifique su información personal para “poder” ser desbloqueada. El mensaje contiene un link para hacer clic y entrar al sitio web, que envía al usuario a la supuesta página para confirmar la información de él mismo y este entra sus datos y el atacante se apodera de su información.

Figura 14 Phishing attack.

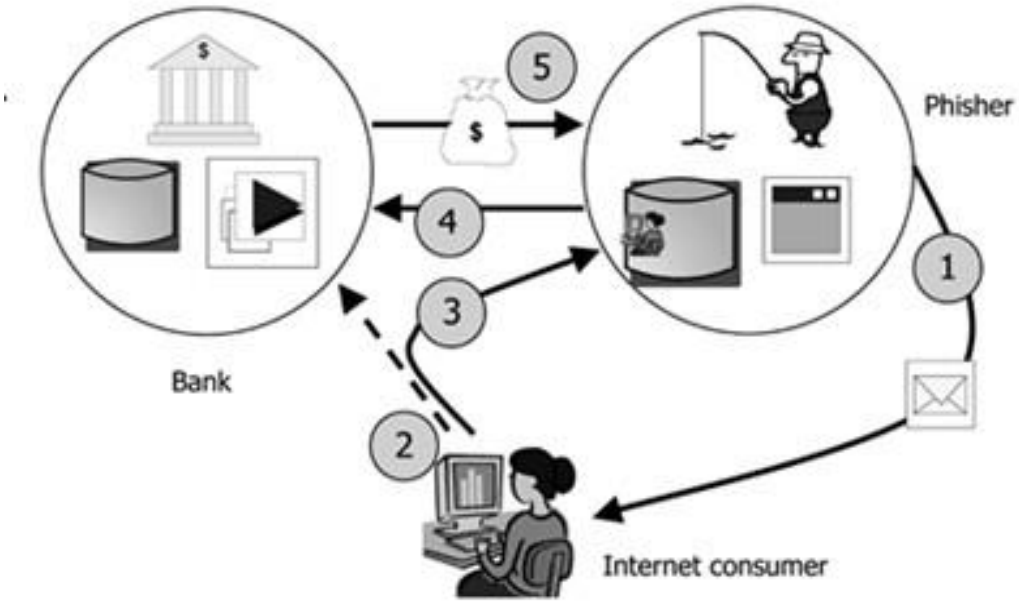


Figure – Phishing attack

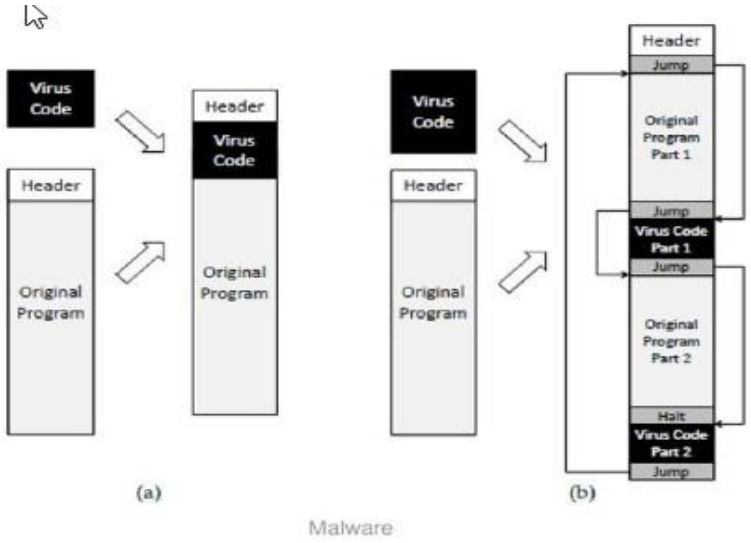
Fuente: INFOSEC INSTITUTE. Modern Online Banking Cyber Crime. [consultado 27 de Octubre de 2018].Disponible en internet: https://resources.infosecinstitute.com/modern-online-banking-cyber-crime/#gref

En la figura 14 se ve el proceso desde el punto 2 cuando el usuario recibe un correo del atacante, este usuario usa el link del correo y va a la página suplantada del atacante y este sujeto consigue ganancias.

3.2.5.3 Virus y gusanos (virus and worms).

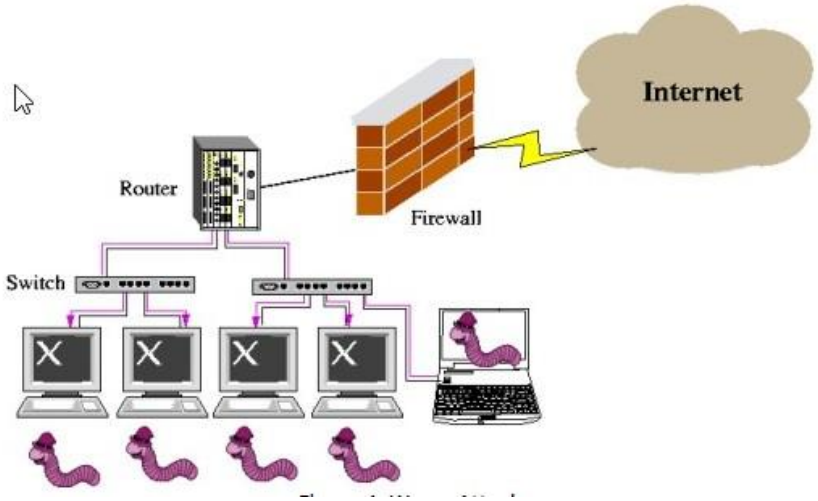
Los virus y gusanos de las computadoras causan perdidas de billones de dólares por año. Estos tipos de programas (códigos) de computadoras se liberan y esparcen por ellos mismos, después que han infectado una máquina computacional, causando así daños. Los virus requieren que un usuario (victima) ejecute alguna acción como por ejemplo: abrir un correo. Los gusanos se esparcen y se reproducen por ellos mismos automáticamente sin requerir alguna acción manual (realizada por el usuario). Estos gusanos y virus (malware) han causado que bancos, empresas y aerolíneas se “desplomen”, las redes de los cajeros ATM han sido bloqueadas muchas veces

Figura 15 Virus.



Fuente: PENN STATE NEWS. Probing Question: What are computer viruses and where do they come from?.[consultado: 3 de Noviembre de 2018]. Disponible en internet: https://news.psu.edu/story/141201/2008/07/17/research/probing-question-what-are-computer-viruses-and-where-do-they-come

Figura 16 Worms.



Fuente: CERTIFICATIONSKITS. CCNA Security: Worm, Virus and Trojan Horse Attacks. [consultado: 3 de Septiembre de 2018]. Disponible en internet: https://www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-describe-security-threats/ccna-security-worm-virus-and-trojan-horse-attacks/

En general, virus y gusanos se esparcen por las redes causando problemas a las organizaciones de diferentes formas: como bajar la productividad de las empresas de la competencia y poder algunas veces hacer espionaje. Ver figuras 15 y 16

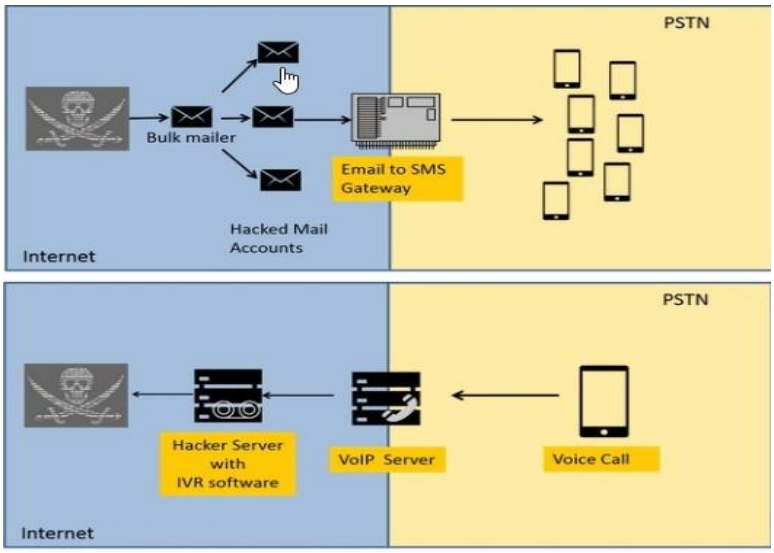
3.2.5.4 Spyware.

El Spyware es tal vez el Malware “ideal” para los atacantes poder hacer espionaje a empresas y a individuos en particular. El Spyware es instalado sorpresivamente en el PC de la víctima y chequea todas las acciones y movimientos que la víctima realiza sea un individuo o algún empleado en una compañía. El Spyware es usado para buscar y robar información personal y corporativa. Este tipo de malware se ubica en el PC de la víctima y puede tomar el control de la computadora, este se puede obtener o contagiar, descargando archivos en sitios WEB que no son seguros, también a través de correos usando la técnica maliciosa de Phishing.

3.2.5.5 Vishing.

Se puede definir que Vishing es el acceso ilegal a datos en forma de Voz Internet Protocol (VoIP) Vishing es la versión telefónica de Phishing el cual usa mensajes de voz para robar identidades y recursos financieros, el término Vishing es la combinación de (Voice) y Phishing. Ver figura 17

Figura 17 Ataque Vishing.



Fuente: SOFTPEDIA NEWS. Customers of US Banks Targeted in Vishing Attacks. [consultado: 4 de Noviembre de 2018].Disponible en internet: https://news.softpedia.com/news/Customers-of-US-Banks-Targeted-in-Vishing-Attacks-440070.shtml

Los ataques de Vishing son diseñados para generar miedo y presionar para obtener una respuesta inmediata de la víctima, estos ataques son difíciles de trazar.

3.2.5.6 Los hackers.

El término hacker fue originalmente usado para referirse a los estudiantes de ciencias de los computadores en M.I.T Cuando los computadores personales (PC) comenzaron a proliferar durante los 80" una nueva "raza" de hacker emergió. Estos nuevos hackers usaron sus PC´s para conectarse a compañías, empresas y universidades a través de sus servidores, usando modem sobre líneas telefónicas sin permiso alguna, lo cual era ilegal.

Al final de la década de los 80´s, algunos de los primeros hackers ya habían crecido y se dedicaban a vender información y servicios. Miembros de una de los más notorios grupos de hackers "los maestros de la decepción", han sido acusados de modificar y vender reportes de créditos, venta de información a investigadores privados, robar servicios telefónicos, entre otros crímenes.

Algunos miembros del grupo de hackers "los maestros de la decepción" se declararon culpables de los cargos imputados en los años 90´s. Sus acciones son consideradas criminales cuando ellos/ellas se involucran en un uso no-autorizado de un computador. Como el Internet comenzó a tomar forma a comienzos de los 90´s, el número de los hackers que andaban comenzó a incrementarse. Sin

embargo, la habilidad y el conocimiento requerido para ser un hacker decrecieron rápidamente. El hacker original tuvo que desarrollar sus propias técnicas para explotar computadoras.

Los hackers de hoy tienen que mirar en Internet para encontrar un programa de computadora que pueda explotar el computador por ellos, aplicaciones novedosas y muy fáciles de utilizar. El primer hacker quería aprender acerca de sistemas computacionales, los nuevos hackers justamente quieren irrumpir el sistema sin el desafío de aprender acerca de ellas.

3.2.5.7 Como hackear un computador.

Hay dos (2) formas fundamentales para irrumpir dentro de un PC y que estas formas requieren muy poca habilidad. Algunas personas pueden afirmar que hay miles de diferentes explotaciones y tácticas que un hacker puede usar.
La primera forma de irrumpir un PC es tomar ventaja de las vulnerabilidades del sistema. Todas las computadoras son controladas por un Software o programas de computadoras. Aunque un PC generalmente tiene un Hardware y Software, vulnerabilidades encontradas en el hardware son extremadamente raras e igual, aquellas vienen del “Firmware” que es básicamente Software “quemado” en el Hardware.

La segunda forma para influir en un PC es tomando ventaja de saber cómo un computador está configurado y mantenido por un administrador o usuario. Asumiendo que todo el software en un PC está perfecto alguien puede crear una vulnerabilidad en ese sistema.

3.2.5.8 Empleados de confianza.

Insiders: Personas con acceso físico a una empresa poseen la más grande amenaza para la seguridad de esa empresa. Ellos tienen el tiempo y la libertad para buscar dentro de los escritorios de los otros empleados, leer memos privados, copiar documentos y abusar de la amistad de los compañeros de trabajo, conocen acerca de las operaciones de la empresa, simplemente porque han estado dentro, típicamente tiene bajo riesgo actividades de espionaje, y si ellos son inteligentes, cuidadosos y pacientes, son raramente cogidos en el acto y en el tiempo.

Lo más importante es saber que estas personas saben dónde y cómo hacer daño a la empresa. Ellos conocen los secretos de precios, conocen la competencia, y usualmente conocen como esconder sus acciones. Los “Insiders” constituyen una formidable amenaza; amenaza que es común. Aunque los Insiders hacen cosas por sus propias razones, son frecuentemente instrumentos de otros grupos.

3.2.5.9 Los empleados corrientes.

Los primeros y corrientes empleados pueden poseer las más destructivas amenazas que puedan encarar una empresa. Una de las cosas que hacen a ellos muy peligrosos es que son a menudo muy difíciles para descubrir o desenmascarar.

Los empleados que atacan a sus empleadores o jefes lo hacen por muchas razones: lo hacen por plata, por amor, y por ideologías políticas. Cuando la codicia es el motivo, las empresas que funcionan con grandes volúmenes de transferencia de fondos electrónicos automatizados, son muy frecuentemente objetivos o blancos de robo. El público en general, podría estar sorprendido del número de compañías que realizan estas clases de transacciones. Tiendas de venta al por menor, mercaderes directos, grandes vendedores, compañías de seguros, y firmas de inversión, entre otras, regularmente envían millones de dólares a través de computadores alrededor del mundo. **Los desfalcadores** crean falsas cuentas para mover dinero a cuentas privadas. Esto ha ocurrido en el pentágono, como en grandes compañías.

Hay algunos casos en donde un **espía** es colocado dentro de una empresa por un competidor (competencia). Algunas veces eso es realizado por objetivos de seguridad nacional, y el tal espía es un miembro de una agencia de inteligencia extranjera. Otras veces el espía estaría sirviendo a competidores domésticos y/o locales. Estos casos generalmente No son intencionales. Sin embargo, cuando compañías observan que sus competidores tienen ventaja de una posición, ellos algunas veces consiguen a alguien para aplicar a otras posiciones.

Esta persona tiene como tarea, descubrir toda la información que más pueda durante la entrevista. Algunas ocasiones, a una persona se le ofrece la posición, en algunos casos, el empleador ofrece pagar al empleado que sale para que siga dando información a la nueva empresa.

3.2.5.10 tipos de empleados que pueden ser una real amenaza.

Se encuentran los siguientes:

1. Empleados descontentos.
2. Empleados buscadores
3. Trabajadores partiendo
4. Antiguos empleados
5. No empleados “ON SITE”

1. **Empleados descontentos.** Algunos sienten que ellos merecían más reconocimiento y respeto de lo que sus empleadores mostraron hacia ellos. Un trabajador frustrado puede ser una amenaza real para una organización.

Los empleados descontentos son fácilmente manipulados por personas externas y son considerados un importante recurso entre los espías profesionales. Estos empleados cometen espionaje industrial por el propósito de satisfacer sus propios egos, buscan aprobación y respeto, y sus manejadores saben cómo darles eso a ellos.

Un buen espía –maestro- diría a los trabajadores descontentos que la gente tan importante e inteligente como ellos, pueden conseguir con sus manos cualquier cosa en la compañía. En muchos casos, empleados quieren lastimar a sus empleadores; ellos están mal en la compañía por una variedad de razones como:

1. No son bien pagados
2. Se encuentran trabajando en condiciones insatisfechas
3. No se la llevan bien con los compañeros
4. No gustan del jefe.

Entonces, lo que ellos quieren es venganza, entonces planean sus ataques meticulosamente y se enfocan en cómo castigar a sus empleadores de la mejor manera; en algunos casos, sus venganzas involucran vender información a la competencia y eso se manifiesta en los actos de sabotaje.

2. **Empleados buscadores**. Cometen espionaje, para romper la rutina de sus vidas aburridas, por simple deseo.

3. **Trabajadores partiendo**.- Otra versión de esta amenaza son los empleados quienes están dejando la compañía. Estas personas están algunas veces tentados para llevar favores con sus nuevos empleadores tomando o agarrando información muy importante antes de salir de sus empleos.

Estos trabajadores han asegurado una posición y quieren demostrar sus conocimientos y valores al nuevo jefe.

4. **Empleados antiguos**. Estos pueden ser una seria amenaza a la organización, ellos pueden buscar lastimar la organización posiblemente para impresionar al nuevo jefe.

Pueden lastimar a la compañía No intencionalmente, simplemente porque ellos saben que ellos la conocen. Aunque ellos no tengan acceso directo a la información más importante, conocen la composición de la empresa, los procedimientos, los hábitos y las fortalezas y debilidades de la empresa.

Las posibilidades las hay, ellos conocen las operaciones de la empresa mejor que algunos de los empleados actuales. ***Quizá lo más importante***, conocen la

competencia de la empresa, significa que ellos conocen y saben quién podrá valorar la información que ellos tienen de la empresa y pagar por ella.

5. **No. –empleados- "on-site**". Hoy en día, casi todas las organizaciones contratan algunos trabajadores temporales y en algunas organizaciones, estos trabajadores son más del 30% de todo el personal. Estos tienen acceso físico a la empresa.

Grandes compañías típicamente contratan empresas que hagan otros servicios para ellos, como servicios de celaduría. Estas grandes empresas no quieren invertir sus recursos en entrenamiento y mantenimiento de este grupo de trabajadores especializados, entonces, contratan a otros; es bueno para los negocios pero muy malo para la seguridad de la compañía.

3.2.5.11 amenazas de los diferentes tipos de empleados.

Para las compañías comerciales, hay amenazas como:

1. Sabotaje
2. Robo de propiedad intelectual
3. Robo de información de los clientes
4. Impactos de reputación
5. Pérdidas financieras directas.

1) **Sabotaje**. Este es comúnmente caracterizado por un empleado descontento con la empresa, quien fue despedido recientemente y ha decidido tomar algún tipo de acción en esperanza de que la compañía falle. Aunque la mayoría de los casos encaja en ese molde, no siempre es el mismo caso, los individuos también se pueden involucrar.

2) **Robo de propiedad intelectual**. Competidores con los EE.UU., pueden robar propiedad intelectual a un gobierno extranjero y esto es hacer espionaje económico, para aventajar a compañías en su propio país.

En este evento, las compañías necesitan trabajar despiadadamente y fuertemente para prevenir este tipo de robos.

Las tecnologías más vigiladas y espiadas son:

- Sistemas de información
- Sensores
- Aeronáutica
- Electrónica
- Armamento y materiales energéticos

3) **Robo de información de clientes.** Las Listas de los clientes son bien guardadas en las empresas, con esta información tan importante, la competencia puede acercarse a estos clientes y ofrecer a ellos descuentos en los mismos servicios.

4) **Impacto de reputación**. Una compañía no puede sobrevivir con una pobre y mala reputación.

5) **Pérdidas financieras.** El robo directo financiero es el tipo más obvio de perdida que puede ser causado por un infiltrado. Esto incluye:

- Fraude de tarjeta de crédito corporativo.
- Robo de materiales como: equipamientos, sobornos, contratos, subcontratos y servicios.
- Entre otros.

3.2.5.12. Casos de estudio.

Caso 1. Un programador con las contraseñas del sistema de la empresa USPA borra información de la nómina de pagos.

1) TEMA. un programador y oficial técnico de seguridad de la empresa USPA toma y borra información muy importante de la Base de Datos necesaria para el pago de nómina mensual, dos (2) días después de ser despedido.

2) FUENTE: Estado de Texas (U.S.A.) nombre: Donald Gene Burleson.

3) DETALLES: Donald Burleson trabajó como programador Senior y analista para USPA, una compañía de seguros en Folit Wortn Texas. La compañía tuvo cerca de 450 agentes empleados, y la mayoría fueron distribuidos alrededor del mundo.

Los agentes entraban su información de comisiones dentro del sistema de USPA cada mes, y pocos días más tarde se les paga un salario. Antes de ser despedido el 19 de septiembre de 1985, Burleson tuvo el rol de administrador para el sistema 38 de IBM usado para los cálculos de las comisiones. Por su posición estuvo informado de claves usadas por otros empleados para tomarse el Servidor.
Dos (2) días después que Burleson fuera despedido a las 8:30 am., un empleado de USPA chequeó el reporte de nómina para septiembre, y eso fallo, para completar porque algunos registros no pudieron ser encontrados. Los archivos logs fueron analizados y ellos indicaron que, extrañamente, algunos computadores en USPA (incluyendo el de Burleson) habían sido encendidos entre las 3:00 am., y 3:48 am de ese mismo día.

Pensamientos iniciales giraban en torno a Burleson, pero él tenía sus claves desactivadas cuando él fue despedido. A través de testimonios en la Corte, vino a colación que Burleson tuvo posesión de no menos de una clave extra en el edificio de la empresa. En el juicio él insistió que en esos días estuvo por fuera de la ciudad con sus hijos. Finalmente, Burleson fue encontrado culpable, un juez lo condenó de "acceso dañino" a un computador y fue sentenciado a siete (7) años de libertad condicional y US$ 11.800 de multa.

4) **ANÁLISIS**. Este caso hace énfasis de la importancia de manejar bien información de propiedad de la compañía como son las claves.

Mientras Burleson no devolvió su grupo de claves, la corte dio testimonio que otros empleados estuvieron declarando que él estuvo haciendo copias de respaldo para el mismo en esos días.

Raramente las compañías consideran las consecuencias de un empleado convirtiéndose en un infiltrado para hacer sabotaje con las claves a su disposición. Cuando el empleado Burleson fue despedido, todas esas claves debieron ser recuperadas por la empresa. Este entonces, es un caso de un empleado descontento con la empresa en cuestión.

Caso 2. Un programador lanza un ataque en línea de denegación de servicio (DoS) contra su empresa.

1) **TEMA:** Un programador está contrariado con su empresa porque no está de acuerdo en relación a unos bonos y extensión de contrato, entonces, el programador, se resigna y sabotea la compañía con una serie de ataques en serie de "denegación de servicios" (DoS).

2) **FUENTE:** U.S.A .Nombre: Abdelkader Smires.

3) **DETALLES**: Abdelkader fue un programador de base de datos en la empresa: Internet Trading Technnologies Corporation (ITTI), localizada en la ciudad de Nueva York. En el año 2000, ITTI estuvo procesando un número grande y considerable de transacciones de negocios en línea. El entonces, jefe oficial de desarrollo quien además, supervisor de Smires se retiró de la compañía el 6 de marzo, la compañía entonces, contrató consultantes para reemplazar al empleado que renunció, y le preguntaron a Smires y al otro programador para entrenar a los nuevos consultantes.

En un intento para mantener un medio ambiente estable, ITTI ofreció pagar a estos dos programadores grandes bonos en efectivo de US$7000 + US$50.000 en opciones de reserva y un (1) año de contrato. Inicialmente, en marzo 8 ellos aceptaron la oferta pero entonces cambiaron de opinión a los días siguientes.

Para estos dos (2) empleados, esta compensación no fue suficiente y ellos hicieron una contraoferta a la compañía ITTI, la compañía rechazó sus peticiones y unas horas después la compañía encontró su Red de Negocios bajo ataque desde un centro de copiado en Manhattan (N.Y.).

Estos ataques continuaron por tres (3) días seguidos; pronto investigadores rastrearon un punto de lanzamiento del ataque en un computador en el campus de la Universidad de Queens en Nueva York. Y se pudo testificar en 10 minutos después del ataque y saber quiénes estuvieron ahí en tiempo real.

4) **ANÁLISIS:** Unos US$5000 o US$6000 en diferencia en bonos no es probablemente la raíz del problema en este caso. Igual, después Smires aceptó una cantidad específica inicialmente, pero luego demandó más.

En un sentido, eso es como que ninguna cantidad podría haber sido suficiente. Hipotéticamente, es posible que Smires pudiera haber sentido que él estuvo muy cerca de la línea para la posición de su supervisor, y él puede haber sido lastimado cuando los consultantes que fueron contratados. El esperaba ser ascendido a supervisor pero eso es muy difícil decirlo. Esto demuestra la importancia de que tan cuidadoso debe ser el empleador cuando contrata, despide o transfiere empleados.

Caso 3. Los negocios de una compañía caen después que uno de sus empleados roba código fuente.

1) **TEMA**. Ellery Systems, INC. Sale de sus negocios cuando un empleado alega el haber vendido código de Software a una compañía China.

2) FUENTE: U.S.A.
Nombres: Liadsheng Wang Andrew Wang Jing Cut

3) **DETALLES**: Ellery Systems INC fue una pequeña compañia localizada en Boulder (Colorado), que diseñó y construyó dispositivos computacionales. Ellos fueron financiados por el Departamento de Defensa de Estados Unidos y la NASA para construir varias aplicaciones de Software.

Uno de los empleados de confianza fue un ciudadano chino llamado LIADSHENG WANG, mientras WANG trabajaba en Ellery, él agendó un viaje a China para “visitar a su madre enferma”. Unos días después el regresó, y él de repente renunció.

En una actividad completamente sin autorización, el día después, el código fuente que pertenecía a Ellery fue descargado a través de Internet por un amigo de WANG llamado JING CUT que también era ciudadano de China.

WANG confesó que él recibió US$550.000 de parte de una empresa “contraria por el gobierno chino llamada” BEIJING MACHINERY IMPORT & EXPORT (GROUP). En el momento de este crimen no había un estatuto en contra del espionaje corporativo y/o económico y los cargos fueron retirados. Ellery fue dejado sin nada. La compañía rápidamente quedó fuera de los negocios, y varios empleados sin su empleo.

4) **ANÁLISIS**: Por este caso, el antiguo oficial jefe ejecutivo de Ellery, el Ingeniero Gedfrey, estuvo “haciendo fuerzas” para la creación de una legislación en contra del espionaje económico.

Hoy en día, ya existe la legislación para casos de esta naturaleza. En esta situación, la actual descarga del código fuente ocurrió un día después que WANG renunciara. Después de su renuncia, su acceso debería haber sido limitado y las contraseñas cambiadas para proteger la propiedad intelectual de Ellery, que en este caso fue el código fuente del Software.

Caso 4. Antiguo empleado vende código fuente de su empresa a la competencia.

1) **TEMA**. Un antiguo empleado ofrece copias de Software propietario desde el repositorio “CYS” a la competencia.

2) **FUENTE**: EE.UU. – Timothy Kissane.

3) **DETALLES**. Timothy Kissane fue un ingeniero en la compañía: SYSTEM MANAGEMENT ARTS INCORPORATED” (SMARTS). La empresa SMARTS tuvo un producto que ellos llamaron INCHARGE diseñado para monitorear el estado de grandes redes de computadoras.

SMARST vendió este producto a empresas de Telecomunicaciones alrededor del mundo y mantuvo su código fuente guardado en secreto. Como otros empleados de SMARTS Kissane firmó un acuerdo legal, para mantener esto en secreto y no revelar esta información a nadie.
Kissane terminó en SMARTS en noviembre 28 de 2001; dos (2) semanas después de esta fecha, dos (2) competidores se acercaron a SMARTS e indicaron que ellos recibieron una oferta No-solicitada para la venta de información propietaria. Lo ofrecido había venido de un correo electrónico de una cuenta de Yahoo de “Joe Friday”. El correo ofrecía código fuente propietario, en particular, “Repositorio CYS de SMARTS INCHARGE”.

La transmisión del correo fue rastreado desde una librería en White Plains, Nueva York. Además, la cuenta de Yahoo fue accesada muchas veces desde la dirección del domicilio de Kissane en Lavallete, Nueva York. Finalmente, Timothy Kissane

fue encontrado culpable para lo que corresponde al robo de secretos de negocios, y fue sentenciado a dos (2) años de prisión y dos (2) años de libertad supervisada.

4) **ANÁLISIS.** Es muy difícil tener empleados que operan de manera eficiente sin libertad y confianza. Sin embargo, Kissane pudo haber intentado vender "su pieza" de trabajo. Cuando llega un desarrollo de Software, hay "espacio" de tecnología entre la conveniencia y la protección. Es decir, el empleado programador en este caso Kissane tiene la posible tentación de vender o tomar el camino de la lealtad a su empresa.

Caso 5. Empleado se va en contra de su compañía.

1. **TEMA**: El sujeto en este caso es un miembro importante de una compañía. Cuando él descubre que la compañía va a detener sus operaciones, este empleado pierde su lealtad y trata de obtener ganancias valiéndose del espionaje económico.

2. **FUENTE:** Nombre: Brent Alan Woodard.
   Empresa: Lightwaye Microsystems, Inc.

3. **DETALLES:** Brent Alan Woodard fue el director de tecnología de información en Lightwaye Microsystems, Inc; cuando la compañía anunció planes para parar operaciones al final del 2002, su lealtad terminó. Este cambio llevó a Woodard a robar secretos de negocios y ofrecerlos en venta a sus grandes competidores de la empresa.

Woodard realizó un espionaje económico, copiando información de Ligtwaye en cassettes. Entonces, estableció un alias de "Joe data" y envió un correo electrónico de la cuenta llghewaryedata@yahoo.com al competidor JDS-UNIPHASE. Cuando el jefe de tecnología en la empresa de JDS recibió el sospechoso correo, inmediatamente contactó al FBI, ellos clandestinamente tomaron las comunicaciones y comenzaron los "negocios" con Woodard. Mientras esto sucedía investigadores tomaron lugar y fueron capaces de ubicar el origen de los correos electrónicos desde la residencia de Woodard.

Con evidencia en mano, el FBI ejecutó una búsqueda en la casa de Woodard en diciembre de 2002, y una acusación fue hecha claramente después. En agosto del 2005, fue declarado culpable de "robo de secretos de la empresa" bajo la Ley USC 18 1832.

4. **ANÁLISIS**: Después que un empleado de una compañía sabe que esta cerrara pronto, hay una tendencia natural para perder la lealtad, cuando se declara que la compañía parará para siempre en el próximo año.

Este caso es una especial circunstancia que necesita ser manejada con gran cuidado y con gran supervisión de la protección de la información propietaria. Es una situación que puede causar en algún momento inesperado, como el caso de un director en una organización, volverse en contra de la compañía.

3.3. LAS DISTINTAS TÉCNICAS QUE UTILIZAN LOS GOBIERNOS PARA COMETER ESPIONAJE ECONÓMICO E INDUSTRIAL.

Los gobiernos de todo el mundo utilizan diferentes grupos especializados de personas para estas funciones de espionaje, entre estos grupos están:

a) **Guerreros de la información**. Son entidades nacionales que toman acciones estratégicas para las necesidades de sus naciones.

Estas personas son extremadamente buenas en lo que hacen. Estos grupos llevan a cabo sus metas estratégicas, tienen bien definidos los requerimientos y toman acciones para ganar ventaja estratégica a largo término, ellos toman su tiempo para hacer planes y cometer sus acciones.

Sobre el largo término, lo que estas entidades hacen es prepararse para la "guerra". Ellos se infiltran en infraestructuras extranjeras y planean tomar el control de los sistemas o dejarlos caídos en su propia discreción. Esta estrategia involucra la infiltración de ambos: infraestructura física e infraestructura del ciberespacio.

El núcleo computacional se ha convertido en un método primordial para algunos países para infiltrarse en las infraestructuras. Eso permite igual que pequeños países cometan guerra asimétrica. En las guerras tradicionales, el más grande y fuerte militarmente gana.

La meta de la guerra asimétrica es cometer actos sin contemplar la fuerza militar. En octubre del 2004, en Korea del sur, oficiales sur koreanos anunciaron que Korea del Norte colocó 500 personas a lo largo de cinco (5) años en un programa de entrenamiento para ejecutar guerra basada en los computadores. Este anuncio vino a raíz de una revelación del gobierno Sur Coreano, de que Sur Korea sufrió un ataque coordinado proveniente de Korea del Norte hacia sus sistemas de cómputo. Korea del Norte es relativamente nuevo en ese campo.

b) Colectores de inteligencia nacional. Aunque estas personas pueden trabajar en conjunto con los guerreros de la información, ellos tienen diferente motivación. Ellos son, además, parte de una inteligencia nacional o entidad militar.

Mientras que la información de guerra para estos expertos radica en determinar una infraestructura, los colectores de inteligencia continúan ejecutando ataques secundarios para recoger información y otras acciones.

Es cierto que los guerreros de la información necesitan recoger información para ejecutar sus acciones; sin embargo, la tarea es para que los recolectores tomen la información. Más de 100 países están desarrollando una habilidad en este campo. Aunque la mayoría de la gente en los EE.UU., cree que estos esfuerzos ponen en riesgo la información de la seguridad nacional, de hecho, ellos primeramente se interesaron en organizaciones e individuos.

El rango de motivaciones desde la piratería de Software a espionaje industrial. Su motivación es ayudar a la economía, NO su capacidad militar. De acuerdo a Gene Spafford, el director ejecutivo del centro para la educación e investigación en información y seguridad de la Universidad de Purdue, junto a Korea del Norte el más activo de los países en estos esfuerzos también se pueden incluir: China, India, Brasil, Korea del Sur, y Cuba. Pero también Rusia, Francia, Alemania e Israel deben estar en esta lista.

3.3.1 Países notables y sus esfuerzos de espionaje.

Rusia. Es el país emergente más fuerte de la desaparecida Unión Soviética. A pesar de la gran disponibilidad de recursos naturales y de su talento intelectual, la economía Rusa está en “confusión” y a pesar de la apariencia de que ahora es un país amigable, todavía permanece como el gran adversario de Estados Unidos.

Aunque muchos de los líderes de Estados Unidos muestran que la inteligencia de Rusia está más activa que durante la guerra fría, el mejor indicio viene del general Valentín Korabelnikov, el jefe del “Directorado principal de inteligencia” mejor conocido como el GRU.

Aunque mucho de la actividad de espionaje del país involucra inteligencia militar, la mayoría del enfoque de Rusia se ha movido al espionaje industrial. Antes de su salida, Boris Yeltsin declaró que la prioridad de la inteligencia de Rusia fue la inteligencia económica.

Virtualmente todos los negocios americanos son blancos potenciales de las agencias de inteligencia de Rusia. Aunque la KGB se dividió en varias agencias de inteligencia separadas con diferentes funciones, la inteligencia rusa permanece viva y latente. La mayoría de las actividades familiares de la KGB a americanos fue asignada a una organización conocida como la SYR. Esta organización continua usando recursos de la KGB y espía redes que han sido desarrolladas en décadas. La GRU, cual es considerada igual o más “diabólica” que la KGB, se ha mantenido intacta a pesar de algunos problemas políticos y se mantiene todavía fuerte.

Los nuevos rusos capitalistas se dieron cuenta que robar tecnología es mucho más barato que desarrollarlo por ellos mismos. Ellos además, tienen los mecanismos de distribución para vender bienes hechos con tecnología pirateada o robada. Porque ellos además tienen un control significante del gobierno ruso.

Hoy en día, a pesar de su anterior enfoque en actividades militares, la agencia de inteligencia de la Rusia moderna utiliza un modelo decididamente capitalista para la recolección de información. A través de auspicios del Ministro de Defensa, la inteligencia Rusa genera un documento donde identifica cada requerimiento de las agencias de inteligencia. Este documento vital de inteligencia es dividido en cuatro (4) partes principales:

1) Estructura política
2) Estructura militar
3) Estructura industrial
4) Colección de requerimientos

La estructura política se enfoca en los Estados Unidos y las infraestructuras políticas del mundo. La estructura militar es muy cercana a la estructura política, excepto que se enfoca en mirar el personal de la organización.
La estructura industrial identifica todos los negocios que pueden ser de importancia militar o política al gobierno ruso. Las agencias de inteligencia rusas mantienen listas de negocios en Estados Unidos por sectores de mercado, el tipo de información que cada compañía podría tener y personas clave de la compañía en cuestión.

Compañías de todos los tamaños tienen algo para ofrecer a las agencias de inteligencia de Rusia, el proceso de espionaje industrial ruso es muy efectivo y de alta ganancia. Estas personas son muy buenas en conseguir exactamente de lo que ellos quieren de compañías estadounidenses. Aunque, la economía de Estados Unidos no irá a “desmoronarse” por estos ataques, ciertos negocios e industrias podrían sufrir drásticamente.

Es extremadamente importante notar que el GRU tiene uno de los grupos más avanzados en habilidades de Hacking de computadores del mundo. Ellos probablemente rivalizados solamente por los centros de información de guerra de los Estados Unidos. Ese hecho es especialmente importante porque el grupo es responsable por preparar estratégicamente para la guerra.

El GRU probablemente ha colocado el “trabajo en tierra” para causar que estos sistemas choquen o de otra forma causar inmenso daño.

China. Tiene una de las más grandes economías del mundo. A pesar de la carencia aparente de expansión de tecnología hacia afuera del país. China está enfocada en la adquisición de nuevas tecnologías para traerle a su economía. El

gobierno chino está buscando una serie de reformas a su economía para permitir la expansión extranjera dentro del país.

Sin embargo, en contraste a Rusia, China no está buscando simultáneamente reformas políticas. El espionaje industrial siempre ha jugado un rol importante en el desarrollo de la economía China. Por algunos años, China ha usado su capacidad de inteligencia militar y tácticas para objetivos económicos. Sin embargo, las tácticas chinas son diferentes de las rusas.

Expatriados rusos a menudo No mantienen un fuerte lazo con un país, ellos pelean duro para escapar. A pesar de la represión del gobierno, una sociedad totalitaria, la gente de China descendiente frecuentemente siente la devoción étnica hacia sus ancestros y su tierra (China).

Entonces, las agencias de inteligencia China conocen esto (devoción étnica) y luego explotan esta devoción en cada oportunidad que puede. Las agencias de inteligencia china enfocan sus esfuerzos de reclutamiento en chinos nacionales viajando y viviendo fuera del país, como también gente de descendientes chinos que son ciudadanos de otros países. Ellos encuentran esas personas principalmente a través de clubes sociales, y grupos para ciudadanos chinos.

Las agencias de inteligencia “cuentan” con amistades que son agentes potenciales y tratan de reclutar a ellos en actividades de espionaje. No todos los nacionales chinos viajando, estudiando o trabajando en el extranjero son agentes de inteligencia. Pero China considera a ellos como un recurso primario para el “espionaje económico”, y con muchos ciudadanos chinos alrededor del mundo, las agencias de inteligencia necesitan explotar solamente un pequeño porcentaje de ellos para poner en amenaza a las compañías de Estados Unidos.

Como los rusos hacen, los chinos usan satélites espías, barcos espías, aviones, y monitoreo telefónico en sus actividades de recolección de inteligencia, los chinos tienen una de las redes de espionaje más grandes del planeta y esta va cada vez en alza, ellos utilizan muchos recursos de espionaje.

Francia. Ha sido dos (2) veces públicamente identificado por la CIA como uno de los dos (2) aliados de Estados Unidos que cometen actos de espionaje corporativo en contra de compañías norteamericanas como frecuentemente hacen los adversarios de Estados Unidos. El gobierno francés ha estado usando su capacidad de inteligencia para apoyar sus negocios domésticos desde el reinado de Luis XIV.

Compañías francesas regularmente se aproximan a el DGSE (la agencia de inteligencia de Francia) y solicitan apoyo de inteligencia. Cada compañía debe justificar su solicitud con criterio específico financiero. Si la DGSE considera la

solicitud válida, entonces se usan esos recursos para conseguir la información deseada.

Las actividades de espionaje de Francia no solo se limitan al territorio francés. Porque Macron ha dicho que Francia exitosamente ha colocado espías dentro de algunas compañías de Estados Unidos, incluyendo IBM y Texas Instruments. Hay cargos operativos para largo plazo, esperados para avanzar a través de los Rankings de la compañía y obtener acceso a los más recientes desarrollos del momento.

Francia ha probablemente puesto el ojo en compañías no norteamericanas también. Francia tiene la distinción de apoyar activamente la comunidad de Hackers de computadoras. Francia ha largamente reconocido la importancia del Hacking computacional y entrenado a un grupo de clase mundial de Hackers de su propiedad.

Francia además, apoya a otros Hackers, principalmente para ayudar a esconder sus propias actividades y recoger información. El doctor Spafford (de la Universidad de Purdue) dijo que Francia además encuentra nuevas vulnerabilidades computacionales y se las entrega directamente a la comunidad de Hackers; esto permite a los Hackers usar muchas técnicas avanzadas, mientras inadvertidamente enmascaran las actividades ilegales del DGSE. Si el Hacker promedio puede comprometer un sistema computacional con un avanzado ataque, entonces, las compañías hackeadas por Francia asumen entonces, que el ataque vino de un Hacker adolescente en vez de un bien entrenado Hacker de la DGSE.

Israel. Israel comparte con Francia la distinción de ser nombrado por la CIA como uno de los dos (2) líderes aliados perpetradores de espionaje económico e industrial. En contraste con Francia, los israelíes prefieren mantener sus actividades de espionaje bajo cuerda. Ellos son muy dependientes de los EE.UU. por apoyo político y militar.

Con relación a algunas fuentes de inteligencia, Israel tiene la mejor y mayor capacidad de inteligencia del mundo, persona a persona. Fuentes confiables creen que los israelíes tienen la tercera mejor agencia de inteligencia del mundo después de EE.UU., y Rusia. El espionaje primario de Israel es la parte de tecnología militar, Israel quiere armas avanzadas para mejorar su habilidad de defenderse y venderlas a sus aliados. Israel siempre busca fortalecer su economía y conseguir un balance en el comercio.

Para obtener información, Israel usa algunas de las mismas técnicas que son a menudo asociadas con países más hostiles, por ejemplo: Israel coloca personas dentro de las compañías a través de negociaciones contractuales justo como China lo hace. Ellos reclutan espías e infiltrados.

Como Francia, la inteligencia Israelí ha tenido significante éxito en reclutar hackers de computadoras. El “Mossad” y probablemente el “Lakam” ambas de la inteligencia Israelí tiene hackers y apoyan las actividades de hackeo tanto como la DGSE y ocasionalmente tratan de reclutar más hackers talentosos.
Israel tiene una increíble base de datos de profesionales de la computación. Además, Israel es casa de algunas empresas vendedoras de seguridad computacional.

Alemania. Alemania es ampliamente conocida para estar entre las más colectoras de inteligencia activas en el mundo, mantiene una organización muy grande de inteligencia llamada la BND, aunque su primer enfoque fue el bloque Este, la BND siempre ha estado relacionada en una gran cantidad de actividades industriales.

La BND continúa monitoreando las comunicaciones internacionales y trata muy activamente de obtener información que pueda ayudar a las empresas alemanas.
La agencia ha apoyado a SIEMENS, una de las compañías más grandes de Alemania, infiltrando alta tecnología de compañías alrededor del mundo. No hay la duda que BND ha estado involucrada en varios hechos de espionaje económico.

Al igual que la DESE, la BND tiene un sistema muy completo de Hacking computacional. El proyecto RAHAB es un esfuerzo de la BND para hackear dentro de las redes de las computadoras y sistemas comprometidos en la infraestructura de la información global. Eso comenzó a inicios de los años 90´s y continúa hasta este punto; este RAHAB quiere desarrollar la capacidad de irrumpir el sistema computacional corporativo y/o del Gobierno.

Japón. Quizás ningún país ha integrado espionaje industrial dentro de su cultura. Los negocios de Japón miran siempre a su competencia en ambas formas: Doméstica y en el extranjero. Las más grandes compañías tienen unidades enteras observando la inteligencia de la competencia.

Como el espionaje industrial está embebido dentro de la forma de funciones del Gobierno, casos demuestran como ninguna compañía japonesa es afectada por ejemplo: La compañía Pillsbury descubrió que después de pasar una aplicación de una patente, el Ministerio de Economía, Industria y Comercio (MII) pasó la aplicación de la patente a la Asociación de la Industria y Comercio. La información de Pillsbury fue básicamente distribuida a su competencia antes que la compañía pudiera protegerla como suya. De igual manera, Japón es un importante aliado de EE.UU., y este representa una significativa amenaza para las empresas de Estados Unidos.

Irán. Irán ha saltado a una alta posición en eventos recientes, es casi seguro que Irán está tratando de desarrollar más capacidad en armas nucleares.

Hay indicios de fuentes confiables que muestran que el Gobierno iraní tiene algunas interacciones con Al-Qaeda. Irán está activamente tratando de manipular eventos en Irak y tiene un grupo grande de inteligencia actuando en conjunto hacia la meta.

Irán gasta las ganancias del petróleo en una despiadada búsqueda en tecnología de armas avanzadas, incluyendo armas nucleares, químicas y biológicas. Irán tiene una de los más financiados grupos de inteligencia en el mundo.

Irán para obtener ciertas tecnologías, asegura la cooperación de las empresas aliadas a Estados Unidos, como Alemania y Francia. Estas compañías tienen su propia tecnología y no son sujetas a reglas que limiten la adquisición de equipo "controlado". Consecuentemente, estas compañías están disponibles para usar su estatus aliado y para adquirir tecnología supuestamente por ellos mismos y entonces, y la venden legalmente a Irán.

Irán usa estas compañías como intermediarias para realizar sus actividades. Científicos iraníes especifican sus requerimientos, y cuando el dinero no es el objetivo primordial, entonces ellos consiguen lo que quieren. Aunque el uso de Irán de tecnología parece ser limitada a la ganancia No-económicas, sus actividades de espionaje ponen en una gran amenaza para compañías de Estados Unidos y el mundo en general.

Cuba. Cuba está en lo alto de la lista de países involucrados en espionaje industrial. En contraste con Irán, cuba es un país de tercer mundo con una economía tercermundista. Con el rompimiento con la unión soviética, cuba ha perdido su principal apoyo en relación con dinero y tecnología, cuba igualmente ha perdido una base militar rusa.

Además de Estados Unidos, otros países han evitado involucrarse económicamente o tener relaciones económicas con cuba. Aunque algunos países están claramente negociando con cuba, el efecto es mínimo en la economía cubana, haciendo que el crecimiento de la economía sea muy mínima. La necesidad de cuba en la administración del gobierno de Fidel Castro se enfocó en lo militar que en el crecimiento de la economía, con la adquisición de tecnología.

En relación a los recursos de cuba para cualquiera significaría ser más importante adquirir nueva tecnología. Como con Irán, los operativos de la inteligencia cubana son entrenados por rusos. Usando su educación, ellos tratan de infiltrarse en las compañías y empresas para robar tecnología. Ellos además sobornan a la gente, interceptan llamadas telefónicas, cometen "blackmail" y reclutan simpatizantes comunistas.

Ellos además usan compañías extranjeras para evitar el embargo del comercio cubano. En algunos casos, los cubanos han adquirido tecnologías para comerciar con sus aliados y amigos. Los robos cubanos de tecnologías de Estados Unidos impactarían significantemente el mercado compartido con firmas de EE.UU. sin embargo, cuba es el mayor abastecedor al mercado negro. El efecto sobre la economía es mínimo, pero eso puede lastimar a compañías americanas individualmente, dependiendo en la tecnología especifica que ellos adquirieron.

India. India es un país del Tercer Mundo, aunque claramente tiene centros tecnológicos de excelencia, la mayoría del país es extremadamente muy pobre, tiene una población muy numerosa y sus recursos económicos son escasos, pero tiene algo muy bueno y es que está basado en su educación que en algunas áreas es muy sobresaliente a nivel mundial.

India, tiene mucho a su favor. El hecho de que fue una de las primeras colonias británicas significa que mucha gente habla inglés. Aunque solamente un pequeño porcentaje de la población tiene educación universitaria, eso representa un gran número de personas. Del hecho de que el estándar de vida en el país es generalmente bajo significa que puede ofrecer trabajo en tasas muy bajas. Por estas razones combinadas, India es uno de los beneficiarios primarios del “Offshoring” y “Outsourcing”.

India además, tiene un gran esfuerzo por el espionaje. Por una variedad de razones políticas, sus agencias de inteligencia han sido apoyadas por servicios de inteligencia británicos y rusos. Eso ha desarrollado una mentalidad similar a la francesa: “Lo que es mejor para los negocios nativos, es mejor para el país”. El espionaje económico, es “Integral”, pero escondido y es parte de hacer negocios.

Algunos indios están viviendo y atendiendo el colegio en los Estados Unidos, quienes tienen mucha devoción a su país: India como también los chinos lo tienen por su país. Por esta razón, hay inmensos beneficios para algún ciudadano de la India que robe tecnología de empleadores de Estados Unidos y traer ellos a India para comenzar una nueva empresa.

El crecimiento del “Offshoring” y “Outsourcing” en las industrias en India ha sido de gran ayuda para sus esfuerzos de espionaje, esto quiere decir que al dar servicios de outsourcing a empresas de EE.UU. por ejemplo, estas compañías de la india pueden infiltrarse en toda la información de la empresa que los contrato y así entonces poder obtener información relevante de dicha empresa.

3.4 ENFOCAR EL PROBLEMA DE ESPIONAJE ECONÓMICO E INDUSTRIAL EN COLOMBIA

Espionaje económico. Con relación al espionaje económico, Colombia es un país que no tiene casi antecedentes en el ámbito del espionaje entre países. Pero

ha habido unos hechos entre Colombia con Venezuela y Ecuador respectivamente, que fueron considerados como “hechos de espionaje”.

En general, Colombia es un país en vías de desarrollo y por lo tanto, no tiene muchas invenciones en tecnología y otras áreas de la ciencia, y por lo tanto, no es tan espiado como países desarrollados tales como: Estados Unidos, Alemania, China entre otros.

3.4.1 Posible espionaje de Venezuela en Colombia

A raíz de la crisis del Gobierno venezolano, se han entregado más de 700 militares de Venezuela al gobierno colombiano, y muchos de ellos dicen que hay espías infiltrados en Colombia provenientes de Venezuela.

El periódico el Tiempo de Colombia, conoció y publicó un artículo en el 2018, donde se anuncia que organismos de inteligencia colombianos le atribuyen al CEOFANB (Comandos estratégicos operacional de las fuerzas armadas de Venezuela), un posible despliegue de las redes de inteligencia venezolana sobre Colombia, para llevar a cabo operaciones encubiertas con relación al tema militar y a las amenazas que provienen de Estados Unidos y Colombia.
También se dice por parte de organismos de la inteligencia colombiana que hay al menos 50 miembros del SEBIN repartidos en 8 regiones de Colombia. Estos dos (2) grupos: EL CEOFANB y EL SEBIN (servicio Bolivarianos de Inteligencia Nacional), están enfocados a controles y seguimientos de algunos opositores de Maduro que viven refugiados en Colombia. Como también llevarles seguimiento a miembros que tienen misiones diplomáticas contra el gobierno de Nicolás Maduro.

Existe evidencia de que planes de espionaje en Colombia aumentaron cuando el presidente de Colombia Iván Duque se puso al frente del grupo de países que exigen la salida inmediata del dictador Nicolás Maduro.
Fuentes de inteligencia colombiana afirman que el SEBIN y algunos grupos Chavistas tienen alianzas con sectores que apoyan al régimen de Nicolás Maduro, para crear escenarios de crisis en Colombia.

Finalmente, Colombia ha expulsado al menos 12 espías infiltrados y a órdenes del régimen de Nicolás Maduro. Pero todavía la situación es preocupante, y se teme un posible atentado contra el presidente colombiano Iván Duque.

3.4.2 Posible caso de espionaje en conjunto entre Ecuador y Colombia.

Este fue un caso de espionaje militar en cooperación entre ambos gobiernos de Colombia y Ecuador, para investigar y dar con el lugar de donde estaban las FARC sobre el territorio ecuatoriano, y en la cual después se ordenó por parte del presidente de ese entonces Álvaro Uribe, de bombardear el lugar donde se

encontraban las FARC en ese momento y en la cual resulto un éxito porque falleció el segundo jefe de esa guerrilla el comandante: Raúl Reyes.

Espionaje industrial. En Colombia se han presentado diversos casos de espionaje industrial o corporativo entre empresas nacionales como extranjeras.
Hay varios casos relevantes en los últimos años, como en el caso de HYUNDAI, empresa Sur Coreana de automotores ocurrida en el año 2016.

Según un artículo de la página web colombiadigital.net del año 2018 en los últimos años se han conocido 3 incidentes a amplia escala como fueron los ataques:

- STUXNET
- DUQU
- FLAME

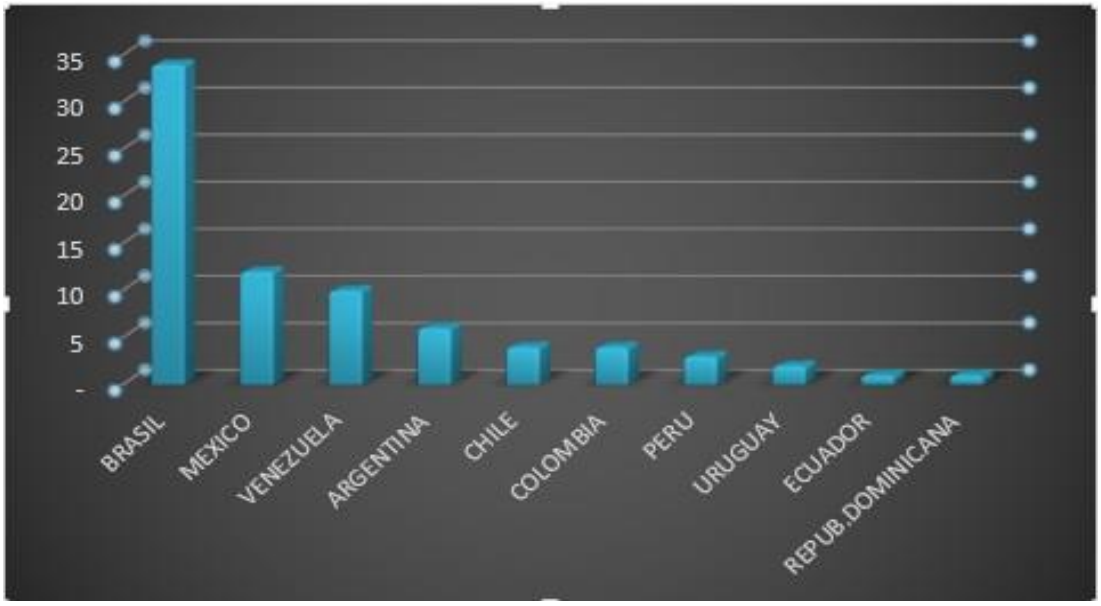
Que son fuertes códigos maliciosos (Malware), dirigidos contra plantas industriales que están en el Medio Oriente y Europa, con la finalidad de capturar información corporativa importante. Y también para saboteo. En América Latina ciberataques de esta dimensión No ocurren, porque no hay una infraestructura crítica para afectar, pero si han detectado ciberataques con el fin de robar información corporativa.

En Latinoamérica son más frecuentes los ataques de ciber espionaje dirigidos contra organizaciones privadas que contra Organizaciones Gubernamentales. Estos ataques no son tanto por el ciberespacio sino por medio de infiltraciones menos complejas o empleados fraudulentos que están dentro de la empresa como también aquellos que abandonan las empresas ya sea por haber sido despedido o de renuncia voluntaria.

En estadística el 51% de las compañías Latinoamericanas han sufrido alguna clase de ataque relacionado con código malicioso (Malware) durante el último año (2017), según un reporte ESET SECURITY. En el documento también se destacó que Colombia, Brasil, Ecuador, Bolivia, Perú y Venezuela se colocaron por encima de la media ponderada de la región (Latinoamérica).

Colombia es a menudo menos afectada por ciberataques que los Estados Unidos, pero es uno de los países con mayor tasa de crímenes cibernéticos en América Latina, actualmente ocupa el quinto puesto en Latinoamérica en relación a información del año 2017. El Malware o código malicioso es la modalidad que prefieren los cibercriminales para el hurto de información confidencial en el interior de las empresas colombianas.

Figura 18 Ciberataques en la Latinoamérica en 2017



Fuente: LAROTTA, Santiago. CRIPTOMONEDAS, el terreno en el que más crecen los ciberataques. [consultado: 30 de Agosto de 2018]. Disponible en internet: http://www.simbiosystemas.com/2018/04/15/criptomonedas-el-terreno-en-el-que-mas-crecen-los-ciberataques/

En Colombia el robo de la información y datos de las compañías y empresas ocurren diariamente, donde muchas veces pasa desapercibido. Este problema más el fraude en el proceso de adquirir activos físicos es mostrado como uno de los fraudes que genera grandes pérdidas en las compañías colombianas hoy en día. En relación a una encuesta global sobre el fraude, realizado por la empresa KROLL, el 18.9% de las empresas en Colombia han sido afectadas por esta clase de delitos, la cual es una cifra que causa mucha preocupación. Según la policía nacional de Colombia, los ciber-delitos en general, le han producido perdidas de alrededor de 6.49 Billones de pesos colombianos a las compañías nacionales.

En Colombia, los estragos del ciberespionaje no es solamente de índole económica, la mayoría de las empresas que han sufrido de espionaje industrial piensan que si lo denuncian y lo dan a conocer entonces, podría afectar “la imagen” de la empresa, porque podrían mostrarse como muy vulnerables y débiles en materia de seguridad y posiblemente podrían volver a ser atacados por hackers o ciber-criminales. Por esta razón de inseguridad de actuar de las empresas es que no llegan estos casos de espionaje corporativo a las autoridades locales de Colombia. Casi siempre los directivos de estas empresas atacadas optan por la “discreción” en lugar de mostrarlo al país y al mundo.

Espías colombianos. En Colombia, donde la tecnología de punta solo se limita a algunos campos, los espías no hacen sus ataques hacia campos de la investigación y la manufactura de nuevos productos. Los espías en Colombia se enfocan más en el mercadeo y las formas de piratería comercial y las actividades del contrabando.

Un caso de una empresa colombiana que se dedica a la fabricación de ascensores, que debido a no tener una buena política de seguridad, fue afectada con el hurto de información muy importante. Unos empleados salientes que cometieron el hecho se pasaron a la competencia. Consecuencia de esto, a los pocos meses las ventas de la empresa de ascensores bajaron en un 30%, mientras que en el competidor se incrementaron. Pero donde la filtración de la información juega un papel clave es el negocio de la publicidad, por ejemplo, COCA-COLA, se dio cuenta que cada vez que estaba a punto de lanzar una promoción, su rival PEPSI hacía lo propio.

Lo mismo pasó entre COMCEL y CELUMOVIL en su momento, con relación a sus promociones y planes ofrecidos. Como también el caso de las empresas Farmacéuticas que lanzan al mercado productos genéricos muy similares a los de sus competidores. Colombia, prácticamente ha comenzado a meterse en el apasionante mundo de la inteligencia de mercadeo empresarial. Actividades de espionaje industrial pasan todos los días y en cualquier clase de empresa.

Caso HYUNDAI. Este caso sucedió en el año 2015. Entre HYUNDAI Colombia Automotriz S.A y HYUNDAI Motor Company que es la casa matriz Sur Coreana. Hoy en Colombia hay 9.143 vehículos nuevos represados en Zonas Francas sin ser vendidos en Colombia, esta es una restricción Aduanera como medida cautelar por un Juzgado en Colombia, mientras llegan a un arreglo ambas partes.

El principal damnificado con la medida cautelar fue NEOCORP, empresa colombiana que se asoció con el grupo Ecuatoriano ELJURY; cuando HYUNDAI Corea rompió lazos con HYUNDAI Colombia, NEOCORP y ELJURY pasaron al lugar de HYUNDAI Colombia. La cuestión del espionaje industrial es que Gustavo Lenis (exempleado de HYUNDAI Colombia) entregó información confidencial al Grupo ELJURY hasta lograr que HYUNDAI Corea terminara el contrato con HYUNDAI Colombia S.A.

Lenis, trabajó como Vicepresidente Ejecutivo de HYUNDAI Colombia Automotriz S.A., y luego al dejar el cargo filtró información al Grupo ELJURY del Ecuador. Luego de este incidente la casa matriz Coreana HYUNDAI rompió lazos con la empresa HYUNDAI Colombia Automotriz S.A., y se presentó una demanda de HYUNDAI Colombia a HYUNDAI Corea (la casa matriz).

HYUNDAI Corea dejó claro que no le interesa hacer negocios con HYUNDAI Colombia y esta última dice que merece indemnización por esa “terminada”

repentina de los lazos comerciales. En realidad, la empresa HYUNDAI Colombia S.A., no tiene culpa de que el Ex-empleado Gustavo Lenis haya infiltrado información a la compañía ecuatoriana ELJURY después que dejó el cargo como Vicepresidente de la Empresa.

Figura 19 Controles en Latinoamérica de los ciberataques en el 2016

Fuente: LA RAZON. Latinoamérica es 'altamente vulnerable' a ciberataques. [consultado: 1 de Abril de 2019]. Disponible en internet: http://www.larazon.com/suplementos/el_financiero/Latinoamerica-altamente-vulnerable-ciberataques_0_2474752564.html

Como se puede ver en la gráfica, los países de América Latina y el caribe carecen de buenas políticas de seguridad para que puedan controlar y contra restar ataques desde el internet, solo 6 países tienen algunos controles de seguridad en Latinoamérica y ellos son:

- Brasil
- Colombia

- Jamaica
- Panamá
- Trinidad y Tobago
- Uruguay

Que están en un nivel medio de desarrollo muy lejos todavía de los países desarrollados como: EE.UU. Israel y Corea del Sur. El enfoque futurista del **espionaje económico** en Colombia en los próximos años o décadas no va a ser tan “ACTIVO” en materia de espiar a otros países o ser espiado por otros.

El espionaje económico se enfocaría más en un espionaje de tipo militar y político de países vecinos de la región tales como: Venezuela, Cuba, y Ecuador. No olvidando que Cuba es uno de los países que más espía en la región y que tiene fuertes nexos con el gobierno de Venezuela, y que los ha tenido por largo tiempo. Sería un espionaje de poder adquirir información importante de Colombia para pasarla a otros países, como en el caso actual con Venezuela, de los espías del SEBIN en territorio colombiano.

El enfoque futurista del **espionaje industrial o corporativo** en Colombia podría ser de gran crecimiento en los próximos años venideros debido a varios factores tales como:

1. **El crecimiento y expansión de las redes computacionales** y el desarrollo del Software, en aplicaciones maliciosas (virus y malware).

2. La falta de organismos que brinden apoyo en la ciber-seguridad para las empresas en los diferentes sectores comerciales en Colombia. Cuando haya más control de la seguridad, se disminuirían los ataques de espionaje corporativo.

3. Con la llegada de nuevas empresas y compañías a Colombia, esto podría incrementar la competencia entre ellas y así llevar a algunas empresas a “tratar” de espiar a su competencia, ya sea por el ciberataque o ingeniería social dentro de las mismas.

4. CONCLUSIONES

1. El inicio del espionaje en los pueblos, estados y reinos en la época antigua se dio debido al interés de mejorar su economía y así su estándar o nivel de vida adquiriendo nuevas tecnologías en diferentes áreas.

2. El espionaje económico o entre estados en la época antigua se dio en realizar espionaje sobre el correo y la correspondencia entre reinos principalmente, buscando información relevante y útil en toda la correspondencia obtenida.

3. Las técnicas de ciberataques que los delincuentes utilizan actualmente han venido evolucionando en paralelo con el desarrollo de la tecnología computacional en los últimos años.

4. Los ataques corporativos han venido aumentando en los años recientes a una tasa de 31% anual debido principalmente al poco control de la seguridad en las compañías y/o empresas, viéndose más en las compañías en países de Latinoamérica.

5. El número de países que cometen espionaje económico ha venido en alza en los últimos años, esto debido al desarrollo de las comunicaciones y a las nuevas tecnologías de software.

6. Algunos países tales como: china e india principalmente, utilizan a sus ciudadanos que están radicados en el exterior estudiando o trabajando como en Estados Unidos, para utilizarlos y aprovecharlos como espías y así poder colaborar con sus países de origen enviando información clave.

7. Colombia es un país en vías de desarrollo y por tanto la actividad de espionaje económico es casi nula dirigida hacia este país, en los años recientes se ha visto un tipo de espionaje político hacia Venezuela a través de Colombia que sirve como puente la cual es realizado por los países de EE.UU. y Rusia principalmente.

8. En Colombia hay bastantes casos de espionaje corporativo o industrial, se han visto empresas de diferentes sectores que espían a su competencia de muchas maneras, y este podría ir en alza debido al poco control que las empresas aplican a su propia seguridad de su información, dentro como fuera de ella.

9. A medida que se desarrolla la tecnología en el área de software y hardware, la tendencia de los ciberataques aumenta y cada vez son más precisos y dañinos.

10. Algunos países tales como: Francia, Rusia, Israel, Irán entre otros, subsidian y dan apoyo a grupos de hackers para entrenarlos y así poder utilizarlos como herramientas para el espionaje económico o entre países.

11. El desarrollo de la tecnología ayudó al desarrollo de las técnicas de espionaje ya sea corporativo como también del espionaje económico, desarrollándose bastante desde el comienzo de la guerra fría entre la ex URSS y los Estados Unidos hasta nuestros días.

12. La educación es un punto muy importante para poder tomar conciencia de la importancia de los riesgos que llevaría el espionaje ya sea corporativo o económico sobre empresas o estados, y así poder prepararse para futuras amenazas.

REFERENCIAS BIBLIOGRÁFICAS

ABC Internacional. La evolución del espionaje en la Historia: la profesión más Antigua del mundo.[en línea]. Madrid. (11 de abril de 2013). [Fecha de consulta: 15 de noviembre de 2018]. Disponible en: https://www.abc.es/internacional/20131104/abci-evolucion-espionaje-historia-201310311329.html

BURGESS, Christopher. Secrets Stolen, fortunes lost: preventing intelectual property theft and economic espionaje in the 21st century. Burligton. Syngress publishing. 2008. 357 p

COLOMBIA DIGITAL. Espionaje industrial: una realidad incómoda [en línea]. Colombia digital. Bogotá. (3 de mayo del 2013). [Fecha de consulta: noviembre 12 de 2018]. Disponible en: https://colombiadigital.net/actualidad/articulos-informativos/item/4852-espionaje-industrial-una-realidad-incomoda/4852-espionaje-industrial-una-realidad-incomoda.html

DURAN, Diana. Líos y más líos: así se resume el caso Hyundai. [en línea]. El Espectador. Bogotá. (15 de octubre de 2016). [Fecha de consulta: 11 de noviembre de 2018]. Disponible en: https://www.elespectador.com/noticias/judicial/lios-y-mas-lios-asi-se-resume-el-caso-hyundai-articulo-660596

ECURED. KGB. [en línea]. Ecured. La Habana. (15 de marzo de 2015). [Fecha de consulta: noviembre 12 de 2018]. Disponible: https://www.ecured.cu/KGB

FIALKA, John. War by other means: economic espionage in America. New York. ww. Norton & company. 1997. 242p

FINK, Steven. Managing the global risk of economic espionage. Chicago. Dearborn trade books. 2002. 353p.

JAVERS, Eamon. Broker, trader, lawyer, spy: the secret world of corporate espionage. New York. Harper-collins publishers. 2010. 306p

LA INFORMACIÓN. Desvelan el secreto del KGB en la Guerra fria para detector a los agentes de la CIA.[en línea]. La Información. Madrid. (25 de febrero de 2016). [Fecha de consulta: 13 de noviembre de 2018]. Disponible en: https://www.lainformacion.com/politica/espionaje-e-inteligencia/desvelan-el-secreto-del-kgb-en-la-guerra-fria-para-detectar-a-los-agentes-de-la-cia_pnAnceCrFjcJknwo0TcbZ/

LA NACIÓN. Del imperio Romano a la NSA: la historia del espionaje internacional. [en línea]. La Nación. (3 de noviembre de 2013). [Fecha de consulta: el 13 de noviembre de 2018]. Disponible en: https://www.lanacion.com.ar/1635104-del-imperio-romano-a-la-nsa-la-historia-del-espionaje-internacional

LUTZE, Heather. Marketing espionage: how to spy on yourself. Your prospects and your competitors to dominate online. Parker,CO. Findability press. 2016. 211p.

NASHERI, Hadieh. Economic Espionage and Industrial spying. Cambridge. Cambridge University Press. 2005. 287p

PENENBERG, Adam. Spooked. Espionage in corporate America. New York. perseus publishing. 2000. 205p

QUIEN.NET Redacción Quien, Biografía de Edward Snowden. [en línea]. Quien.NET. México DC. (3 de junio de 2013). [Fecha de consulta: 15 de Octubre de 2018]. Disponible: https://www.quien.net/edward-snowden.php

REVISTA SEMANA. Espías S.A. [en línea]. Revista Semana. Bogotá DC. (23 de Octubre del 2000). [Fecha de consulta: 11 de Noviembre de 2018]. Disponible en: https://www.semana.com/economia/articulo/espias-sa/43741-3

REVISTA SEMANA. Quien espía en Colombia?. [en línea]. Revista Semana. Bogotá DC. (21 de Julio de 2003). [Fecha de consulta: 13 de Noviembre de 2018]. Disponible en: https://www.semana.com/nacion/articulo/quien-espia-colombia/59460-3

VELASCO, Jaime. La máquina Enigma, el Sistema de cifrado que puso en jaque a Europa. [en línea]. Hipertextual. Madrid. (12 de julio de 2011). [Fecha de consulta: 15 de Octubre de 2018]. Disponible en: https://hipertextual.com/2011/07/la-maquina-enigma-el-sistema-de-cifrado-que-puso-en-jaque-a-europa

WINKLER, Ira. Corporate espionage: what ii is, why it´s happening in your company. Rocklin CO. Wiley publishing. 1999. 365p

WINKLER. Ira. Spies among us: how to stop the spies, hackers and criminals you don´tr even know you encounter every day. Indianapolis. IN. 2005. 326p