La colección de ensayos ACAPOMIL tiene por objeto poner a disposición de los oficiales de Ejército y del público en general, textos que signifiquen un aporte a la discusión académica en temas de ciencia y tecnología para la defensa.

Se espera llenar un vacío en la cultura profesional de todos los interesados en la discusión y reflexión sobre estas materias que representan un gran desafío.

Títulos de la Colección:

1. De Fantasmas y de Máquinas
2. Explosivos, Propelentes y Pirotecnia
3. Guerra Electrónica
4. SeriousGames, una alternativa para la capacitación y entrenamiento en la toma de decisiones
5. De Ciberseguridad a Ciberguerra

El presente ensayo Nº 5 titulado "De Ciberseguridad a Ciberguerra", editado por el Fondo Editorial de este instituto, fue escrito por el Comandante de Escuadrilla e IPM Pedro Jarpa Martínez. En sus páginas el autor explica en forma pedagógica los conceptos ciberseguridad y ciberguerra.

Este binomio de conceptos se debe adicionar a los tradicionales de la guerra moderna: terreno, mar, aire y espacio.

En los cuatro capítulos el profesor Jarpa detalla ataques cibernéticos en contra de empresas civiles e instalaciones militares. Un ejemplo dramático fue la agresión a través de un malware a las instalaciones nucleares de Irán, que provocó la destrucción de las ultracentrifugadoras destinadas a enriquecer uranio 235, isótopo que constituye la materia prima para las centrales nucleoeléctricas y/o armas atómicas.

Al final el autor realiza un análisis crítico de la situación actual en nuestro país relativo a la ciberseguridad y formula valiosas sugerencias para su perfeccionamiento.

Este libro es un aporte real y significativo para todo el personal dedicado a la ciberseguridad y a la ciberguerra, logrando introducir estos conceptos al ámbito de la defensa.

El comandante Jarpa escribió con anterioridad, el ensayo Nº 3 "Guerra Electrónica", publicado por la Academia Politécnica Militar el año 2015.

Pedro Jarpa Martínez

DE CIBERSEGURIDAD A CIBERGUERRA

5

Pedro Jarpa Martínez
(Ms. Sc)

DE CIBERSEGURIDAD A CIBERGUERRA

Colección Academia Politécnica Militar del Ejército de Chile
ACAPOMIL

BIOGRAFÍA

Pedro Jarpa nació en Concepción, Chile. Ingresó a la Escuela de Aviación y egresó como oficial de la Fuerza Aérea el año 1990. Egresó de la Academia Politécnica Aeronáutica como Ingeniero de Ejecución en Sistemas de Armas con mención en Telecomunicaciones, posteriormente estudió Ingeniería Electrónica en la Academia Politécnica Militar.
Sus estudios de posgrado los realizó en la Naval Postgraduate School de Monterey-California, y obtuvo el grado de Master of Science in Electrical Engineering con mención en Joint Services Electronic Warfare, paralelamente obtuvo una certificación como Information Systems Security Professional. En la Escuela de Negocios Española IEDE, obtuvo el grado de Master in Bussiness Administration.
En la Fuerza Aérea se desempeñó como oficial de telecomunicaciones e informática y ocupó entre otros cargos el de jefe de mantenimiento del sistema de alarma temprana aerotransportado, fue operador e instructor de sistemas COMINT y ELINT. Fue jefe del departamento de Guerra Electrónica de la Dirección de Telecomunicaciones e Infor- mática y posteriormente se unió a un selecto grupo de oficiales y personal para formar el Centro de Guerra Electrónica.
En el año 2009 se unió a la empresa de telecomunicaciones Raylex S.A., como Gerente de Operaciones apoyando la gestión de los servicios de ingeniería y en el año 2011 ingresa al Ministerio del Interior como Jefe del Departamento de Tecnologías. Paralelamente es profesor de pre y posgrado en la Academia Politécnica Militar y profesor invitado de la Academia Nacional de Estudios Políticos y Estratégicos.

DE CIBERSEGURIDAD A CIBERGUERRA

Pedro Jarpa Martínez

ACADEMIA POLITÉCNICA MILITAR
SANTIAGO, 2016

Editor:
Brigadier Víctor Aguilera Acevedo, Investigador del Departamento de Investigación y Desarrollo.

Diseño de Portada:
Sr. Mario Ramírez Peralta

Inscripción Registro de Propiedad Intelectual Nº 193.320
Impreso en los talleres del Instituto Geográfico Militar
Primera edición 2016
300 ejemplares

Presentación

Es un honor para el Director de la Academia Politécnica Militar que suscribe, presentar el ensayo Nº 5 titulado "De Ciberseguridad a Ciberguerra", editado por el Fondo Editorial de este instituto y cuyo autor es el Comandante de Escuadrilla e IPM Pedro Jarpa Martínez.

El comandante Jarpa, en un lenguaje sencillo pero riguroso, desarrolla los conceptos ciberseguridad y ciberguerra. Este binomio poderoso se debe adicionar a los tradicionales de la guerra moderna: terreno, mar, aire y espacio.

Los Estados nacionales han dedicado ingentes esfuerzos humanos, materiales y financieros para ejercer controles sobre determinadas armas convencionales y nucleares. Sin embargo, en la actualidad es urgente tomar decisiones para reducir las amenazas a la ciberseguridad, procedentes de la ciberguerra.

En los cuatro capítulos de esta obra el profesor Jarpa detalla ataques cibernéticos en contra de empresas civiles e instalaciones militares. Un ejemplo dramático fue la agresión, a través de un malware, a las instalaciones nucleares de Irán, que provocó la destrucción de las ultracentrifugadoras destinadas a enriquecer uranio.

Finalmente, el autor realiza un análisis crítico de la situación actual en nuestro país relativo a la ciberseguridad y formula valiosas sugerencias para su perfeccionamiento.

El presente ensayo es un aporte real y significativo para todo el personal dedicado a la ciberseguridad y a la ciberguerra, logrando introducir estos conceptos al ámbito de la defensa.

Santiago, Julio de 2016

SERGIO NAZAR MARTÍNEZ
Coronel
Director de la Academia Politécnica Militar

Índice

DE CIBERSEGURIDAD A CIBERGUERRA

Juppiter Terminus

El dominio del ciberespacio y las vulnerabilidades de las tecnologías de la información

Pedro Jarpa Martínez

(Ms.Sc.E.E.)

Introducción

A pesar que nuestro país ha experimentado un incremento en el empleo de las tecnologías de la información, este desarrollo no ha sido acompañado de un nivel equivalente en seguridad, tanto para la operación de los distintos sistemas como para la integridad de la información que por estos fluye, comprometiendo por uno u otro medio los derechos y la privacidad de las personas, empresas y/o instituciones. Cuanto mayor es el índice de desarrollo de una sociedad, mayor dependencia tiene de los sistemas de información y comunicaciones. Estos sistemas tienen la particularidad de estar presente en la operación de toda la Infraestructura Crítica (IC), como es el caso del control a distancia de la generación y distribución de energía o del agua potable. Cualquier intrusión, manipulación, sabotaje o interrupción de los sistemas de información y/o comunicaciones o de la infraestructura de redes que estos utilizan como soporte, puede afectar al funcionamiento de los mismos y sus efectos pueden afectar a ciudades enteras e incluso paralizar la IC de todo un país, pudiendo afectar así a millones de personas.

En los conflictos tradicionales normales existen fronteras y límites, mientras que en el ciberespacio esta condición no existe. Para realizar un ciberataque no es necesario desplazarse, moverse o tener que pasar de una frontera a otra para alcanzar un blanco. Esta es una de las principales características de este escenario. El ciberespacio es un ambiente único, sin fronteras geográficas, anónimo, asimétrico y puede ser fácilmente clandestino.

El grado de conocimiento que necesita un atacante para realizar una agresión a sistemas de información ha decrecido a lo largo del tiempo debido al espectacular aumento de la calidad, cantidad y disponibilidad de herramientas ofensivas expuestas en instancias como internet, donde es relativamente fácil encontrar multitud de herramientas de hacking que se intercambian en los diferentes foros de-

dicados a esta materia. Todo ello conforma un escenario de nuevos riesgos para el que es necesario que los gobiernos desarrollen planes o estrategias y consideren las ciberamenazas como un riesgo al que es preciso hacer frente para mejorar la seguridad nacional. En este contexto, la OTAN ha definido la ciberdefensa como *"la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques"* (MC0571 - NATO Cyber Defence Concept). La forma de defenderse de estos ataques es compleja, dado que influyen factores muy diversos. Uno de ellos es el hecho que muchos de los objetivos susceptibles de ser atacados se encuentran en manos de empresas privadas, por lo que su seguridad depende en gran medida de las acciones que toman estas para salvaguardar sus sistemas, debiendo asumir costos que en ocasiones no son incluidos en sus presupuestos de implementación ni operación, por consiguiente, las medidas no son implementadas y así se concreta el riesgo. Otro factor importante es la falta de conciencia en seguridad en algunos sectores de la sociedad, lo que dificulta la toma de medidas eficaces, medidas que, en todo caso, deberían coordinar los gobiernos.

Bajo el punto de vista de la defensa de un país se puede entender la ciberguerra como el conjunto de acciones cuyo objetivo es lograr el dominio del ciberespacio, para lo cual las armas son las tecnologías de la información y las comunicaciones (TIC), y a diferencia de los otros ámbitos de acción de la guerra, en este caso no se requiere enfrentar físicamente al adversario. Bajo esta idea emerge el concepto de Ciberdefensa que involucra todas las actividades ofensivas y defensivas en las que se utilizan como medios aquellos relacionados con las infraestructuras TIC (ejemplo: redes de computadores, softwares o programas informáticos que soportan sistemas de información de empresas, del Estado o de personas), y cuyo campo de batalla es el ciberespacio. Por lo anterior el desarrollo de la Ciberdefensa se enfoca en la capacitación de los Estados para enfrentar la Ciberguerra, en donde las acciones son ejecutadas por personas con un conocimiento específico ya sea en técnicas de ataque o en manejo de vulnerabilidades preexistentes en los sistemas de información.

Entonces, para lograr el dominio del ciberespacio se requieren acciones ofensivas y defensivas, coordinadas con información necesaria para proveer inteligencia y reconocimiento de amenazas que per-

mitan la ejecución de las primeras acciones con la mayor eficiencia posible. Básicamente la ciberguerra es la batalla por el control del ciberespacio. Sin embargo, actualmente se reconoce que el ciberespacio es un componente fundamental de la Infraestructura Crítica de cualquier país y su función primaria es ser un "carrier" o proveedor de información esencial para cualquier actividad cotidiana dentro de la sociedad y también para cualquier operación militar (Mando y Control). Por esto, la ciberguerra es un componente crítico de lo que se define como Guerra de la Información (GI), cuya función es negar al enemigo el uso de los sistemas de información crítica, mientras se protegen los recursos de información propios.

La ciberdefensa es, por lo tanto, un ámbito de la Seguridad Nacional en el que los Estados deben tomar medidas específicas, que deben ejecutarse en coordinación con los sectores público y privado, ser compatibles con los derechos y libertades individuales de los ciudadanos, ser coordinadas con otras acciones de seguridad y defensa tomadas para responder a otras modalidades de agresión, establecer sistemas de respuesta a los ciberataques y fomentar la cooperación internacional. Un ciberespacio seguro es esencial para la seguridad nacional y, por lo tanto, el trabajo que aquí se propone es un tema de máximo interés en el que varias instituciones de las FF.AA. y del Estado de Chile, y algunos sectores de la industria, han puesto su atención y lo consideran un ámbito de trabajo fundamental para la seguridad del siglo XXI.

Este ensayo pretende presentar progresivamente las definiciones de las amenazas que se pueden encontrar en el ciberespacio a partir del espionaje industrial y estatal, el fraude a pequeña y gran escala, y el sabotaje o ataques a la Infraestructura Crítica. Paralelamente busca definir las vulnerabilidades de los sistemas que interactúan en este medio, el estatus actual de la sociedad chilena y los actores que se distinguen en ella en el empleo del ciberespacio, las capacidades actuales desarrolladas por algunas instituciones del Estado y algunos sectores de la industria. También se pretende recoger las iniciativas de diversos países y organizaciones internacionales sobre políticas y estrategias para abordar la ciberamenaza, revisando cómo las naciones más desarrolladas del mundo y algunas organizaciones internacionales han adoptado el concepto de ciberdefensa en sus estrategias de seguridad nacional.

De esta forma el presente ensayo se conforma como un punto de partida para comprender la ciberseguridad y valorar su alcance y su influencia, planteando un conjunto de conceptos y medidas que constituyen un buen inicio para el necesario debate que en el ámbito de la Defensa Nacional se debe afrontar y así satisfacerlas expectativas, tanto de los lectores menos versados en la materia, que buscan un conocimiento genérico en su primera aproximación al concepto de ciberdefensa, como de los más experimentados, que dispondrán de una recopilación de fuentes nacionales e internacionales, lo que les permitirá profundizar en los nuevos retos de la Seguridad Nacional, consecuencia de esta nueva amenaza.

Por tal razón, haciendo uso de la experiencia y conocimientos adquiridos hasta hoy, el autor considera que redactar un volumen único que abarque el concepto de ciberdefensa, bajo un enfoque de seguridad desarrollado a partir del mismo ciberespacio, su empleo en la sociedad, las vulnerabilidades que presenta, la proposición de medidas que el autor estima debiesen implementarse, el reto y los requerimientos a que se enfrenta la Defensa Nacional en cuanto a elevar el nivel de conocimientos y preparación, estructurar una capacidad conjunta para enfrentar este medio que constituye el quinto elemento y dominio de la guerra moderna, puede ser de mucha utilidad para aquellos ingenieros, oficiales, especialistas o quienes requieran obtener un entendimiento de la aplicación de la ciberguerra en el desarrollo de los conflictos actuales. Especial atención debe ponerse en la palabra conflicto, porque no necesariamente debe existir una declaración de guerra o enfrentamientos de fuerzas, para que se concrete un ciberataque, que en si puede ocurrir sin mediar acciones o declaración de guerra de por medio.

Claramente la ciberguerra tiene su origen en el ciberespacio, el que se divide en dos grandes concepciones bajo los criterios de seguridad, siendo la primera y más amplia la misma ciberseguridad, cuyo enfoque es la implementación y operación de los sistemas de información crítica bajo un criterio transversalmente enfocado en la seguridad. La segunda es la ciberdefensa que, bajo el entendimiento del autor, está entregada a la defensa de una nación, la que ante un conflicto deberá estar preparada para ejecutar tanto acciones ofensivas como coordinar las acciones o emplazamiento defensivo de su IC para hacer frente a un ciberescenario reconocidamente hostil.

Capítulo I
El Ciberespacio

Las Tecnologías de la Información (TI), basadas en telecomunicaciones principalmente móviles, llegaron para quedarse y acompañar nuestro diario vivir en forma transparente, abarcando cada día más y más procesos que soportan nuestras actividades cotidianas, incluso mientras descansamos o simplemente dormimos. ¡Así es!, incluso mientras dormimos nuestra vida digital sigue activa ya sea recibiendo emails en nuestras respectivas casillas de correo, moviendo los depósitos o cobros programados en nuestras cuentas bancarias, nuestros smartphones siguen activos registrándose en la red a través de la cobertura de la antena más cercana a nuestro sitio de descanso e incluso actualizan las aplicaciones que regularmente utilizamos. Quienes son un poco más avanzados programan cámaras ip de vigilancia de su entorno para alertar de cualquier eventual intento de robo en casa y mucho más.

Caso aparte es la operación de los servicios que soportan nuestra vida diaria, me refiero a la Infraestructura Crítica (IC). Esta infraestructura controla la producción, transporte y entrega de la energía (electricidad, gas, agua, telecomunicaciones y otros) fundamental para el funcionamiento, desarrollo y proyección de toda sociedad moderna. Gran parte de la IC, si no toda, controla sus procesos en forma remota a través de comunicaciones digitales no necesariamente bajo el formato del protocolo ip, pero digital y electrónicamente al fin. Así los flujos de agua que pasan a través de una central hidroeléctrica son monitoreados y controlados a grandes distancias. En este sentido, basta con ver como el Centro de Despacho Económico de Carga del Sistema Interconectado Central (www.cdec-sic.cl) dispone elevar la generación ante el aumento de la demanda por energía eléctrica en el país. Un ejemplo más cotidiano es la Unidad Operativa de Control de Tránsito (www.uoct.cl) que tiene como responsabilidad adminis-

trar y operar los sistemas de control de tránsito y otros sistemas complementarios, como circuitos cerrados de televisión, letreros de mensaje variable, estaciones automáticas de conteo vehicular, entre otras tecnologías. Todo ese control se lleva cabo a través de líneas de comunicaciones digitales que nos permiten hasta acceder en tiempo real a las imágenes del tránsito en distintas ciudades.

Hoy el concepto de "smartcity" es una realidad y se basa en la aplicación eficiente de tecnologías de la información para el desarrollo urbano basado en la sustentabilidad, satisfaciendo adecuadamente las necesidades básicas de empresas y ciudadanos en el plano económico, como en los aspectos operativos, sociales y ambientales. Una ciudad podrá llamarse inteligente en la medida que las inversiones que se realicen en educación, aspectos sociales, infraestructuras de energía (electricidad y gas), tecnologías de comunicaciones (electrónica e internet) e infraestructuras de transporte, contemplen y promuevan una calidad de vida superior, un desarrollo económico-ambiental durable y sostenible, una gestión considerada de los recursos naturales, y un buen aprovechamiento del tiempo de los ciudadanos. Así, cuanto mayor es el índice de desarrollo de una sociedad, mayor dependencia tiene de los sistemas de información y comunicaciones.

Respecto al empleo de las tecnologías de la información por parte de las Fuerzas Armadas, para nadie es un misterio que tanto sistemas de armas como también sus sensores asociados y los respectivos sistemas de mando y control operan y generan información, la transmiten, procesan y analizan gracias al soporte de sistemas de telecomunicaciones que forman parte de toda esta cadena. Sin ir más lejos, muchos de los enlaces de comunicaciones de radio frecuencia militares modernos levantan redes de comunicaciones ip móviles y hoy incorporan tecnologías como la comunicación móvil 4G. En otras palabras, los sistemas de mando y control militar actualmente tienen una alta dependencia de las tecnologías de la información y no es posible conducir las operaciones militares sin un alto grado de información proveniente del teatro de operaciones.

Dentro del ámbito de la defensa, no debemos olvidar que un segmento del Departamento de Defensa de Estados Unidos formó la agencia Advanced Research Projects Agency (ARPA), encargada de

asegurar el liderazgo de esa nación en ciencia y tecnología con aplicaciones militares, generando también los estudios conceptuales de lo que hoy conocemos como internet y el TCP/IP (Transfer Control Protocol / internet Protocol).

Lo que hasta aquí hemos descrito nos lleva a encontrar un factor común que impulsa a todas las instancias analizadas confluir a las tecnologías de la información, que por su naturaleza son altamente dependientes de ese elemento. Ese factor común es el ciberespacio.

El ciberespacio es un dominio interactivo compuesto por redes digitales que es utilizado para almacenar, modificar y comunicar información. Incluye la internet, pero también otros sistemas de información que apoyan nuestros negocios, la industria, los servicios y la IC. Por consiguiente, toda red digital que considere medios de almacenamiento de información (pendrives, CDs, microSD, discos duros, bases de datos, clouds y data centers, etc.), medios de procesamiento de información (aplicaciones, softwares, nodos de conmutación, procesadores en general), todas la líneas de comunicaciones digitales físicas e inalámbricas, incluyendo a sus elementos transmisores y receptores (redes de banda ancha domiciliaria y móvil, enlaces satelitales, televisión satelital, redes microondas, telefonía móvil e internet) conforman el ciberespacio.

La UIT, Unión Internacional de Telecomunicaciones, define el ciberespacio como el lugar creado a través de la interconexión de sistemas de ordenador mediante internet. Define también conceptos como ciberentorno y ciberseguridad. El ciberentorno incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes.

Algunas personas necesitan ver para comprender, por tal razón existe un proyecto denominado OPTE que fue originalmente creado para generar una imagen (o mapa) de internet, según se puede apreciar en la figura 1.1. Opte (pronunciado op-tee) proviene de la palabra latina *Opti*, cuyo significado es óptico. El nombre finalmente proviene del creador del proyecto, el Sr. Barrett Lyon, a quien le hizo sentido el nombre opte.org. [1]

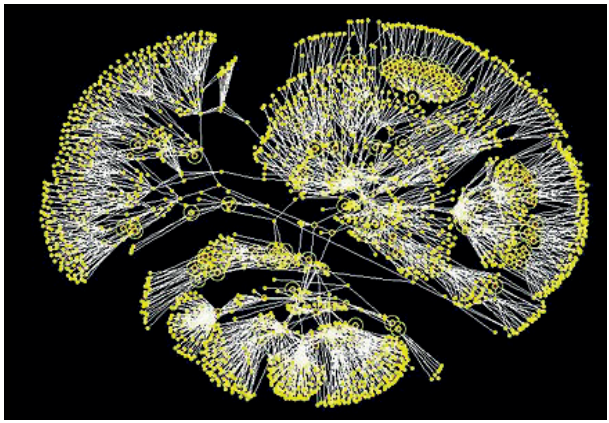

Figura 1.1: Imagen o mapa de internet. Fuente: [1].

Dado que internet es básicamente una vasta constelación de redes que de alguna manera se interconectan para proporcionar la comunicación de datos de una forma relativamente fluida, parece lógico que uno podría dibujar líneas de un punto a otro. La visualización resultante es una colección de trazos que, en conjunto, arrojan una imagen de todas las interconexiones de cada red en internet. El resultado fue una representación galardonada de internet que se exhibe actualmente en el Museo de Arte Moderno de Nueva York. Esta representación tiene versiones de acuerdo a los años representados en su gráfica. (Se sugiere visitar la página www.opte.org) [1].

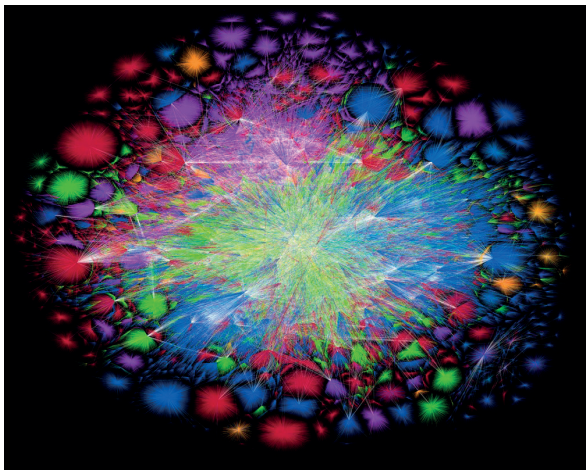

Figura 1.2: Representación del mapa de internet del año 2015.
Fuente [1].

Gracias al ciberespacio hoy podemos relacionarnos con personas al otro lado del mundo, obviando las barreras geográficas e idiomáticas, en otras palabras, el ciberespacio no tiene una estructura asociada a un orden geográfico ni mucho menos a un orden estático, por el contrario, se basa en una disposición dinámica de sus elementos e interacciones y no reconoce fronteras. Esta última característica permite que nos relacionemos con muchas más personas que las que podríamos en una relación real, así se potencia el conocimiento y el desarrollo económico. Hoy no necesito desplazarme de mi lugar de conexión para ir a buscar información respecto a un tema de mi interés, por el contrario, navego en la web y puedo obtener lo que busco en muy poco tiempo (conocimiento), y si quiero cotizar un producto o un servicio, mis opciones ya no son solo locales, por el contrario, mi opción es el mercado global. ¿Quién, desde Chile no ha comprado algún producto en el extranjero a un precio más conveniente que en el mercado local incluyendo su despacho e impuesto?

Entonces, si proyectamos las características del ciberespacio y su empleo por parte de todo un país, es fácil comprender que se facilita el camino al conocimiento y la educación de su población, como así también el intercambio social y cultural entre sus ciudadanos y los del mundo entero. A su vez, el ciberespacio es una herramienta potenciadora del desarrollo económico de una nación, permitiendo ofrecer globalmente la producción local, agilizando el mercado y demandar localmente la adquisición de bienes lejanos, incentivando de esta forma la competitividad de la industria.

Chile desde hace más de una década ha demostrado altos índices de aceptación y penetración de las tecnologías de la información. Estos índices van a la par de países desarrollados y reflejan la evolución que ha tenido la industria de las tecnologías de la información a nivel internacional. Por ejemplo, hasta el año 2010 las conexiones de banda ancha fija fueron en aumento hasta alcanzar 1.800.000 conexiones en el país, sin embargo, a partir de ese año la cifra disminuye anualmente producto del interés de los ciudadanos en disponer de acceso a comunicaciones móviles y la disponibilidad de esa tecnología. Así, hoy ya no se concibe adquirir un dispositivo móvil que no disponga de capacidad *wireless* y todo apunta a la integración, alta disponibilidad, miniaturización y multitarea de los dispositivos, sean estos smartphones, tablets, notebooks, relojes, etc.

El ciberespacio como un espacio virtual de interacción, existe solamente como espacio relacional; su realidad se construye a través del intercambio de información; es decir, es espacio y es medio. Una red sin interacción entre sus miembros deja de ser una red; la red existe porque existen relaciones entre sus integrantes. Ciertas tareas que antes era necesario realizar físicamente, ahora se pueden realizar a través de escenarios virtuales alojados en el ciberespacio. En muchos casos, la eficacia del mundo virtual ha hecho desaparecer del mundo real elementos que no hace mucho parecían firmemente anclados en nuestro entorno material.

En ocasiones, se entiende el ciberespacio como una gran acumulación de información. Esto es cierto, pero no es lo básico. No dejaría de ser simplemente una gran base de datos en la que los usuarios se limitarían a localizar información y saldrían como de cualquier biblioteca. A diferencia de otros medios -el ciberespacio es también medio-, permite la convivencia, la construcción de relaciones de diversos tipos y grados. Es, en efecto, espacio en todos los sentidos, aunque sea virtual.

La internet ha revolucionado nuestra sociedad manejando el crecimiento económico y entregando a las personas nuevas maneras de conectarse y cooperar entre ellas. La baja en los costos de las tecnologías que soportan internet significa una mayor facilidad de acceso a esta, permitiendo a más personas alrededor del mundo utilizarla, "democratizando" el uso de la tecnología y alimentando el flujo de la innovación y la productividad. Esto motiva la expansión de ciberespacio, así como el valor de su utilidad.

La World Wide Web solo empezó en 1991, pero hoy 2.000 millones de personas están online, casi la tercera parte de la población mundial. Hay más de 5.000 millones de dispositivos conectados a internet. Así es fácil ver por qué el crecimiento de internet ha sido tan dramático. El ciberespacio transforma el negocio, lo hace más eficiente y efectivo. Abre mercados, permitiendo el comercio a los costos más bajo y permitiendo a las personas hacer negocios en movimiento (on the move), ha promovido el pensamiento fresco, modelos de negocio innovadores y nuevas fuentes de crecimiento. Permite a las compañías proporcionar un servicio mejor, más barato y más conveniente a los clientes. Y faculta a los individuos comprar, comparar los precios y encontrar lo que desean.

Al igual que la mayoría de los cambios, el aumento de nuestra dependencia del ciberespacio trae nuevas oportunidades, pero también nuevas amenazas. Mientras el ciberespacio fomenta los mercados libres y abre las sociedades, esta apertura también nos puede hacer más vulnerables a criminales, piratas informáticos, servicios de inteligencia extranjeros que buscan dañarnos comprometiendo o afectando nuestros datos, nuestra información crítica y los sistemas que la soportan.

Las redes en que nosotros hoy confiamos nuestra vida diaria sobrepasan las fronteras organizacionales y nacionales. Los acontecimientos en el ciberespacio pueden suceder a una inmensa velocidad, sobrepasando respuestas tradicionales (por ejemplo, la explotación del ciberespacio implica que crímenes como el fraude pueden ser cometidos remotamente y a una escala industrial). Aunque tengamos maneras de administrar riesgos en el ciberespacio, estas se nivelan con este ambiente dinámico y complejo.

La introducción del cloud computing y las *smart-grids*, el crecimiento continuo del trabajo en movimiento y el crecimiento en el número de usuarios del ciberespacio demuestra que este llegará a ser cada vez más valioso e importante para Chile y el mundo.

En los años 40, el matemático alemán/estadounidense Norbert Wiener acuñó el término cibernética, para denominar *"la teoría de control y comunicación, ya sea en la máquina o en el animal"*. En la imaginación popular, el término cibernética y por ende ciber se empezó a asociar principalmente con robots humanoides o criaturas controladas de una forma similar. Pero, ¿cómo llegó ciber a su asociación actual con internet? El vínculo es el término ciberespacio, el mundo electrónico virtual en el que exploramos, jugamos, aprendemos y compartimos información.

Teóricos del ciberespacio como Howard Rheingold admiten que la palabra viene de las novelas de ciencia ficción de William Gibson, particularmente el cuento Quemando Cromo, publicado en 1982, y en la novela Neuromante, de 1984. Sin embargo, la historia que cuenta el mismo Gibson sobre cómo acuñó el término ciberespacio contiene una lección para quienes le buscan mucho significado a las derivaciones de las palabras. Según dice, necesitaba un nombre atractivo

para el escenario en el que sus historias se desarrollarían y ciberespacio sonaba como que significaba algo o que podría significar algo, pero entre más la miraba, lo que más disfrutaba es que no significaba absolutamente nada.

Figura 1.3: William Gibson acuñó el término ciberespacio. Foto: Wikipedia

La sociedad chilena en el ciberespacio

Podemos distinguir tres actores fundamentales de la sociedad chilena en el ciberespacio. Estos son el Estado, los privados (empresas) y los ciudadanos. Los conocimientos y la conciencia en aspectos de seguridad y las capacidades de desenvolverse en forma segura en el ciberespacio de cada uno de estos actores son diametralmente opuestos o al menos muy dispares.

- **El Estado:** provee servicios a los ciudadanos quienes perciben estos con bastante seguridad y confianza. Sin embargo, las prestaciones y potencialidades se presentan dispares entre los servicios que prestan los distintos ministerios y organismos públicos. Por ejemplo, tenemos los servicios del Registro Civil que por medio de su página web es posible descargar una variedad de certificados y documentos de forma rápida y eficiente. Lo mismo ocurre

con el Servicio de Impuesto Internos, que para nadie es un misterio la efectividad de su plataforma en el seguimiento tributario de los ciudadanos contribuyentes y las facilidades que presta en los meses de abril cuando corresponde presentar la declaración correspondiente. Ambas instituciones son reconocidas internacionalmente por las aplicaciones y servicios implementados en pos de una atención rápida y expedita a los ciudadanos.

Sin embargo, otros organismos del Estado no están a la altura y se presentan en vías de coordinación permanente para entregar un mejor servicio online, pero que a la fecha no han concretado, llegando a adoptar alguna solución de servicio, para quienes los temas de disponibilidad en la red y la seguridad de estos han quedado relegados a un segundo plano, perjudicando la imagen de esos organismos como sus desarrollos web. Un ejemplo de esto han sido los recurrentes ataques del tipo "defacement" que han sufrido varias páginas gubernamentales ante ataques coordinados por hackers que apoyan diversas campañas y movimientos sociales en el país y a nivel global. De igual forma, la exposición involuntaria de bases de datos con información sensible respecto a ciudadanos, que han llevado a cabo otros organismos nacionales.

- **Los Privados:** entendiendo a los privados como todo tipo de empresas que prestan servicios o comercializan productos, se puede apreciar que algunos poseen grandes capacidades y conocimientos en temas de ciberseguridad y los aplican en pos de diferenciarse en los servicios que entregan, es el caso de las grandes empresas de telecomunicaciones que inherentemente a su negocio han evolucionado en paralelo con el desarrollo de las tecnologías de la información, sus requerimientos de seguridad y vulnerabilidades, pero lamentablemente no han invertido de manera equivalente en instruir a sus clientes en aspectos de ciberseguridad.

  Otro ejemplo es la industria financiera, no cabe duda que las inversiones en seguridad llevadas a cabo por esta industria se relaciona directamente con los valores que transa, y a pesar de esa inversión permanentemente se le ha visto expuesta a fraudes realizados por hackers que utilizan las últimas técnicas para lograr apoderarse de algún monto de dinero cuando encuentran una vulnerabilidad en los sistemas bancarios, ya sea en las interfaces de atención a

clientes (tarjetas bancarias, accesos on-line a cuentas corrientes, clonaciones, etc.), o en sus redes corporativas.

Otros actores privados no tienen conciencia respecto a la seguridad de los servicios que levantan a través de la web exponiendo sus productos, alternativas de crédito, sistemas de fidelización de clientes, información corporativa, etc. El punto es que al no considerar las medidas de seguridad adecuadas están exponiendo su negocio, todas sus transacciones comerciales y las bases de datos de clientes a potenciales ladrones de información, quienes pueden comercializar esa información entre la competencia y/o explotar esa información ya sea contra el negocio mismo o contra los clientes de este. Es aquí cuando se vulnera la información privada de los clientes, pudiendo hacer un mal uso de esta partiendo por sus datos personales para una eventual suplantación, o sus datos financieros para un eventual fraude, incluso datos de contacto (email, teléfono móvil, dirección, etc.), para campañas de email masivo (spam), publicidad telefónica, campañas publicitarias, registro de falsos votantes o adherentes en campañas políticas o movimientos sociales, etc.

Con todo lo descrito anteriormente solo depende de la capacidad de imaginación que pueda tener algún experto informático mal intencionado, que día a día no dejan de sorprender inventando una y mil formas de aprovecharse de la información que obtienen y realizar fraudes de todo tipo, tanto contra clientes como contra las mismas empresas.

Otros actores privados, son totalmente desconocedores del problema de seguridad en el manejo digital de la información. Este hecho se presenta con mayor frecuencia en empresas de menor tamaño. Es el caso de páginas web en donde se comercializa un número acotado de productos y/o servicios en las que fácilmente se puede encontrar y extraer información relevante del negocio cuyo servidor de soporte es utilizado para el control de las operaciones internas de la empresa, permitiendo acceder a los servicios corporativos desde el exterior sin mayores resguardos o filtros lógicos que evite esta situación. Esta es la vulnerabilidad mayor que pueda presentar la arquitectura de una red y expone gran parte de los recursos informativos de las empresas, sus trabajadores y clientes al ciberespacio.

- **Los Ciudadanos:** la verdad es que si se les pregunta directamente a las personas ¿si están preocupadas por los temas de ciberseguridad en su vida digital?, ellos responderán afirmativamente, que es un tema de prioridad y preocupación. Sin embargo, ellos se encuentran en general poco informados, tienen un bajo nivel de conciencia y capacitación respecto al tema y son altamente vulnerables. Gran parte de la población chilena actual nació antes de la masificación de los computadores personales, es decir, su educación y vida personal no fue directamente sustentada por el mundo digital, por lo que debieron asumir el ingreso de su vida al ciberespacio, aunque unos más tardíamente que otros.

  Por otro lado, la juventud chilena nació con procesadores personales y se reconoce ciberdependiente por el amplio empleo que hace de los servicios digitales, principalmente a través de dispositivos móviles. Pero ellos lamentablemente han demostrado ser tan ignorantes en aspectos de seguridad como el grupo etario anterior. Los jóvenes asumen que el ciberespacio es un medio más confiable que la vida real en sí misma, llegando a perder el pudor al exponer su propia vida en las redes sociales con quienes ellos asumen son sus amigos y que estos conservarán bajo resguardo la información compartida. El tema es que en el momento de que algo de información se digitaliza, ya forma parte del ciberespacio y en el momento que esa información es subida a la internet no se tendrá más control de esta, pudiendo llegar a todo el mundo en tiempo real. *"¡Lo que se publica en internet, de internet no sale!"*.

  Es muy penoso ver como adolescentes han subido videos, comentarios e imágenes que los comprometen a ellos directamente o sus propias amistades. Esto ocurre porque no existe una capacitación formal respecto al empleo de forma segura de los medios digitales y las redes sociales para el manejo de información, ni mucho menos respecto del uso de internet, las aplicaciones que soporta y las mismas redes sociales. Los planes de educación básica consideran programas de formación orientados a desarrollar habilidades en el empleo de los computadores, lo que es complementado en casa por los padres al facilitar un pc de uso domiciliario. Pero ambas instancias no asumen los riesgos de en-

tregar esta herramienta y conocimiento a niños y adolescentes. Ninguna de estas instancias instruye en términos de seguridad en el empleo de la tecnología. Basta con preguntarse entre quienes han instalado wifi en casa, ¿cuántos le han asignado una password de acceso?, ¿quiénes tienen activados los filtros de contenido para adultos en la programación de los televisores en casa o de igual forma, los filtros de páginas web con contenidos no aptos para menores de edad en los routers para wifi? Entonces si yo no dejo la puerta de mi casa abierta todo el día, ¿por qué permito que mis hijos queden expuestos al mundo entero a través de una conexión wifi?

Con la irrupción de las tecnologías de la información y su omnipresencia, es increíble la vulnerabilidad que se genera en la vida de las personas por el solo hecho de por ejemplo utilizar un dispositivo móvil, sea este un smartphone, tablet, notebook u otro cualquiera. Partiendo por el levantamiento del perfil personal en el dispositivo, como así también en los servicios asociados, es posible revelar de manera involuntaria información sensible respecto de uno mismo. El amplio empleo que se hace de las redes sociales en las que lamentablemente se vuelca mucha información personal en todo formato (imágenes, video, texto, etc.), ha materializado un canal de información en la práctica infinito que expone vulnerabilidades que explotan a diario algunos delincuentes para coordinar fraudes y/o suplantaciones. Vuelvo a la pregunta anterior, ¿por qué si uno no deja la puerta de su casa abierta, expone imágenes propias del interior de esta?, ¿por qué si uno no publica en el frontis de su casa que esta va a quedar sola por unos días, va a publicar que se encuentra con toda su familia de viaje en alguna red social?, ¿por qué si yo no publico los datos de mis tarjetas de crédito, los doy para comprar en una página web extranjera cuyo servidor probablemente ni siquiera está en el país donde dice residir esa página? Con esta última pregunta alcanzamos otro aspecto de las vulnerabilidades del ciberespacio… hoy son muchos los chilenos afectados por el fraude a través de la clonación de tarjetas, robo de claves de acceso y, finalmente, transferencias bancarias producto de phishing vía web.

¿Podríamos decir que Chile es "el ciberparaíso... para los ciberdelincuentes y hackers"?

Interrelaciones

Para entender un poco más las interrelaciones que se producen entre los actores nacionales que toman parte en el ciberespacio podemos referirnos a la relación entre:

- **El Estado y los privados.** En este caso el Estado proporciona el marco legal regulatorio de operación para la industria de las tecnologías de la información, los servicios de telecomunicaciones y la comercialización de los productos y servicios involucrados.

- **Los privados y los ciudadanos.** Los ciudadanos perciben los servicios prestados por las empresas con un nivel de seguridad referencial. Así es, los ciudadanos ven que los servicios que adquieren tienen un nivel de seguridad muy bajo y definitivamente referencial por cuanto se enfrentan a servicios que para diferenciarse de la competencia ofrecen seguros complementarios cuyo objetivo es aparentar cubrir aspectos de seguridad en la oferta a sus clientes, pero que en realidad lo que hacen es traspasar los costos de un problema a los propios ciudadanos.

  El mejor ejemplo de esta situación ocurre en los servicios bancarios. Si el cliente de un banco sufre un fraude contra sus tarjetas o cuenta corriente, lo mejor será que disponga del seguro correspondiente que lo cubra, de lo contrario la única forma de lograr que el banco responda con los fondos sustraídos será con la competencia de un buen abogado, instruido en aspectos de seguridad de las tecnologías de la información, como así también de un juez competente y a la vez instruido de igual forma. Entonces la seguridad se transforma en un costo traspasado a los clientes, cuando debería ser un aspecto a garantizar por quienes entreguen un servicio.

- **El Estado y los ciudadanos**. Para este caso, los ciudadanos perciben los servicios que les otorga el Estado con seguridad y confianza, aunque han visto como algunas entidades estatales han sufrido ataques persistentes en contra de sus páginas web. Aun cuando han pasado desapercibidos, también se ha visto vulnerada información confidencial producto de algunas negligencias que han terminado por exponer información de los ciudadanos por errores en el manejo de bases de datos publicadas errónea-

mente, afectando la privacidad de las personas y organismos involucrados.

Igualmente, existen relaciones que tienen lugar en el ámbito social cuyos componentes son personas y ciberidentidades. El componente persona está formado por los individuos que interactúan con el ciberespacio. La relación entre personas y ciberidentidades puede ser de "*1 a n*" y de "*n a 1*", es decir, una persona puede disponer de una o más ciberidentidades y una ciberidentidad puede ser utilizada por una o más personas. Estas ciberidentidades pueden ser reales o suplantadas, lo que permite gozar de cierto anonimato y dificulta la persecución de conductas punibles que se ejecuten en el ciberespacio. Las ciberidentidades están constituidas, entre otros, por cuentas de correo electrónico, cuentas de usuarios en redes o perfiles en redes sociales.

Finalmente, los ciudadanos reconocen en el Estado el seguimiento del delito informático con el apoyo de la Brigada del Cibercrimen de la Policía de Investigaciones (PDI). En efecto, se ha logrado en mayor o menor medida dar con representantes de colectivos hactivistas, clonadores de tarjetas de crédito, comerciantes de material pornográfico y/o pedófilos, gracias al personal de la Brigada del Cibercrimen.

Estado de Chile y ciberseguridad

El Estado de Chile dispone de una red de conectividad interministerial que une gran parte de los servicios y ministerios en una red informática consolidada. Esta red considera a más de 120.000 terminales de computadores y es administrada por el Ministerio del Interior. Sin embargo, no es una red homogénea ni ha sido concebida con un criterio uniforme ni orgánico, menos en aspectos de seguridad. Esto se debe principalmente a que en sus orígenes los desarrollos informáticos fueron impulsados de manera individual por cada ministerio y al interior de estos por cada una de las divisiones en la medida que estas destinaran recursos. Así se llegó a disponer de redes locales que finalmente el Ministerio del Interior concluyó uniéndolas y conectándolas para de esta manera consolidar una Red de Conectividad del Estado (RCE). Así hoy la RCE es la proyección natural de la intranet del Estado creada en el año 2001.

La Agenda Digital que cubrió los años 2004 al 2006 representó un esfuerzo colaborativo público-privado. En ella participaron asociaciones de empresas relacionadas a las tecnologías de la información, proveedores de internet, secretarías de gobierno y universidades. Una de las misiones consignadas en esta agenda, para el Ministerio del Interior fue la Iniciativa 17 que indicaba lo siguiente: *"El Ministerio del Interior buscará establecer y mantener un sistema nacional de respuesta a incidentes cibernéticos, administrar un programa de reducción de amenazas y vulnerabilidades, desarrollar un programa de capacitación en seguridad, asegurar el ciberespacio en que opera el gobierno y administrar un sistema de cooperación nacional e internacional en materia de seguridad".* (http://www.economia.gob.cl/1540/articles-187092_recurso_1.pdf). Esta iniciativa se cumplió parcialmente con la conformación del Equipo de Respuesta a Incidentes de Seguridad de Computadores (CSIRT, en inglés: Computer Security Incident Response Team) del Ministerio del Interior, instancia creada a partir del año 2011.

Regulación y marco jurídico

Dentro del Estado de Chile existe un marco regulatorio y jurídico basado en la emisión de decretos y leyes dedicados a atender los temas de las tecnologías de la información y la seguridad que estos deben presentar. Algunos se mencionan a continuación:

- Decreto 77: Aprueba norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la administración del Estado y entre estos y los ciudadanos.

- Decreto 81: Aprueba norma técnica para los órganos de la administración del Estado sobre interoperabilidad de documentos electrónicos.

- Decreto 83: Aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

- Ley 19.223 sobre Delito Informático.

- Ley 19.628 sobre Protección de Datos Personales.

- Ley 19.799 sobre Firma Electrónica.

- Ley 20.478 sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones.

- Ley 20.453 consagra el principio de neutralidad en la red para los consumidores y usuarios de internet.

- Ley 20.500 sobre participación ciudadana en la gestión pública.

- Incorporación de buenas prácticas en materia de ciberseguridad: PMG-SSI.

A lo anterior podemos reiterar la creación del CSIRT, cuya misión es *"proveer información y asistencia a la red gubernamental, administrar un sistema de cooperación nacional e internacional en materias de ciberseguridad, con el objetivo de reducir el riesgo y articular la respuesta a estos cuando su materialización sea efectiva. Tiene la facultad de exigir parámetros de seguridad en las redes de comunicaciones del Estado y promueve acuerdos de colaboración con actores importantes a nivel nacional e internacional"*. (www.csirt.gob.cl/mision_csirt.html).

En el país existen otras instancias similares al CSIRT de Interior, tales como el CLCERT.CL dependiente de la Universidad de Chile, algunos CSIRT provistos por empresas privadas del rubro de la seguridad informática (servicios pagado) y otros por ejemplo de las Fuerzas Armadas, cuyo ámbito de acción se enmarca exclusivamente en las redes de comunicaciones de la defensa.

Con lo descrito hasta ahora quisiera incorporar el siguiente concepto de seguridad: un computador o una red de computadores no monitoreados genera una incertidumbre total respecto de su seguridad. Se puede invertir mucho en seguridad para un computador, para una red y para sus usuarios (firewalls, antivirus, encriptación, etc.), pero si no se monitorea esa red no existe certeza de su seguridad y/o vulnerabilidad. Esto es lo que un CSIRT realiza, monitorea las redes de su responsabilidad en términos de la seguridad de los flujos de información tanto internos como las comunicaciones de entrada y salida con el exterior, evitando que se genere fuga de información por canales no autorizados, ya sea voluntaria o involuntaria-

mente, deteniendo el flujo de esta cuando no obedezca a conductas autorizadas y esperadas por parte de sus componentes y/o contactos externos.

Entonces, el equivalente a un CSIRT es el cuerpo de guardia de una unidad militar, que como tal tiene muros muy altos o al menos cercos con alambre con púas (equivalente a un firewall), con cámaras en un circuito cerrado de televisión para tener imagen las 24 horas del día del perímetro evitando de esta forma el ingreso no autorizado y habilitando un pórtico de acceso donde existe un control de acceso positivo de quien ingresa o se retira de la unidad, impidiendo de esta forma el ingreso de personas no autorizadas a la unidad e impidiendo que salga material de esta a la vía pública. En el mismo sentido opera un CSIRT, pero su foco es la comunicación de las redes y la información que se gestiona internamente y la información que se envía y se recibe del exterior.

Pero volviendo al marco regulatorio y legal, más allá de la existencia o no de decretos y leyes, se hace muy notorio la falta de un documento superior del Estado que canalice y oriente los esfuerzos en proteger los sistemas de información críticos. En realidad es notoria la falta de visión país respecto de la seguridad de los sistemas de información. En una sociedad que se compara permanentemente con las estadísticas y rankings de la Organización para la Cooperación y el Desarrollo Económico (OCDE), seguramente en este tema debemos ser uno de los países más distantes del primer nivel internacional. Hoy se necesita a todas luces una Estrategia Nacional de Ciberseguridad que entregue los lineamientos, visión y objetivos en materia de seguridad para sistemas de información en el Estado y con un enfoque de protección de la Infraestructura Crítica.

Entendiendo a la Infraestructura Crítica como el conjunto de servicios básicos, estructura vial y plataformas de soporte que sustenta el normal funcionamiento y desarrollo de la vida diaria de una sociedad, se debe poner especial atención en proteger sus sistemas de información. Esto porque gran parte de la industria y la Infraestructura Crítica del país es controlada remotamente por tecnologías de la información, las que si no son protegidas quedan expuestas a ataques perpetrados a través del ciberespacio. Ejemplo de esto es la parálisis general que sufrió Estonia el año 2007 cuando por una de-

cisión política tuvo una reacción social inesperada que produjo una severa reacción en contra de la medida inicial. El resultado fue una serie de ciberataques en contra de distintos servicios básicos como las telecomunicaciones, la banca, los servicios web del Estado, las universidades y otros, paralizando electrónicamente al país durante casi un mes.

Otro ejemplo más específico es el ciberataque que sufrió Irán en contra de su capacidad de generación de energía nuclear. Este ciberataque se enmarca dentro de los más sofisticados y fue llevado a cabo a través de un malware denominado "Stuxnet". Se sabe que este malware infectó una planta de enriquecimiento de uranio de ese país al menos unos seis años antes de que este se activara. Al momento de su activación, Stuxnet sobrerrevolucionó las centrífugas de enriquecimiento de uranio, pero en la central de monitoreo de estas el reporte era de normal funcionamiento. Al final, todo el sistema de control industrial tipo "SCADA" estaba comprometido, teniendo que detener la totalidad de la capacidad para evitar una catástrofe nuclear, incluyendo las plantas nucleares asociadas para la generación de energía eléctrica con la consecuente pérdida de recursos involucrados.

Para evitar lo descrito anteriormente se han generado instancias de coordinación a nivel internacional que han agrupado a un gran número de países en desarrollo y en vías de desarrollo. Estas instancias han buscado que los países adopten una política de seguridad tendiente a satisfacer los requerimientos de protección de su Infraestructura Crítica. Pero unos en mayor o menor medida se han ido quedando relegados por decisión propia o por ignorar la verdadera relevancia de este aspecto en la seguridad del país. Este último parece ser el caso de Chile.

Capítulo II
Conceptos Básicos e Incidentes Globales

El elemento de fondo que establece la razón de ser de la seguridad del mundo actual es la información. Como tal la información constituye el elemento esencial del poder en los distintos ámbitos de la vida real. Por tal razón es bueno definir qué se entiende por información.

La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento de un sujeto o sistema que recibe dicho mensaje. Esto proceso es representado en la siguiente figura.

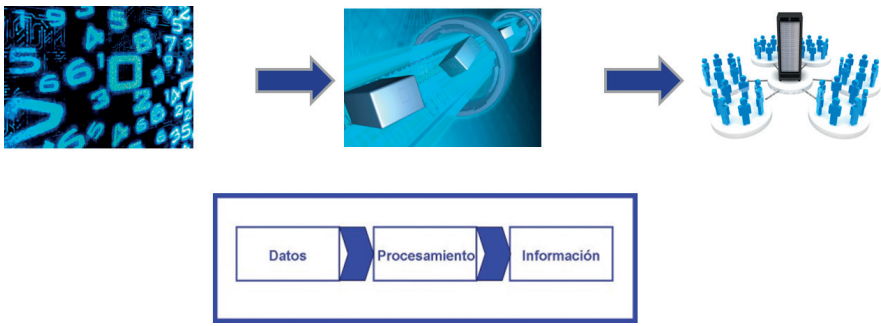

Figura 2.1: Definición de Información. Fuente: elaboración propia.

El ciclo de vida de la información comienza con la búsqueda para posteriormente encontrarla o crearla. Una vez disponible es necesario almacenar esta información y es en este estado en donde puede ser susceptible a ser convertida en un formato digital para ser archivada. A partir de un archivo digital el proceso puede reiniciarse con una nueva búsqueda y luego crear o hacer una actualización de la información existente. La siguiente figura grafica el ciclo de vida de la información.

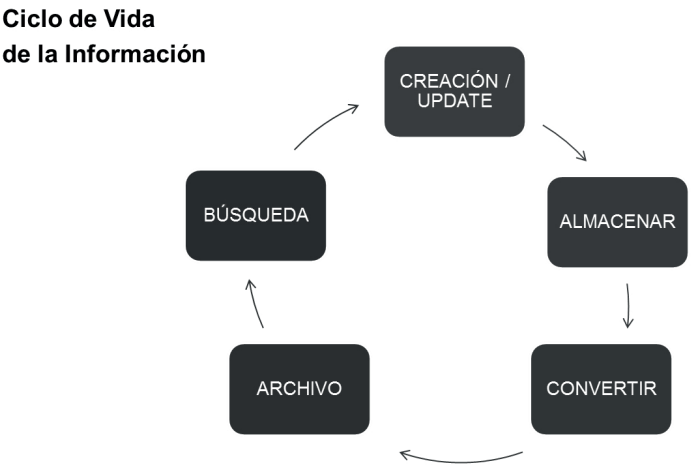

Figura 2.2: Ciclo de vida de la información. Fuente: elaboración propia.

La información puede encontrarse en diferentes estados y dependiendo de estos estados requiere diferentes medidas de protección. Por ejemplo, la información puede encontrarse en "Descanso" sometida a un almacenaje administrativo en archivos impresos o en CDs, como así también en dispositivos móviles tales como discos duros externos, pendrives o en la memoria de un Smartphone. Otro estado y tal vez el más representativo en nuestros tiempos es en "Tránsito" o en transmisión y se refiere a la información que se encuentra en camino a su destino luego de haber sido transmitida o enviada por algún medio, como puede ser un correo electrónico enviado, las líneas físicas de transmisión, tales como cables de red y fibra óptica o a través de ondas de radio en un enlace inalámbrico como el Bluetooth, Wifi, 4G, satelital y otros. El último estado correspondería a la información en "Procesamiento", que correspondería a la información sometida a distintos procesos dentro de una base de datos o simplemente en procesadores.

La protección de la información se basa en tres objetivos internacionalmente reconocidos y aceptados por los distintos especialistas y catedráticos del área. El primero de estos objetivos es la confidencialidad, referida a las medidas tendientes a prevenir la fuga de información hacia individuos o sistemas no autorizados manteniendo la información en el entorno autorizado y para el que fue concebido su acceso. El segundo de estos objetivos es la integridad y autenticidad,

indicando que la información es genuina y de una fuente confiable, que la información no ha sido alterada o modificada y que su autor es de quien se entiende la creó. El tercer objetivo es la disponibilidad, señalando que la información debe estar disponible en el momento que se requiere.

En lo particular el autor considera que un cuarto objetivo a considerar en la protección de la información es plena y totalmente aceptable y dice relación con la trazabilidad y dice relación con que toda la información debe tener un registro indicando quién la generó, cuándo, quién accedió a ella, quien la modificó, envió, recibió, etc. Es decir, que los mismos archivos vayan registrando quienes han accedido a ellos y quiénes y en qué momento los han modificado. Esto es totalmente factible de realizar en cualquier archivo digital. Por ejemplo, un archivo de texto Word, al abrir sus propiedades se podrá acceder a la fecha de su creación, autor, último acceso y otros campos de información relacionados a su trazabilidad. La siguiente figura muestra los objetivos descritos.

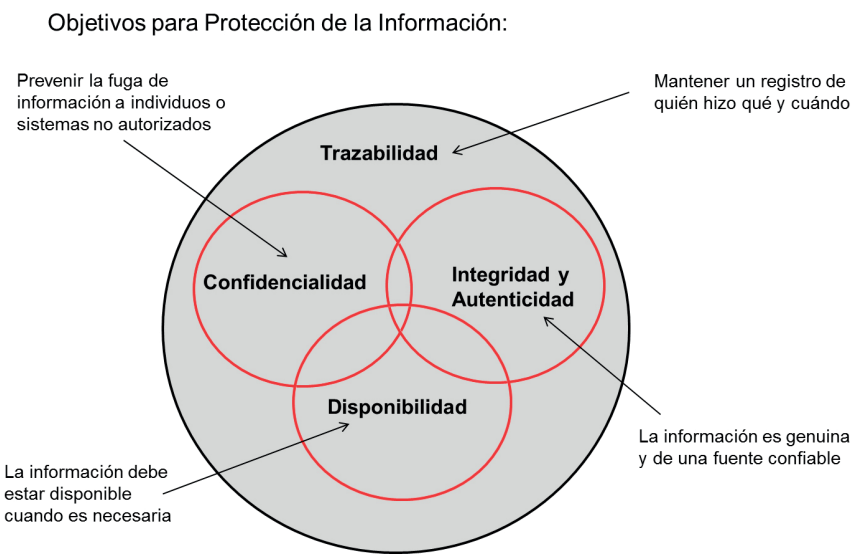

Figura 2.3: Objetivos para la protección de la información.
Fuente: elaboración propia.

La información entonces es un activo esencial del negocio de una organización y requiere en consecuencia una protección adecuada.

Especialmente en ambientes de negocio actuales cada vez más conectados.

Como consecuencia de esa creciente interconectividad, la información está ahora expuesta a un número mayor y a una variedad más amplia de amenazas y vulnerabilidades. Las organizaciones y sus redes y sistemas de información se enfrentan con amenazas de seguridad tales como fraudes informáticos, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daño como código malicioso y ataques de intrusión o de negación de servicios son cada vez más comunes, sofisticadas y de alto impacto. En respuesta a estas amenazas la seguridad de la información es la encargada de disponer de un conjunto de medidas preventivas y reactivas en las organizaciones para permitir resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Se protege la información contra una amplia gama de amenazas para asegurar la continuidad de negocios, minimizar los daños a negocios y maximizar el retorno de las inversiones y las oportunidades, siendo importante tanto para los negocios del sector público como privado, y para proteger infraestructura crítica.

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en ella.

Hasta aquí queda claro que la seguridad de la información no es exactamente lo mismo que la seguridad informática. Por otro lado, la ciberseguridad es definida como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberespacio. La ciberseguridad garantiza que se alcancen y mantengan las propie-

dades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberespacio. Así entonces podemos aceptar que la ciberseguridad involucra y comprende la seguridad de la información como la seguridad informática dentro de su campo de acción.

Para ello existe una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. Comprende software (bases de datos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

Estándares y normas de seguridad de la información

En nuestro país existe la NCh-ISO 27002:2009 [26]- Norma Chilena Oficial: Tecnología de la Información (Código de prácticas para la gestión de la seguridad de la información). El objetivo de este documento es establecer las actividades y protocolos que deben ejecutarse para asegurar la confidencialidad, integridad y disponibilidades de los sistemas de información de una organización. Establece recomendaciones y principios generales para iniciar, implantar, mantener y mejorar la gestión de seguridad de la información de una organización.

Esta norma contiene 11 cláusulas de control de seguridad, que en su conjunto contienen un total de 39 categorías principales de seguridad:

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de los activos.
- Seguridad ligada a los recursos humanos.
- Seguridad física y ambiental.
- Gestión de la comunicaciones y operaciones.
- Control de acceso lógico.
- Gestión de incidentes.
- Planes de contingencia.
- Cumplimiento de requisitos legales.

Entre estas 11 cláusulas, podemos decir que la política de seguridad de la información tiene como objetivo establecer las normas y requisitos de seguridad que permitan garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información de la organización. Es un documento que denota el compromiso del mando con la seguridad de la información y debe contener la definición de la seguridad de la información bajo el punto de vista de la organización.

Los aspectos más importantes a tener en cuenta en la política de seguridad de una organización o empresa son:

- Garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información de la empresa.
- Disponer de un responsable de seguridad encargado de la gestión de la seguridad de la empresa.
- Cumplir los requisitos legales que sean aplicables en la empresa.
- Gestionar las incidencias de seguridad de forma adecuada.
- Disponer de un plan de contingencia que permita a la empresa recuperarse en caso de desastre o discontinuidad de los sistemas. Informar a los empleados de sus obligaciones con respecto a la seguridad de los sistemas, sus obligaciones y los procedimientos definidos que les afectan
- Formar a los empleados en los principales conceptos de la gestión de la seguridad de los sistemas.

Otra de las cláusulas de la norma es la gestión de incidentes cuyo objetivo es resolver de la manera más rápida y eficaz posible, cualquier incidente o no conformidad relacionada con la seguridad de los sistemas. Dentro del procedimiento es necesario definir:

- Fases y actividades a realizar para la gestión de incidencias.
- Flujo básico de una incidencia: registro, clasificación, diagnóstico y resolución.
- Roles que intervienen en el proceso.
- Responsabilidades de los roles.
- Sistema de clasificación de incidencias: niveles de incidentes y criticidad.
- Estructura del registro de incidentes: campos para documentar la incidencia.

- Documentación y registros a generar.
- Documentación y plantillas de referencia.

A continuación, se incluyen algunos ejemplos de incidentes de seguridad:

- Pérdida de servicio, equipos o instalaciones.
- Fallos o sobrecargas del sistema.
- Incumplimiento de políticas o directrices.
- Incumplimientos de los acuerdos de seguridad física.
- Cambios no controlados de sistemas.
- Fallos del software o del hardware.
- Violaciones de acceso.
- Eventos que afecten a la identificación y autenticación de los usuarios.
- Eventos que afecten a los derechos de acceso a los datos.
- Eventos que afecten a los procedimientos de copias de seguridad y recuperación.
- Incidencias que afecten a la gestión de soportes.

Esta norma constituye una segunda versión de un documento aceptado por el Estado de Chile y de amplia aplicación entre las distintas empresas e industrias del país. Esta norma se ha transformado en la biblia de los oficiales de seguridad de la información a nivel nacional y es el referente estándar para implantar, gestionar y auditar los niveles de seguridad de cualquier organización o empresa.

Ataques contra dispositivos

Si nos fijamos en ataques contra distintos tipos de dispositivos, estos pueden oscilar desde teléfonos móviles hasta tablets inteligentes. La gente hoy en día tiende a utilizar una gama más amplia de dichos dispositivos que hace apenas una década. Estos dispositivos, incluidos los que han estado con nosotros durante mucho tiempo, además están equipados con algunas de las posibilidades de comunicación, ya sea a través de una radio de corto alcance o a través de una conexión a internet, lo que suele fomentar las interacciones sociales. Esto, a su vez, significa que tienen más probabilidades de ser atacados.

Si consideramos el amplio uso del término dispositivo nos permite referirnos a un estudio de los muchos tipos de ataques que son posibles. Por ejemplo, a continuación pasamos a discutir los teléfonos inteligentes y otros dispositivos tipo tablets, equipos electrónicos de consumo y pequeños equipos de oficina, como impresoras, routers, sino también dispositivos de streaming de señal de TV y marcos de fotos digitales, RFID, dispositivos médicos, y mucho más. El grupo no es homogéneo, pero diferentes tipos de dispositivos tienen diferentes problemas de seguridad. Por ejemplo, un router siempre conectado a la energía eléctrica puede ejecutar mecanismos de protección más avanzados que un teléfono celular que se lleva en el bolsillo la mayor parte del día. Por otro lado, el usuario puede actualizar el firmware del teléfono celular regularmente para obtener las últimas características, mientras que nunca actualizar el router dejándolo expuesto a antiguas vulnerabilidades.

Algunos de estos dispositivos, especialmente el teléfono móvil, siempre está con nosotros, siempre encendido, y dispone de una gama de sensores que incluye GPS, giroscopio, micrófono, cámara, brújula, sensor de luz, etc. El teléfono móvil también puede comunicarse a través de GPRS, a través de SMS/MMS, a través de Bluetooth, mediante redes locales inalámbricas. También tiene gran capacidad de almacenamiento y la capacidad de realizar transacciones financieras, es decir, realizar una llamada o enviar un MMS. Muchas personas también lo utilizan para acceder a sus bancos o comprar una aplicación que les sea atractiva, útil o entretenida. Por otra parte, funciona con batería y cualquier mecanismo de protección necesita considerar uso de energía. Pero otros dispositivos, tales como los relojes o pulseras biométricas, a menudo pasan por alto los aspectos relativos a la seguridad debido a que son desarrollados por ingenieros de otras disciplinas que pueden no estar conscientes de las implicancias en la seguridad de las comunicaciones inalámbricas.

Los ataques contra estos dispositivos son a veces de naturaleza similar a la de un computador normal, después de todo un teléfono inteligente de alta gama es como un notebook o laptop. Estos dispositivos pueden a menudo no admitir una solución de seguridad completa, como la que se encuentra en un computador

normal. Pueden carecer de mecanismos de seguridad de operación adecuada, operar con firmware antiguos y vulnerables con ningún mecanismo para actualizar parches, o tener muchas vulnerabilidades. También puede ocurrir que el propietario no tenga un control total del dispositivo, por lo que no puede controlar todos los parámetros de este para investigar si se ejecuta algún malware.

Muchos de los ataques y los sistemas de protección los encontramos descritos en recientes conferencias académicas que se centran en la privacidad del usuario y a menudo en la develación involuntaria de la ubicación de los usuarios. Esto incluye ataques contra los teléfonos celulares, el uso de tags RFID (Radio-frequency identification) como los dispositivos para el pago de peajes que se instala en los vehículos para circular en autopistas concesionadas. El seguimiento de dispositivos realmente plantea interrogantes contradictorias, muchas veces es ventajoso realizar un seguimiento de un dispositivo, en algunas circunstancias, pero no en otras. Por ejemplo, el propietario de un servicio de transportes puede querer ver el camino tomado por las mercancías en la cadena de suministro, pero esta información no debe ser filtrada a su competencia. Un usuario puede no querer que su teléfono, ni él mismo sean rastreados, a menos que se lo roben. Una persona puede estar dispuesta a revelar su ubicación automáticamente, pero solo en caso de emergencia o a amigos de confianza.

Se crearon botnets de routers ADSL y los investigadores han descubierto la posibilidad de propagación de gusanos utilizando solo señales bluetooth o wifi. Esas botnets pueden ser utilizadas para ataques de denegación de servicio (DoS) y sorprendentemente se ha demostrado que, en circunstancias especiales, el ataque DoS no depende tanto del ancho de banda disponible. Otro dato sorprendente, sobre malware dirigido a teléfonos móviles es que varias versiones han sido instaladas por el mismo usuario. Han sido disfrazados como troyanos en el mercado de las aplicaciones, o simplemente son tan persistentes en su solicitud de instalación que el usuario termina autorizando el requerimiento.

Con la evolución de los teléfonos celulares a los teléfonos inteligentes, con conectividad a internet y la capacidad de ejecutar software de terceros, era solo cuestión de tiempo para que apareciera

el primer malware. Al principio fue muy notorio que faltaban mecanismos básicos de seguridad de los sistemas operativos. Un gusano masivo se preveía por varios expertos que ocurriría pronto, pero aunque ha habido muchos tipos de malware, ningún gusano ha alcanzado una acción altamente masiva. Un hecho sorprendente es que, los primeros malwares para smartphones requirieron la aprobación del usuario para su instalación. Esto se lograba mediante ingeniería social o por una alta repetición de solicitud de permiso al usuario.

Los teléfonos móviles contienen un amplio conjunto de sensores y a menudo los llevamos con nosotros. La información en los smartphones se encuentra algo más estructurada que en un computador normal y a menudo pueden ser accedidos a través de una aplicación bien definida, como la libreta de direcciones, el historial de llamadas, etc. El smartphone contiene información confidencial. Puede ser utilizado para rastrear nuestros movimientos y registrar la temperatura ambiente, voz o hacer una grabación de vídeo cuando dos personas se reúnen. Las tablets han sido introducidas en el mercado de consumo. En muchos sentidos, el tablet comparte propiedades similares con el teléfono inteligente y a veces incluso el sistema operativo subyacente es el mismo. La siguiente discusión se aplica a menudo a tablets, móviles o portátiles, pero para simplificar la presentación utilizamos el término smartphone.

Ataques contra teléfonos móviles

Para el año 2016 ya existen más de 23 millones de usuarios de teléfonos móviles en Chile. La evolución de este número presentó un crecimiento permanente hasta el año 2012 alcanzando casi los 24 millones de abonados. En los tres últimos años ha experimentado un leve retroceso, pero se mantiene sobre los 23 millones. Esta información proporcionada por la Subsecretaría de Telecomunicaciones es representada en el gráfico de la siguiente figura.

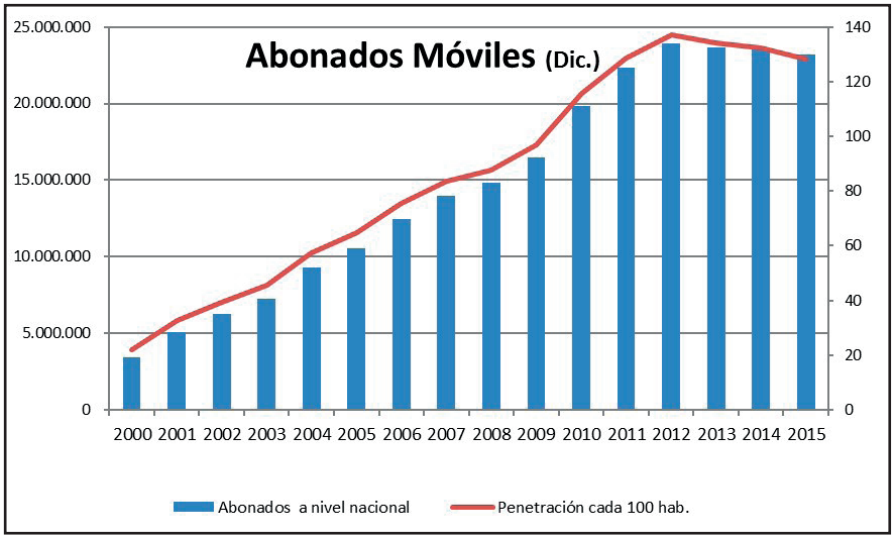

Figura 2.4: Número de abonados totales en el país. Fuente: SUBTEL, sobre la base de la información proporcionada por las compañías móviles. (www.subtel.gob.cl/estudios-y-estadisticas/telefonia/)

Al inicio de 2015 en nuestro país existían 23,6 millones de usuarios de smartphones, que representaban un porcentaje superior al 100% de la población total según la misma Subsecretaría de Telecomunicaciones.

Cada dispositivo actualmente posee una gran cantidad de aplicaciones que alojan, envían y reciben información sensible (como coordenadas de ubicación, saldos, búsquedas, fotos, email, documentos, videos y otros más). El intercambio y manejo de información personal (generalmente sensible) desde los smartphones afecta una gran cantidad de personas que en la gran mayoría de los casos ignoran qué está sucediendo con esa información, dónde está alojada, para qué se utiliza, o incluso que esa información existe en sus dispositivos. Entonces cabe preguntarse, ¿qué ocurre con la seguridad y cuáles son las principales vulnerabilidades de seguridad relacionadas a los dispositivos móviles?

Es por eso que desde los web services y en la aplicación local en el mismo smartphone (y cualquier otro componente que intervenga en el manejo de los datos de usuarios) debe protegerse la integridad y confidencialidad de los mismos como política de seguridad. Algunas

veces, las aplicaciones se publican, comercializan, propagan, etc., con todo su esfuerzo aplicado a las funcionalidades de la misma y la seguridad queda en un segundo plano, o incluso es nula.

Las vulnerabilidades en la tecnología móvil pueden enmarcarse en diferentes categorías. Estas pueden encontrarse explicadas más ampliamente en organizaciones dedicadas como OWASP (Open Web Application Security Project). A continuación se explican, de manera resumida y genérica, las principales 10 vulnerabilidades de seguridad relacionadas a los dispositivos móviles:

- **Controles débiles del lado del servidor.** Este tipo de vulnerabilidades afecta directamente al servidor y la seguridad debe depender exclusivamente del mismo. Las vulnerabilidades que afectan a esta categoría están asociadas a falta de controles y defensas por parte del servidor que espera que los clientes consuman sus servicios a través de parámetros de entrada (inputs de los servicios), que sin las protecciones necesarias puede generar eventos indeseados. No es necesario que los ataques se efectúen desde un equipo móvil, en algunos casos se puede realizar un ataque desde un navegador web o scripts sencillos desde un computador común.

- **Alojamiento inseguro de Información.** Esta vulnerabilidad ocurre cuando información sensible es alojada en el dispositivo móvil con ninguna o pocas protecciones. Es común ver que las aplicaciones utilizan archivos, bases de datos livianas, etc. para guardar datos. Esta información podría ser accedida por malware o usuarios que no deberían tener acceso físico (tener en cuenta que los equipos pueden ser robados). Es por eso que es necesario proteger dicha información no guardando datos a menos que sea absolutamente necesario y con datos que no sean sensibles. Como medida extra se puede recurrir al almacenamiento cifrado. Tampoco hay que confiar en la separación de privilegios del sistema operativo, ya que los equipos pueden ser rooteados (accedidos digitalmente por fuerza).

- **Protección insuficiente en la capa de transporte.** Aquí se presenta el histórico problema en el que las comunicaciones viajan en texto plano y quedan expuestas a cualquiera que pueda observar que

ocurre en la red. Ya sea a través de analizadores de protocolos o cualquier aplicación que pueda ponerse en el medio de la comunicación entre el dispositivo cliente y los servidores a los que se conecta. La mitigación de esta vulnerabilidad es la que desde la seguridad ofensiva se alerta hace años.

- **Fuga de datos involuntaria.** La fuga de datos involuntaria ocurre cuando la aplicación guarda datos sensibles en ubicaciones del dispositivo que pueden ser accedidos por cualquier persona o aplicación. Esto ocurre generalmente sin el consentimiento o sin el conocimiento de los desarrolladores. Es muy común dejar funciones activas como "debug=on" en las aplicaciones desarrolladas y que luego estas en producción comiencen a dejar información sensible en logs accesibles del sistema operativo del smartphone, tablet, etc. La mitigación en este caso pasa por comprender las funciones y particularidades del sistema operativo y los frameworks de desarrollo con los que se trabaja, para evitar funciones por defecto (que desconozcan los desarrolladores) y guarde información en lugares desconocidos.

- **Autenticación y autorización débiles.** Esta debilidad radica en los mecanismos de autenticación y autorización poco efectivos que permiten a un usuario anónimo ejecutar acciones en nombre de un usuario válido o incluso a un usuario válido ejecutar acciones privilegiadas a nombre de otro. Las vulnerabilidades asociadas a la autenticación y autorización débiles consisten en saltar las protecciones de login o funciones de aprobación para realizar determinadas acciones. La manera de mitigar esta vulnerabilidad es asumiendo que los procesos de autorización y autenticación desde el lado del dispositivo cliente son fácilmente "bypaseados" y se deben reforzar con medidas adoptadas desde el lado del servidor.

- **Criptografía rota/quebrada.** Cuando un atacante o software malicioso puede revertir el proceso de cifrado con el fin de llegar a los datos originales estamos frente a la vulnerabilidad de criptografía quebrada. Este problema suele aparecer por el uso de algoritmos de cifrado débil como RC2 o algoritmos de hashing con problemas de seguridad como MD4, MD5, etc. El uso de llaves débiles (generadas sin políticas de contraseñas robustas) también contri-

buye a la posibilidad de romper la criptografía. Algo poco visto pero que debe de tenerse en cuenta es evitar el uso de algoritmos de cifrados propios, asumiendo que el desconocimiento del proceso de transformación bit a bit fortalece un cifrado. Por último, recordar que Base64 no es un cifrado, es un algoritmo de encoding reversible.

- **Inyección del lado del cliente**. Si bien este tipo de vulnerabilidades está dirigido al cliente (dispositivo móvil), los vectores de ataques son varios. El atacante va a intentar realizar acciones maliciosas contra el cliente y no contra el servidor. Las formas de atacar el cliente pueden ir desde levantar un servidor web y esperar a que los clientes se conecten con un navegador web para intentar hacer descargar y ejecutar una aplicación binaria o generar la ejecución de scripts en JavaScript para que el usuario realice acciones indeseadas. La respuesta sencilla para mitigar esto es validar todos los inputs de la aplicación del dispositivo. Es una buena práctica desactivar los plugins de JavaScript y proteger las cookies. Hay aplicaciones que toman variables de servicios web y en base a eso realizan consultas a su propia base de datos. Esto puede aprovecharse para realizar ataques de inyección SQL, así que es importante también validar en la aplicación cliente los datos ingresados (validar inputs).

- **Decisiones de seguridad a través de entradas no confiables**. Esta vulnerabilidad se presenta cuando la aplicación utiliza datos que suelen estar ocultos en la misma aplicación para permitir funcionalidades especiales (como niveles de accesos, aprobaciones, etc.). Un atacante malicioso podría cambiar un valor dentro de la aplicación, comunicación (servicios web) o incluso interferir un proceso y alterar el funcionamiento de la aplicación para que la misma realice acciones especiales o les dé acceso a estas acciones. La mitigación de esta vulnerabilidad es controlar los procesos y también tener una lista blanca de aplicaciones conocidas.

- **Mal manejo de sesiones**. El mal manejo de sesiones ocurre cuando un token de sesión (sobre protocolos como HTTP ó SOAP) se mantiene en el servidor por un período de validez muy largo, cuando la generación del token carece de complejidad (como por

ejemplo que el token esté compuesto por el nombre de usuario y la fecha de login) o la longitud es muy corta. Utilizar los mismos tokens (cookies) previas a la autenticación, también está considerado como mal manejo de sesiones. Para mitigar esta vulnerabilidad es necesario mantener la premisa de seguridad en las sesiones desde el desarrollo, mantenimiento y eliminación de tokens de sesión.

- **Ausencia de protecciones de binarios**. En un resumen rápido, esta vulnerabilidad radica en la posibilidad de analizar y modificar la aplicación en el dispositivo móvil. Esto normalmente está ligado a la realización de ingeniería inversa. Es muy difícil implementar un único mecanismo de control final que mitigue por completo esta vulnerabilidad. Sin embargo, es posible minimizar el riesgo a través de varias capas de seguridad como, por ejemplo:

  • Controles de "certificate pinning".
  • Controles de "checksum".
  • Detecciones de debuggers.
  • Detección de rooting del dispositivo.

La mayoría de las aplicaciones para los dispositivos móviles poseen vulnerabilidades de seguridad. Es altamente recomendable el desarrollo de las aplicaciones móviles en un entorno seguro en las distintas fases del ciclo de vida del desarrollo de la aplicación.

El proceso de manejo de incidentes móviles implica controlar y minimizar el daño, preservar la evidencia, proveer una recuperación rápida y eficiente, prevenir eventos similares en el futuro y ganar entendimiento de los riesgos que enfrenta la organización. Para las empresas que están comenzando a mejorar su seguridad móvil, una buena práctica es comenzar con un modelo de proceso sencillo para luego modificarlo acorde a la experiencia con el paso del tiempo, teniendo en cuenta los recursos disponibles, la cantidad de incidentes y la criticidad de estos eventos.

Un problema grave de la seguridad de dispositivos móviles se presenta cuando las herramientas de seguridad no son suficientes y las infecciones logran afectar a los dispositivos. Qué se debe hacer

y cuáles son las acciones a seguir. Algunas formas de contener y mitigar los efectos en equipos móviles comprometidos son los siguientes [2]:

- **Registrar el evento.** Es necesario contar con herramientas que permitan rápidamente generar un registro del evento, incluyendo un identificador único y adjuntando algunas palabras claves que lo describan, la fecha en que este tuvo lugar y las características de los equipos damnificados, tanto del hardware como de las aplicaciones que en él se encontraban instaladas.

- **Priorización del evento.** Una vez que ha sido registrado, es necesario asignarle una prioridad con base en la criticidad que este incidente tiene para los activos de información organizacional y el normal desempeño de las empresas. Puede ser una explotación de vulnerabilidades, inconsistencias en el acceso y autenticación, o puede ser una infección por malware. Luego de clasificar el tipo de evento, es necesario asignar una categoría (prioridad alta, media o baja) y un responsable para la solución del conflicto. Por supuesto, el último paso en esta segunda etapa del proceso será la emisión del reporte pertinente.

- **Resolución del conflicto.** El tercer paso consiste en subsanar el incidente. Esto implica realizar un proceso cíclico de análisis de datos, investigación de lo que ocurrió, generación de una propuesta de solución, remediación y recuperación. Esto implica el aislamiento del dispositivo infectado, la identificación de los stakeholders y contactarlos para alertar o recopilar información importante, descubrir cómo se inició la infección, recolectar la muestra, determinar qué realiza la amenaza, a dónde se conecta y demás. Es necesario tener cuidado al utilizar herramientas de análisis que hacen conocer sus reportes de manera pública, ya que el código de la amenaza podría contener información sensible de la empresa en caso de tratarse de un ataque dirigido. Como resultado de esta actividad se deberá mejorar el reporte del incidente que fue creado al momento de registrar el evento, incluyendo registros de dominios, archivos de captura de tráfico de red, registros y cualquier otra nueva información arrojada por el análisis de la contingencia. Esta etapa también incluirá la desinfección del equipo.

- **Etapa de posanálisis.** Finalmente, es necesario aprender de los errores cometidos a lo largo del proceso de manejo de contingencias, con el objeto de mejorar el tiempo de respuesta e identificar qué nuevas herramientas pueden ser desarrolladas o adquiridas para optimizar tanto la protección de los equipos como la respuesta ante los sucesos que pueden poner en peligro la seguridad empresarial.

Hay varias taxonomías que describen los ataques contra teléfonos móviles, teniendo en cuenta la motivación del atacante, el vector de infección o el ataque resultante a la red. Uno de los mayores riesgos de un pequeño dispositivo portátil es su robo. Por este motivo, al principio los mecanismos de protección se centraron en el proceso de autenticación del usuario, a menudo a través de una contraseña sencilla y la capacidad de borrar de forma remota toda la información sobre el teléfono. Sin embargo, un reciente ataque indica que es posible adivinar el patrón de la contraseña en un teléfono táctil por estudiar el residuo aceitoso dejados por los dedos del propietario.

Dada la información personal que recopila y almacena el teléfono, muchos esfuerzos de investigación y varios ataques se enfocan en las fugas de información privada en general. Mirando más específicamente a la ubicación del usuario y la capacidad de realizar un seguimiento de su movimiento, hay varios ataques y estudios. Uno de los eventos más relevantes es la fuga inadvertida por Apple. Apple utilizaba un caché sin cifrar para poder localizar un usuario más rápido que utilizando únicamente el GPS. Después de una protesta pública, la compañía respondió y redujo el tiempo que se guardaban los datos.

Algunas investigaciones han demostrado cómo un usuario puede ser rastreado en un área metropolitana, si el teléfono está buscando activamente una red wifi por la difusión de un identificador único. Se llegó a determinar cuántos dispositivos de rastreo debe ser capaz de controlar un hacker para realizar el seguimiento de un usuario de forma eficiente. Técnicas similares, aunque sin enlazar el identificador exclusivo para el usuario real, ya están siendo utilizadas. En este sentido el aeropuerto de Copenhague ha anunciado que utilizará una técnica similar para hacer el seguimiento (anónimo) de los pasajeros y utilizar estos datos para construir un mejor y más estructurado ae-

ropuerto. Afirman que no se realiza un seguimiento de información de pasajeros, solo de los "teléfonos". No obstante, la geolocalización ofrece nuevas oportunidades y servicios. A muchos usuarios no les importa compartir su ubicación con un tercero de confianza y con algunos amigos. Sin embargo, esta información puede ser filtrada por ejemplo si los terceros de confianza tienen empleados deshonestos que pueden utilizar esta información. Se han desarrollado esquemas en los que la confianza solo se otorga a los usuarios si han estado en el mismo lugar antes. De esa manera, no hay necesidad de confiar en un repositorio central y nuevos tipos de servicios son posibles porque se puede compartir información con un amplio rango de personas y no solo con sus amigos más cercanos.

Exploits y gusanos

Como se ha descrito anteriormente, existen registros de varios malwares históricos dirigidos contra teléfonos móviles. Algunos de estos han requerido el permiso del usuario para instalarse, en función de las técnicas de ingeniería social o de defectos en las interfaces de usuario. Sin embargo, también existen ataques que no requieren ninguna o poca interacción del usuario. Una muy grave y reciente vulnerabilidad se basa en enviar un SMS especialmente diseñado a un iPhone o un teléfono con Android, con lo que es posible hacer perder toda la conectividad de la red, resultando en un tipo de ataque de denegación de servicio. Otros intentos han permitido la ejecución de comandos arbitrarios en los iPhone sin ninguna interacción por parte del usuario. El servicio de manejo de mensajes SMS, CommCenter, se ejecutaba como root a diferencia con el explorador web que es sandboxed (aislado). Especulando, muchos ataques anteriores han sido relacionadas con la web, lo que significa que los desarrolladores son más conscientes de los riesgos de seguridad a través de este medio y no han aplicado los mismos mecanismos de seguridad a otros métodos de comunicación.

Un exploit anterior usó una imagen TIFF especialmente diseñada para ejecutar código malintencionado. Así un archivo MP3 especialmente diseñado podría desencadenar un incidente en teléfonos Android y posiblemente la ejecución del código malintencionado. El ataque es muy simple, si los usuarios no han cambiado la contraseña por defecto del SSH el malware podría conectarse de manera sencilla utilizando la contraseña predeterminada que es "alpine".

Se ha estudiado la propagación de gusanos que casi exclusivamente utilizan la conexión vía bluetooth. En las áreas metropolitanas, estos gusanos son una amenaza real y pueden tener un gran impacto debido a que un gusano podría saltar a través de la conexión local entre dos teléfonos, y así no pasar a través del núcleo de la red celular donde podría ser detectado y filtrado. Se ha estudiado un problema similar; como un gusano que puede propagarse mediante redes wifi en áreas metropolitanas densamente pobladas. Aunque sus resultados no son particularmente efectivos contra todos los teléfonos móviles, demuestran que, en determinadas circunstancias, es posible llegar a un 80% de todos los hosts dentro de 20 minutos.

Los teléfonos también tienen la posibilidad de ser controlados remotamente por el usuario. Conectándose al teléfono, uno puede enviar SMS, subir vídeos, ver los registros de llamadas, etc., incluso aunque tales funciones hacen que sea más fácil para el usuario poder administrar su teléfono, esto constituye en sí otro tipo de interfaz que pueden ser explotada para realizar ataques.

Ataques de Denegación de Servicios (DoS)

Cuando es posible tomar el control de un gran número de hosts, estos pueden ser utilizados fácilmente para un ataque de DoS tradicional. Sin embargo, es bastante fácil atacar a los servicios de la red celular desde dispositivos malintencionados en la misma red. Ellos muestran que, en circunstancias especiales, el ataque de DoS no depende tanto del ancho de banda disponible si no de problemas con la conexión de la red celular a internet. Estos dos tipos de redes tienen principios de diseño fundamentalmente opuestos y, a veces, estas diferencias pueden crear vulnerabilidades. Se demostró que el principio de ataque se basa en la solicitud del registro de ubicación, pero también se propuso contramedidas para este ataque [3].

Estrategias de protección general

Proteger el teléfono móvil de malware es un tema de investigación muy activo y aquí tenemos una lista de investigaciones recientes que ofrece identificación general o estrategias de protección. Una de las principales dificultades se basa en la limitada cantidad de energía disponible en el teléfono celular. Cualquier nuevo programa que eje-

cuta usará más energía, lo que significa que el teléfono debe estar cargado con más frecuencia. Esto en realidad se convirtió en una estrategia de defensa como lo explica por Lei Liu [4]; de igual forma los malwares consumen más energía. Al modelar el consumo de energía, su herramienta Virus Meter puede detectar el uso malintencionado. Se ejecuta en dos modos. Se realizan análisis ligeros cuando el teléfono está utilizando la batería y un análisis más pesado se hace cuando el teléfono se está cargando. Otros utilizan también el consumo de energía para detectar malware, esto debido a que el objetivo de algunos ataques es descargar las baterías y, por lo tanto, realizar una especie de ataque de denegación de servicio (DoS) contra el teléfono.

Otros dispositivos

Otros dispositivos, generalmente ignorados por los expertos en seguridad, son llamados dispositivos SoHo, es decir, dispositivos que se pueden encontrar en una pequeña oficina o una oficina en casa. La electrónica de consumo, como los reproductores de música también corren el riesgo de verse comprometidos, aunque la mayoría de la gente no consideraría la posibilidad de ser blanco de estos ataques.

Uno de los más prominentes dispositivos que son utilizados para la propagación de ataques es el pendrive USB. A pesar de que sus vulnerabilidades son bien conocidas, puede causar problemas incluso a los usuarios más conscientes de la seguridad y ha sido utilizado para atacar instalaciones que han sido altamente segurizadas.

Las impresoras son de naturaleza similar a la de un computador y pueden ejecutar una amplia gama de servicios. Por ejemplo, la interfaz web viene y está protegida desde fábrica por una contraseña predeterminada que, por desgracia, no es usual cambiarla. Sin embargo, incluso cuando se cambia hay todavía una serie de vulnerabilidades que pueden ser utilizadas para un ataque. A pesar de que los ataques que utilizan una impresora pueden parecer como una posibilidad remota, ya han sido explotados. En 1999, una impresora situada en el Space and Naval Warfare Space System Command, de la Armada de Estados Unidos, fue hackeada y las tablas de enrutamiento fueron cambiadas. Los archivos de la cola de impresión se dirigieron hacia Rusia y luego volvieron. De esta manera el atacante podía mantener una copia o incluso cambiar el contenido de los archivos que se im-

primieron. Pero otros tipos de equipos, tales como cajas registradoras, cajeros automáticos, puertas, controles de acceso y sistemas de CCTV, también pueden ser vulnerables a ataques similares.

Los dispositivos pueden no ser directamente atacados, pero si influenciado por los ataques contra la red que les brinda soporte. Un ejemplo reciente de tal actividad fue el ataque contra la red de Sony PlayStation, que tuvo dos consecuencias tales como la publicación de información sensible de sus usuarios, así como la desconexión de los dispositivos. Incluso se especuló que este ataque era un intento de controlar la red que emite actualizaciones a las consolas, pudiendo así comprometer y controlar millones de estos artefactos.

Los tags RFID contienen un diminuto chip miniaturizado que se alimenta por medio de inducción. Debido a su tamaño, así como su bajo costo, es que pueden ser conectados a casi cualquier cosa. Se pueden encontrar en tarjetas-llave (para habitaciones de hotel), pases para el pago de transporte público (tarjeta bip), pasaportes, licencias de conducir, mascotas, ropa, y a menudo se utilizan en la gestión de cadenas de suministro.

Los vehículos y aviones, también están profundamente interconectados. De hecho, un auto moderno puede contener entre 50 a 90 computadores y, por lo tanto, su red interna se compone de un gran número de dispositivos. La seguridad de la red de un auto y de los dispositivos que lleva ha sido investigada experimentalmente y se ha encontrado que es factible anular el ingreso de data que el conductor haya hecho, incluso de forma remota. Otros han estudiado el sistema de apertura pasiva y las vulnerabilidades de seguridad-privacidad relacionados con el sistema de monitoreo de presión de neumáticos. Así, tanto autos como teléfonos móviles pueden ser utilizados para rastrear la ubicación de sus propietarios. Entonces para sistemas de control de peajes en carreteras, control de congestión del tráfico, así como otros servicios, existe una razón válida para el seguimiento de los movimientos de los vehículos.

Algunos dispositivos médicos también han demostrado ser vulnerable a los ataques. Por ejemplo, se han registrado ataques en contra de marcapasos y otros dispositivos médicos implantables. Estos dispositivos suelen contener información valiosa para el personal de emergencia, y

esa información que puede salvar vidas se puede leer fácilmente. Por otro lado, dicha información no debería estar disponible para otros.

En una sociedad moderna, utilizamos una amplia gama de dispositivos para simplificar la vida, tanto a nivel de consumidores como así también de usuarios de un carácter más crítico. Para ofrecer más y mejores servicios, estos dispositivos son a menudo conectados entre sí y pueden ser atacados y controlados de forma remota por un adversario malicioso. Los malwares que se han focalizado en dispositivos, hasta ahora comparativamente han seguido un desarrollo similar a los malwares dirigidos contra computadores regulares, y es probable que continúen haciéndolo. Varias veces se ha anunciado ataques a gran escala, especialmente para teléfonos móviles, pero aún no han alcanzado un nivel crítico. Sin embargo, existen numerosos incidentes, entre los últimos el ataque ya mencionado contra la red PlayStation de Sony, mostrando cómo millones de usuarios pueden ser afectados incluso por ataques no dirigidos a los dispositivos directamente.

Denegación de servicio, un análisis más amplio

Según las noticias el 6 de agosto de 2009, Twitter fue cerrado por horas, silenciando a millones de tweeters. Desde el punto de vista del usuario, la primera indicación que se recibió de esta falla en el servicio fue que "El sitio está abajo"; en realidad no solo era que el sitio estaba abajo, sino que todas las aplicaciones de clientes que dependían de la API de Twitter no pudieron conectarse al servicio, creando un completo apagón de esa red social. Según Twitter, admitió que esta falla en el servicio fue causada por un ataque de denegación de servicio.

Un ataque de denegación de servicio (DoS) es un intento del atacante para impedir que los usuarios legítimos de un servicio puedan utilizar ese servicio. Generalmente hablando, cualquier ataque que pueda saturar o agotar los recursos del sistema o dejar el sistema en un estado erróneo, a veces incluso bloquear el sistema, debe ser considerado como un ataque de denegación de servicio. El concepto detrás de los ataques de denegación de servicio no es nuevo, la idea de ataque en general ha estado con nosotros por más de veinte años y aún sigue evolucionando.

Los motivos para lanzar un ataque de denegación de servicio pueden variar. Algunas personas pueden simplemente querer mostrar sus habilidades o demostrar que han encontrado algunas vulnerabilidades de algunos sistemas. El incentivo económico es otra razón poderosa para lanzar un ataque de denegación de servicio. Una empresa puede beneficiarse de lanzar ataques contra sus competidores, o probablemente, la empresa en cuestión contrata a terceros para lanzar el ataque real y de esa forma prevalecer en la industria en que compite.

Por otro lado, cuando el agresor tiene la capacidad de lanzar un posible ataque de denegación de servicio, puede en cambio chantajear a la víctima a pagar para que el ataque no se concrete. Aparte de la propia ganancia, también ha habido varios ataques con motivación política. Los incidentes en Estonia [5] y en Georgia [6] son ejemplos de tales ataques motivados políticamente.

Independientemente de la razón detrás de los ataques, las pérdidas resultantes pueden ser muy importantes. Cuando los objetivos son sitios web o servicios de grandes empresas o gobiernos, las pérdidas pueden ser incluso de millones de dólares [7].

Como los ataques de denegación de servicio han sido tan frecuentes y porque el daño resultante puede ser importante desde un punto de vista económico, la mitigación de estos ataques es un área de investigación muy activa, tanto para la industria y el mundo académico. Sin embargo, prevenir o mitigar los ataques de denegación de servicio no es fácil. Algunos tipos de ataques aprovechan una vulnerabilidad en una aplicación de software, el que puede ser corregido. Otros pueden utilizar un defecto de diseño, o incluso simplemente un método de fuerza bruta para sobrecargar los procesos de la víctima.

Entonces, ¿cómo son estos ataques? El atacante puede estudiar las fallas de los protocolos de comunicación (o sus implementaciones) e insertar paquetes incorrectos o falsos para interferir las comunicaciones legítimas. Este tipo de ataque puede ser llamado ataque semántico. Sin embargo, el atacante no necesita inspeccionar la implementación de protocolos, si es posible inundar con tráfico aparentemente legítimo y congestionar la red de la víctima o mantener

el host de la víctima ocupado procesando los paquetes, así, de cualquier manera, los clientes legítimos no serán atendidos. Este tipo de ataque a menudo se conoce como ataque de fuerza bruta. Para tener éxito inundando con paquetes y saturar la red de la víctima, el atacante a menudo utiliza muchas máquinas comprometidas o zombies para enviar tráfico simultáneamente, esta es una forma de ataque llamado ataque de denegación de servicio distribuido (DDoS). En la siguiente figura se puede ver la arquitectura de un ataque del tipo DDoS.

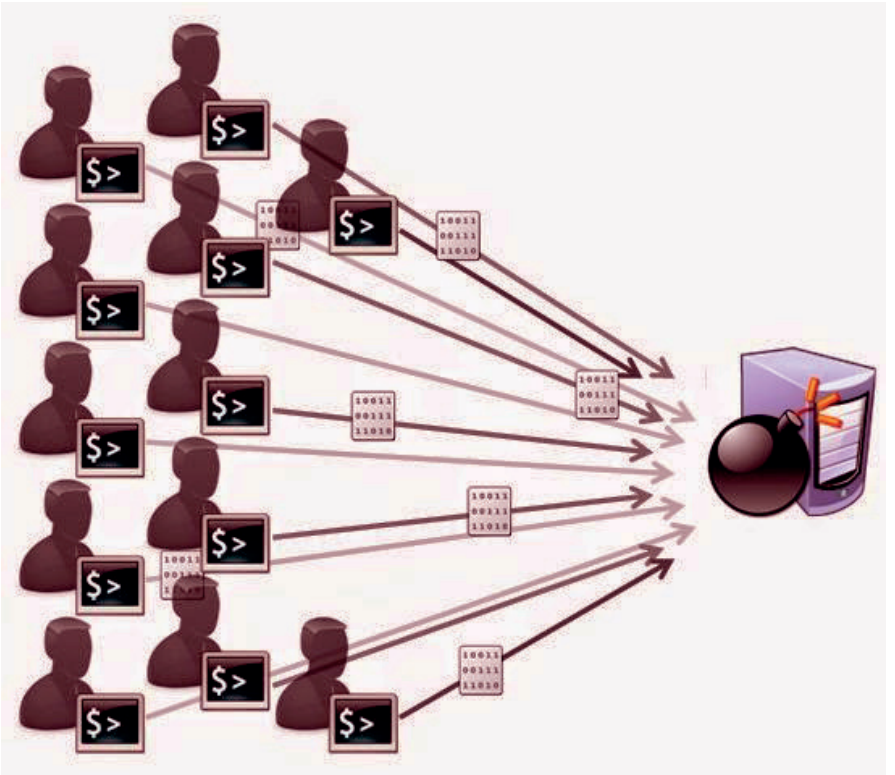

Figura 2.5: Arquitectura de un ataque del tipo DDoS. Fuente: www.blackophn.blogspot.cl/2015/05/tutorial-realizando-ataques-dos-con.html.

En Chile se han registrado incidentes de DDoS en los servicios en que el retail ha ofrecido ciberdescuentos coincidiendo todos en una fecha en particular y, originalmente, cuando sus estimaciones de requerimientos fueron superadas por la demanda real de los clientes online. Así, sus servicios se vinieron al suelo, dejando de atender a sus clien-

tes, quienes en masas generaron un ataque involuntario. Esto es el equivalente a que unas mil personas concurran al banco a cobrar un cheque y todas sean atendidas al mismo tiempo solo por un cajero y en la misma ventanilla, lo que traerá ciertamente como consecuencias que ese cajero colapse y no pueda continuar con su servicio.

Existe además una categoría de ataques de denegación de servicios llamados ataques DoS permanentes o no recuperables. Los ataques no recuperables infringen daños permanentes al hardware de la víctima, el reemplazo o la reinstalación del hardware es entonces necesario para restaurar la función. Pero este tipo de ataque no ha demostrado ser común.

Las páginas web de diversas instituciones gubernamentales y empresas han sido atacadas mediante ataques de denegación de servicio, por "comunidades" o "activistas" en internet, para manifestar su rechazo y malestar ante diferentes situaciones. Por lo general estos ataques han sido públicamente coordinados. Estas agresiones pueden terminar con la caída del sitio atacado, generando para la institución o empresa afectada la imposibilidad de prestar servicios a través de él. Esta situación no solo puede provocar un deterioro en la imagen de la víctima, sino que además entorpecer sus actividades, y generar responsabilidad legal vinculada con la no prestación de servicios o la pérdida de datos.

Los ataques de DoS y DDoS están basados en la saturación de los sistemas por exceso de solicitudes, esto desborda los sistemas víctima y genera la denegación, por lo tanto, contar con infraestructura superior permite resistir el ataque. Para lograr esto se puede contratar los servicios de empresas que ya cuentan con megainfraestructuras y son naturalmente más resistentes a estos tipos de ataques, como por ejemplo, Akamai, Google, Amazon y algunos ISP´s (internet Service Providers). La desventaja está en los costos asociados a estas soluciones.

Teardrops

Para este tipo de ataque, el agresor envía fragmentos ip incorrectos al destino a atacar. El equipo de destino se puede bloquear si no posee implementado correctamente el código de reensamblado de fragmentación del protocolo TCP/IP. Este tipo de ataque se puede

prevenir mediante la corrección de bugs en la implementación ip de los sistemas operativos.

Ping of death

Un ping of death es un ataque donde el atacante envía a la víctima un paquete ping que es mayor que 65,535 bytes. Anteriormente, muchos sistemas operativos no podían manejar esos grandes paquetes de ping, así este ataque da lugar a un bloqueo del sistema.

Ataque SYN

En este ataque, el atacante aprovecha una asimetría en el protocolo TCP. El receptor debe mantener el estado cuando una conexión está a punto de establecerse, pero un remitente malintencionado no lo necesita hacer. Cuando se recibe un paquete TCP/SYN, el receptor almacena el estado en la memoria esperando la finalización del enlace (o un tiempo de espera). Si el atacante continúa enviando paquetes TCP/SYN sin enviar el paquete ACK final para el protocolo de enlace TCP, los recursos del servidor pueden ser rápidamente agotados producto de mantener muchas sesiones a medio abrir. Aunque la asimetría todavía existe, fue un problema mucho mayor en el pasado debido a que la tabla asignada para estas conexiones a medio abrir, en muchos sistemas operativos era de un tamaño limitado.

Ataques de fuerza bruta

Hay muchas variantes de ataque de fuerza bruta, y se usa el ancho de banda de los ataques DDoS como un ejemplo donde muchas máquinas generan de forma simultánea una inundación con paquetes a la víctima, logrando así un efecto de amplificación por el uso de muchos hosts.

El objetivo de los ataques DDoS pueden ser hosts y de infraestructuras de internet (ej. Servidores DNS, routers de núcleo). Un procedimiento típico de un ataque DDoS es mostrado en la Figura 2.6. Básicamente, existen dos fases en un ataque DDoS. En primer lugar, el atacante aprovecha alguna vulnerabilidad para reclutar máquinas, que luego pueden ser utilizadas como agentes de ataque. Los resulta-

dos se conocen regularmente como una botnet, donde los hosts comprometidos son llamados zombis. El procedimiento de búsqueda de equipos vulnerables para luego convertirlos en agentes de ataque se puede realizar de varias maneras. El atacante puede utilizar troyanos o gusanos que aprovechan una nueva vulnerabilidad, como el gusano Code Red [8]. Después de la fase de reclutamiento, el agresor puede lanzar un ataque mediante el envío de un comando a los agentes de ataque (zombies) mediante máquinas maestras o a través de canales de comunicación IRC.

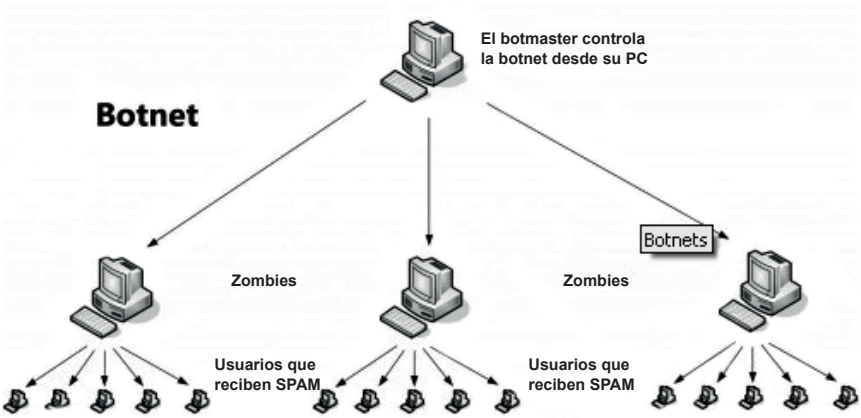

Figura 2.6: Ataque DDoS típico. Fuente: Elaboración propia.

Para cubrir su verdadera identidad, el atacante normalmente recluta zombis con la ayuda de máquinas máster. El atacante primero compromete e infecta a uno o más masters, cada uno de los masters puede comprometer muchos zombies, como se puede apreciar en la Figura 2.6.

Una reciente e interesante tendencia consiste en que el atacante puede montar la botnet a través de la participación voluntaria de las víctimas, si hay una causa común. Un ejemplo de esto fue el ataque orquestado contra organizaciones tales como, Visa.com Mastercard.com, PayPal y Post Finance en el año 2010. Este ataque fue organizado por un grupo llamado “anonymous” para mostrar su indignación por la injusticia contra Wikileaks. El ataque se inicia con una herramienta de ataque llamada LOIC [9], que puede dirigir

a los voluntarios para atacar los sitios web indicados. La herramienta de ataque es fácil de descargar y utilizar. El ataque fue incluso más desarrollado y al final solo requiere que los voluntarios visiten un sitio web para sumarse al ataque. Por lo tanto, no se necesitan habilidades de experto, solo se requiere conocer el sitio web correcto y hacer clic en un botón.

Según se puede entender, un ataque DDoS es más potente que un ataque de denegación de servicio por si solo, ya que puede fácilmente agregar un gran volumen de tráfico malicioso y agotan rápidamente los recursos de la red de la víctima. Muchos de los tradicionales ataques DoS pueden ser fácilmente convertidos en más poderosos ataques de DDoS. Un tipo simple de ataque DDoS se logra haciendo una saturación por ping. Un ataque de saturación de ping puede ser iniciado por una sola máquina atacante. Sin embargo, es más eficaz si el ataque se usa en un ataque DDoS, con muchas máquinas eco enviando paquetes ICMP (ping) de forma simultánea a la víctima. Como el atacante puede obtener un muy gran ancho de banda utilizando muchas máquinas comprometidas, es muy fácil sobrepasar la red de la víctima debido a la asimetría de los recursos de ancho de banda, incluso si la víctima es un gran proveedor de servicios.

IP Spoofing

El atacante puede utilizar direcciones ip falsificadas en los paquetes maliciosos para cubrir la verdadera identidad de los hosts de ataque. La suplantación de ip puede afectar la precisión de las contramedidas de los ataques DDoS. Además, dado que la mayoría de los mecanismos de prevención de ataques utilizan direcciones ip para identificar el origen de los ataques, los hosts inocentes pueden encontrarse bloqueados porque sus direcciones fueron suplantadas por algún intruso.

Hay muchas soluciones contra la falsificación de direcciones ip, sin embargo, cualquier solución que se base en la autenticación de mensajes es potencialmente vulnerable a ataques de denegación de servicio. El filtrado de entrada puede resolver el problema completamente. Un atacante puede falsificar una dirección de subred del agente atacante, o falsificar una dirección de reenvío en la ruta de los paquetes enviados hacia el destino.

Peer to Peer

Las redes peer to peer pueden ser utilizadas en los ataques DDoS, donde dos de las más comunes son el envenenamiento del índice y el envenenamiento de la tabla de enrutamiento. En el ataque de envenenamiento de índice, el objetivo del atacante es hacer que varios peers crean que algunos archivos populares están presentes en el host de la víctima. Para lograr esto, el atacante envía un registro de índice falso con la dirección ip de la víctima y el número de puerto para todos los otros nodos. Cuando un nodo desea descargar este archivo en particular, va a realizar una conexión a la víctima. Durante un breve momento, pueden existir muchas conexiones a la víctima, consumiendo dramáticamente los recursos de la víctima. En el ataque de envenenamiento de la tabla de enrutamiento, el objetivo del atacante es hacer que los peers agreguen a la víctima como su vecino.

Desde su primera aparición, el ataque de denegación de servicio ha cambiado de forma y sofisticación. Como se mencionó anteriormente, hay muchos tipos de ataques de denegación de servicio. La aplicación inadecuada de los protocolos de red y el mal diseño o implementación de servidores de aplicaciones puede ser aprovechado por el agresor, dando lugar a ataques de denegación de servicio. Estas vulnerabilidades pueden muchas veces ser solucionadas a través de parches de software. Sin embargo, el riesgo de los ataques de denegación de servicio no se ha eliminado incluso si el sitio web está bien implementado y actualizado regularmente. Aún puede ser atacado con éxito por un ataque de fuerza bruta. Se dice que, independientemente de cuán bien asegurado pueda estar el sistema víctima, su susceptibilidad a ataques de DDoS depende del estado de la seguridad en el resto de la internet global. Aún peor, un ejército de bots pueden ser formado por voluntarios. Su participación en el ataque no es porque su equipo esté comprometido, sino porque quieren y apoyan la causa del ataque. Por ese motivo, el problema DoS, ya no es solo un problema técnico de seguridad, sino también un tipo de ataque donde los temas y los grandes conflictos de la sociedad ya juegan un papel originador de ataques.

INFRAESTRUCTURA CRÍTICA

Según la definición de la "Directiva sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección" [10] el término "Infraestructura Crítica" para la UE significa: *"... son instalaciones, sistemas o partes de sistemas situados en los Estados miembros de la UE que son esenciales para el mantenimiento de las funciones vitales de la sociedad, la salud, la seguridad, la economía o el bienestar social de las personas, y la alteración o destrucción de uno tendría un impacto significativo en un Estado miembro como consecuencia de la incapacidad de mantener esas funciones..."*. La citada directiva es una consecuencia del "Programa Europeo de Protección de Infraestructuras Críticas" [11], que se refiere a la doctrina y los programas creados para identificar y proteger la infraestructura crítica que, en caso de anomalía, incidente o ataque, podría afectar gravemente tanto al país donde está alojada y/o al menos otro Estado miembro de la Unión Europea (Programa Europeo de Protección de Infraestructuras Críticas).

En el "Análisis de Escenarios" [12] del proyecto IST IRRIS (Reducción del riesgo integral de los sistemas de infraestructura basados en información), las siguientes definiciones pueden ser una referencia para su utilización posterior en este ensayo:

- **Infraestructura (I):** una infraestructura constituye un marco de interdependencia de las redes y sistemas que comprenden industrias identificables e instituciones (incluyendo a personas y procedimientos), y/o la distribución de capacidades que proporcionan un flujo fiable de productos, suministros y/o servicios, para el buen funcionamiento de los gobiernos a todos los niveles, la economía y la sociedad como un todo y de otras infraestructuras.

- **Infraestructura crítica (IC):** una infraestructura crítica es una infraestructura a gran escala que, si se degrada, interrumpe o se destruye tendría un grave impacto sobre la salud, la seguridad o el bienestar de los ciudadanos o en el eficaz funcionamiento de los gobiernos y/o la economía.

- **La infraestructura crítica de la Información (ICI):** son procesos de información soportados por la tecnología de la información

y de la comunicación (TIC), que son las infraestructuras críticas para ellos mismos o que son críticos para el funcionamiento de otras infraestructuras críticas.

- **Protección de infraestructura crítica (PIC):** son programas y actividades de los propietarios de las infraestructuras, fabricantes, usuarios, operadores y autoridades reguladoras, que apuntan a mantener el rendimiento de las infraestructuras críticas en caso de desastres naturales, fallas, errores humanos, ataques o accidentes por encima de un nivel mínimo de servicios, definidas y orientadas a minimizar el tiempo de recuperación y el daño.

- **Protección de infraestructura crítica de la Información (PICI):** son programas y actividades de los propietarios de las infraestructuras, fabricantes, usuarios, operadores y autoridades reguladoras que apuntan a mantener el rendimiento de las infraestructuras de información crítica en caso de fallas, ataques o accidentes por encima de un nivel mínimo de servicios definidas y orientadas a minimizar el tiempo de recuperación y el daño. La PIC es más que la PICI, que es solo un subconjunto de un amplio esfuerzo de protección, ya que se centra en la infraestructura crítica de la información. Pero en publicaciones oficiales, ambos términos se usan a menudo para un mismo significado.

Los ciberataques solo son posibles a través de las TIC, los componentes de IC que implican y consideran a la ICI. La infraestructura crítica y especialmente el ICI se ha vuelto muy vulnerable a los terroristas, los delincuentes y las personas que buscan diversión como hackers, crackers, y otros. Las herramientas utilizadas para atacar las IIC son similares a cualquier otro tipo de herramientas para ejecutar ciberataques en general. Esos tipos de ataques, incluyen entre otros:

- Acceso no autorizado a información sensible o confidencial.
- Destrucción, modificación o sustitución de software necesario para la operación de las infraestructuras críticas.
- Acceso limitado para los agentes capaces de prevenir o reducir las consecuencias de los ataques.

Las posibles consecuencias de ataques a la infraestructura crítica incluyen:

- El bloqueo del transporte, la electricidad y el abastecimiento de agua, comunicaciones, transmisión de datos, plantas de energía nuclear, control de tráfico aéreo.
- La quiebra de estructuras comerciales y los sistemas financieros, el fracaso de las transacciones comerciales internacionales, la desestabilización de los mercados e instituciones financieras, el robo de dinero e información.
- La pérdida de propiedad intelectual o de reputación (debido, por ejemplo, al ataque con un gusano, la empresa de pagos en línea PayPal se enfrentó a una bancarrota en el año 2002).
- Víctimas humanas o pérdidas materiales, provocado por el uso destructivo de los elementos de la infraestructura crítica (cibersabotaje en la industria alimenticia, el tráfico aéreo o ferroviario).
- El acceso no autorizado y/o modificación de información personal.
- La posibilidad de imputar actos terroristas a otro país/gobierno y el agravamiento de la tensión en las relaciones internacionales.

Mientras la restauración de la ICI podría ser una tarea rápida y fácil, los efectos indirectos de incluso los daños más pequeños pueden sentirse durante un tiempo. Los ataques a ICI pueden socavar gravemente la confianza pública y empresarial en el comercio electrónico, iniciativas gubernamentales y otros. Los costos humanos y económicos asociados con la recuperación o estrategias de mitigación son enormes.

Los ataques relacionados con la infraestructura crítica de la Información (ICI) están básicamente conectados a la presencia de puntos débiles en su arquitectura, en sus protocolos de comunicación (por ejemplo, deficiencias en los protocolos de los sistemas SCADA, en los protocolos de los sistemas financieros y de los sistemas de votación), ataques del tipo DoS (para la implantación de botnets, o algunos gusanos), intrusiones de personas ajenas y de personal de planta (outsider/insiders) para un buen o mal impacto social (por ejemplo, el phishing y los fraudes en las redes sociales como Facebook, Twitter, Skype y la influencia social en sitios web como WiliLeaks). Sin embargo, el estudio de los ciberataques contra las ICI podría beneficiarse con el modelamiento de diferentes conceptos, software de entornos y escenarios que permitan la exploración tanto del comportamiento estático y dinámico.

No existen muchas publicaciones científicas directamente relacionadas con los ataques a la infraestructura crítica, solo están a disposición del público a partir de los últimos cinco años. La razón principal es la confidencialidad como uno de los principios fundamentales para el levantamiento de la protección de infraestructuras críticas según se describe en el "Programa Europeo de Protección de Infraestructuras Críticas". Según este principio, el acceso a la información sobre seguridad IC solo debe concederse con arreglo a la necesidad de conocimientos y el intercambio de información relacionada debe clasificarse y ser realizado en un ambiente de confianza y seguridad.

Otra razón relativa a la falta de información acerca de aspectos de seguridad de las IC es que la mayoría de los operadores mantienen un monopolio en su mercado. Esto contribuye a una tendencia de reducir su comunicación con el mundo exterior, especialmente cuando se trata de información confidencial.

Ataques a la privacidad y a redes sociales

Cientos de millones de usuarios están registrados en los sitios de redes sociales y hacen uso regularmente de sus servicios para permanecer en contacto con sus amigos, comunicarse, hacer comercio online y compartir contenidos multimedia con otros usuarios. Lamentablemente, los sitios de redes sociales también son un destino muy atractivo para los atacantes debido a la naturaleza confidencial de la información que contienen sobre los usuarios registrados. Normalmente, los usuarios deben introducir sus direcciones de correo electrónico reales y proporcionar información sobre su educación, sus amigos, sus antecedentes profesionales, actividades en que participan, su actual estado civil y sus preferencias sexuales. Por lo tanto, desde el punto de vista del atacante, el acceso a este tipo de información personal, sería ideal para el lanzamiento de ataques dirigidos de ingeniería social, a menudo conocidos como "spear phishing".

Además, la recopilación de direcciones de correo electrónico e información personal sería invaluable para los spammers ya que podrían tener acceso a las direcciones de correo electrónico que pertenecen a personas reales, es decir, un problema que los spammers enfrentan es que a menudo no saben si las direcciones de correo electrónico que

recogen están siendo utilizadas por personas reales o simplemente son direcciones secundarias que no se leen regularmente y tener información acerca de las personas que utilizan estas direcciones de correo electrónico, lo que les permitiría personalizar eficazmente sus actividades de marketing, adaptándolas según el conocimiento del perfil del blanco u objetivo.

El ataque mejor conocido que compromete la relación de confianza en una red social que emplea un sistema de reputación es el ataque "sybil". En este ataque, el atacante crea múltiples identidades falsas y las usa para obtener una gran influencia desproporcionada sobre el sistema de reputación. El ataque se basa en la suposición de que es relativamente fácil crear perfiles falsos en la mayoría de las redes sociales existentes. Para defenderse contra los ataques sybil, se han propuesto muchos enfoques. En particular SybilGuard y SybilLimit se basan en el hecho de que las redes sociales del mundo real se mezclan rápidamente y esta percepción es usada para distinguir los nodos sibil de los nodos normales. Que se mezclen rápidamente significa que los subconjuntos de nodos honestos tienen buena conectividad con el resto de la red social, mientras que es muy difícil lograr el mismo nivel de conectividad con los nodos falsos. Si esta suposición es cierta, tanto SybilGuard como SybilLimit son buenas soluciones para detectar nodos Sybil. Sin embargo, los atacantes pueden obtener conexiones legítimas de amistad y por lo tanto, no son detectados por los actuales métodos de detección.

El requisito principal para poder acceder a la información personal de un usuario en un sitio de redes sociales es haber confirmado una relación personal con el blanco. Por ejemplo, la configuración predeterminada en Facebook es permitir a los amigos confirmados tener acceso a la información personal (dirección de correo electrónico, fotografías, etc.), pero no para que sea proporcionada a terceros sin haber sido autorizados. Análogamente, en LinkedIn, los contactos de una persona solo se pueden acceder si se confirma el contacto profesional y, por lo tanto, él/ella ya ha aceptado una solicitud y confirmó la relación. Además, los nodos falsos necesitan conectarse a usuarios reales con el fin de presentar un aspecto más realista y evitar las técnicas de detección basadas en la "propiedad" de mezclado rápido.

Los ataques de ingeniería social

Los ataques de ingeniería social son bien conocidos en la práctica como en la literatura. Los objetivos de la ingeniería social son las debilidades humanas en lugar de las vulnerabilidades técnicas de los sistemas. La ingeniería social automatizada es el proceso de ejecutar automáticamente los ataques de ingeniería social. Por ejemplo, el spam y el phishing pueden ser vistos como una forma muy simple de ingeniería social, es decir, para lograr que los usuarios hagan clic en los enlaces.

Un problema general en las redes sociales es que a los usuarios les resulta difícil juzgar si una solicitud de amistad es de confianza o no. Así, pues, los usuarios a menudo aceptan rápidamente invitaciones de personas que no conocen. Por ejemplo, un experimento realizado por Sophos [13], mostró que el 41% de los usuarios de Facebook admitió una solicitud de amigo de una persona al azar. Incluso, los usuarios más cautelosos pueden ser engañados por las peticiones de adversarios que suplantan a sus amigos.

Lamentablemente, una vez que se ha establecido la conexión, el atacante normalmente tiene acceso completo a toda la información sobre el perfil de la víctima. Además, los usuarios que reciben mensajes de supuestos amigos son mucho más propensos a actuar sobre la base de esos mensajes, por ejemplo, haciendo clic en vínculos. Un resultado similar se obtiene con los intentos de phishing que tienen más probabilidades de éxito si el atacante utiliza información robada a los amigos de las víctimas en las redes sociales para crear sus correos electrónicos de phishing.

A diferencia de la ingeniería social activa, que requiere que el atacante establezca contacto con la víctima, en un ataque de ingeniería social inversa, es la víctima la que hace contacto con el atacante.

Los ataques de ingeniería social inversa son una amenaza posible en la vida real, y los atacantes pueden ser capaces de atraer a un gran número de usuarios legítimos sin enviar ninguna solicitud activa de amistad. Algunos experimentos demuestran cómo las sugerencias y cualidades amistosas posteadas por sitios de redes sociales pueden ofrecer un incentivo para las víctimas para contactar a un usuario si

fue creado con la configuración correcta (por ejemplo, una fotografía atractiva, intereses profesionales similares, hobbies en común, y otros).

Así podemos asegurar que existe una serie de graves ataques contra la privacidad del usuario en los sitios web de redes sociales. A veces, las contramedidas están disponibles y en otras simplemente no existen. Una forma de proteger la privacidad del usuario contra aplicaciones malintencionadas y contra las vulnerabilidades del servicio, consiste en aplicar técnicas criptográficas en sus capas de comunicaciones más altas.

Ataques web

Por definición, los ataques web incorporan un amplio espectro de temas relacionados con la seguridad, en esta sección revisaremos los siguientes tópicos:

- Drive-by-downloads: fuertemente relacionados con malwares y sus canales de distribución, drive-by downloads es todavía una importante técnica de distribución para infectar sistemas informáticos con malware. La vulnerabilidad explotada es siempre dirigida contra el navegador web y entregado por páginas web arbitrarias con cargas falsas. Por lo tanto, es la forma más común de ataques web.

- La explotación directa de páginas web y su infraestructura es todavía posible por diversos medios. La inyección SQL (SQLI), cross-site scripting (XSS) y los Cross-site request forgery (CSRF) son ejemplos de técnicas de ataques dirigidos. Aunque estos temas han recibido bastante atención de los investigadores en los últimos diez años, los problemas subyacentes no están todavía totalmente resueltos.

- El Web Spam no es dirigido contra un sitio web específico ni contra los propios clientes. En su lugar, el atacante intenta influir en los resultados devueltos por los motores de búsqueda, inyectar mensajes a foros o utilizar otros medios de distribuir anuncios en recursos web. Aunque no es un ataque directo por si mismo, el web spam es muy molesto y tiene un impacto negativo tanto en la experiencia de navegación del usuario, como en el proveedor del recurso en sí.

Los ataques por Drive-by-downloads aprovechan las vulnerabilidades de los navegadores web y los componentes del explorador web. Estos ataques se desencadenan cuando una víctima utiliza su navegador para cargar una página web que contiene código malicioso. Para atraer a las víctimas potenciales, los atacantes pueden preparar páginas web malintencionadas y distribuir sus URLs (por ejemplo, mediante la inclusión de enlaces en los correos spam). Alternativamente, los atacantes pueden comprometer sitios web existentes e inyectar código malicioso en los resultados del motor de búsqueda o en páginas legítimas. Normalmente, el código de explotación utilizado en un ataque por drive-by-download está escrito en el lenguaje scripts del lado del cliente, tal como JavaScript o ActionScript (como parte de un archivo Flash Adobe). Este código es directamente ejecutado por el navegador o ejecutado con la ayuda de una extensión del navegador. Cuando el ataque tiene éxito, el malware se descarga y se instala en la máquina víctima, frecuentemente en un esfuerzo para reclutar nuevos miembros para una botnet. En los últimos años, los ataques drive-by-download se han convertido en el medio más popular usado por los ciberdelincuentes para atacar e infectar hosts. La razón de la popularidad de este tipo de ataque es que los ataques directos contra hosts y sus sistemas operativos se han vuelto más difíciles. Esto es debido en parte a los crecientes esfuerzos de Microsoft para mejorar la seguridad de sus productos Windows y también debido al hecho de que los usuarios cada vez están más protegidos por firewalls y dispositivos como los routers domésticos. Dada la importancia de los ataques drive-by-download, los investigadores han propuesto recientemente los primeros pasos para proteger los navegadores contra estos ataques.

Google Chrome es por lejos el navegador con la versión más actualizada de clientes, seguido de Firefox. internet Explorer por otra parte, sigue siendo un blanco popular para los ataques dirigidos contra ese explorador o sus plugins. Además, no todos los ataques se dirigen a una vulnerabilidad específica de un navegador. En muchos casos, el exploit está dirigido a un plug-in como el flash player o el lector de PDF. En resumen, los ataques drive-by-download afectan un gran número de usuarios de internet y un alarmante porcentaje de estos usuarios confían en sistemas vulnerables, tales como en versiones antiguas de un navegador o en componentes adicionales vulnerables. Del mismo modo, en el lado del servidor, los administradores

de sitios web de sitios infectados son lentos en la eliminación de código malicioso inyectado en sus páginas y a menudo, cuando lo hacen, son más proclives a ser infectados nuevamente.

Ataques directos

Mientras los ataques drive-by-downloads son dirigidos a una enorme cantidad de computadores para infectarlos con software malintencionado, existen varios escenarios de ataque, donde el entorno del servidor web es elegido específicamente como un blanco.

Cross-site request forgery (CSRF)

Cross-site request forgery (CSRF) es un vector de ataque por aplicación web con el que un atacante fuerza el navegador de un usuario involuntario para realizar acciones en el sitio web de un tercero, posiblemente reutilizando todas las credenciales de autenticación en caché del usuario. En el año 2007, CSRF fue catalogado como una de las más graves vulnerabilidades de las aplicaciones web en el OWASP (Open Web Application Security Project).

Cross-site scripting (XSS)

Estrechamente relacionado a CSRF, los ataques cross-site scripting (XSS) son considerados entre las amenazas de seguridad número uno en internet hoy en día. Estos ataques violan la confidencialidad de los datos sensibles, socavan los sistemas de autorización, estafan a los usuarios, difaman sitios web y mucho más. El sitio web www.xssed.com documenta los ataques de XSS más recientes en los principales sitios de redes sociales y blogs. En particular, Facebook, MySpace de LiveJournal y Orkut han sido afectados por estos ataques. Los ataques de XSS pueden ser autopropagados, y tienen el potencial para rápidamente afectar a millones de personas. En términos generales, XSS es una inyección de código script no autorizado en una página web. Como una aplicación web procesa los datos de usuarios no confiables, genera algunos outputs de contenido web de baja integridad llamamos HTML no confiable. El objetivo de un ataque XSS es insertar código script malicioso en HTML que no es de confianza, causando que el script se ejecute en el navegador web de una víctima. Las estrategias de defensas para XSS apuntan a impedir la ejecución de

secuencias de comandos no autorizados mediante la aplicación de una política de no-script en el HTML que no es de confianza.

Inyección SQL

La inyección de SQL es una técnica de inyección de código que se aprovecha de una vulnerabilidad de seguridad que ocurre en la capa de base de datos de aplicaciones web. La vulnerabilidad se produce cuando la entrada del usuario se filtra incorrectamente resultando en una cadena literal de caracteres integrados en sentencias SQL o la entrada del usuario no es correcta y/o fuertemente tipeada (escrita) y por tal razón es inesperadamente ejecutada. Se trata de una clase más general de vulnerabilidades que puede ocurrir cuando un lenguaje de programación o secuencias de comandos está incrustado dentro de otro. Curiosamente, esta forma de ataque se ha conocido por más de 10 años y se han ideado defensas para proteger a las empresas y organizaciones de los ataques a sus bases de datos. Aun así, las inyecciones SQL se siguen viendo en varias páginas web. El más famoso incidente ocurrió en marzo del año 2011, cuando Mysql.com fue comprometido por un ataque oculto de inyección SQL. Estos incidentes demuestran que incluso los más expertos son propensos a las vulnerabilidades, aunque ya existe una solución de mitigación. Al final, siempre habrá programadores bajo limitaciones de tiempo que decidirán implementar soluciones rápidas sin importarles las consecuencias de seguridad.

El spam web

Una molestia muy común a la cual hacer frente es la publicidad o los anuncios publicitarios en la web. El término web spam hace referencia a páginas de hipervínculos en la World Wide Web que se crearon con la intención de engañar a los motores de búsqueda. Por ejemplo, un sitio de pornografía puede controlar el sitio web agregando miles de palabras clave para su página de inicio, a menudo haciendo el texto invisible a los seres humanos a través del uso de combinaciones de colores ingeniosas. Un motor de búsqueda indexará las palabras claves adicionales y devolverá la página pornográfica como una respuesta a las consultas que contienen alguna de las palabras clave. Como las palabras clave agregadas normalmente no son de naturaleza estrictamente para adultos, personas que estén buscando otros

temas serán dirigidas a la página. Otra técnica de spam web es la creación de un gran número de páginas web falsas, todas apuntando a una sola página objetivo.

Los ataques web, en un sentido más amplio, todavía son de gran ocurrencia. Con la enorme cantidad de personas navegando en la web, donde la mayoría solo tienen una escasa sensibilización en materias de seguridad, una multitud de vectores de ataque resultan viables. Mientras los ataques a la infraestructura de servidores intentan explotar vulnerabilidades muy específicas, los ataques del lado del cliente ahora son predominantes. La razón es simple, la mayoría de los usuarios tienden a esperar la aplicación de parches de seguridad para sus sistemas, lo que a su vez puede ser explotado fácilmente. Aumentar la conciencia sobre la seguridad, por otro lado, siempre ha sido considerada como una gran tarea que no puede hacerse de la noche a la mañana. Por lo tanto, esta forma de ataques también se verá en el futuro, dejando a los investigadores con la tarea de diseñar las contramedidas y técnicas de mitigación adecuadas.

Ataques a nivel de red

En esta sección se verán dos clases principales de ataques a nivel de red. Es decir, ataques en el Border Gateway Protocol (BGP) y en el Sistema de Nombres de Dominio (DNS). Nos centramos en estos protocolos, ya que forman la columna vertebral de la internet de hoy en día, y cualquier compromiso sobre su integridad o funcionamiento puede dar lugar a importantes problemas de seguridad.

Descripción del BGP

Internet es un sistema mundial de redes de computadores interconectados. Las redes están compuestas de sistemas terminales, llamados hosts y routers, cada uno con una o más direcciones ip. En internet para estar conectado debe haber una forma para que los paquetes de un host puedan llegar a cualquier otro, incluso si no están en la misma red. Esto requiere que los datos fluyan de una red a otra hasta que lleguen a su destino final. Los protocolos de enrutamiento son utilizados por los routers para descubrir rutas hacia cada destino. En internet, redes y por lo tanto routers, pertenecen a diferentes organizaciones heterogéneas como universidades, empresas privadas, organismos guber-

namentales, etc. Estas entidades son reacias a compartir información acerca de la estructura de sus redes. Por otra parte, desean ser capaces de administrar y organizar libremente su red según sus necesidades y no se basan en una norma común. Esto hace que la conectividad entre ellos sea una tarea difícil ya que cada entidad intenta equilibrar entre conectividad y accesibilidad, mientras que al mismo tiempo proporciona la menor cantidad de información que sea posible.

Internet se compone de Sistemas Autónomos (SA), un sistema autónomo es una unidad organizacional que controla una serie de redes y ha definido claramente su política de enrutamiento. Cada SA puede controlar muchas redes, pero cada red está controlada por exactamente un SA. Además, cada SA es responsable de la entrega de paquetes a su host y del envío de paquetes que son recibidos en uno de sus routers fronterizos para el router apropiado para que continúen hacia el siguiente SA. El SA puede elegir libremente su estructura interna y no necesita publicar ninguna información al respecto. La única información que necesita publicar son sus routers de borde o frontera. Un router de frontera es un enrutador que conecta un SA con otro. Para que dos SA se comuniquen deben configurar sus routers de frontera teniendo ambos como vecinos. Un SA puede tener muchos routers de frontera, cada uno con distintos vecinos. Esto es posible porque la red puede extenderse a lo largo de una gran área geográfica y, por lo tanto, conectarse con diferentes SA en diferentes áreas. La asignación de direcciones ip está directamente conectada con la noción de SA y por consiguiente al enrutamiento.

La Autoridad de Asignación de Números de internet (IANA, por sus siglas en inglés) a través de sus registros locales (ARIN, RIPE, etc.) asigna a cada SA un número único (SAN) desde 1 hasta 64511. También a través del mismo proceso IANA asigna a cada SA los bloques de direcciones ip, llamadas prefijos de ip. Estas direcciones ip son contiguas y están representadas por la primera dirección y la longitud de la máscara. La delegación de bloques de direcciones es jerárquica, así un SA puede a su vez delegar una parte o la totalidad de su prefijo a otro SA sin notificar a IANA. En la práctica, IANA delega los grandes prefijos ip a los registros locales que luego los delega a los registros nacionales, que, finalmente asigna prefijos a los SA. La delegación de prefijos puede tener más niveles en cascada. Por ejemplo, un SA puede delegar parte de su prefijo a otro SA.

El Border Gateway Protocol (BGP) está diseñado para ayudar a los SA, decide la mejor ruta a un destino ip determinado. El protocolo funciona de la siguiente manera: los routers de borde de un SA anuncian a sus vecinos que tiene una ruta para algún prefijo ip. El que introduce un prefijo en el sistema de enrutamiento global se denomina SA originador de este prefijo. El aviso le permite a los SA vecinos del SA originador saber que el tráfico destinado a ese prefijo ip debe ser remitido a este último, que sabe cómo manejarlo. Además, los SA vecinos reenvían el anuncio a sus propios vecinos, añadiendo la información de la ruta para que el prefijo ip pase a través de ellos para llegar al SA originador. Así, los vecinos de los vecinos también tienen una ruta para el prefijo ip en particular. Los SA siguen propagando el anuncio, agregándose ellos mismos a la ruta, hasta que todos los SA tienen una ruta para ese prefijo.

Cuando un atacante agrede los sistemas de enrutamiento global apunta en uno de los siguientes caminos:

- Hacer un destino inalcanzable para una parte o la totalidad de internet. Normalmente, un router BGP malicioso hace falsos anuncios para atraer el tráfico destinado a un prefijo y luego simplemente se deshace de los paquetes que recibe. Como resultado el prefijo anunciado no está disponible ya que los paquetes no pueden llegar a su destino. La magnitud del ataque depende de en qué medida los anuncios maliciosos se propagan. Este efecto se denomina Blackholing.

- Redirigir el tráfico para escuchar o atacar. El atacante intenta alterar el camino legítimo con otro camino que sustenta sus propósitos malintencionados. El camino falso puede pasar a través de un router controlado por el atacante. En este caso, el atacante puede realizar un ataque de hombre en el medio. O el atacante puede cambiar el destino del camino a un blanco en un host malicioso. El host malicioso puede suplantar al legítimo para extraer información confidencial. Además, el atacante puede incluir en la ruta un router benigno para saturarlo con tráfico adicional, esencialmente para realizar un ataque de denegación de servicio DoS.

Descripción de un DNS

El Sistema de Nombres de Dominio (DNS) es uno de los componentes críticos de internet. Su función principal es traducir nombres de dominio en lenguaje humano a direcciones ip en formato legible a las máquinas. Aunque no es esencial para la funcionalidad de internet se considera crítico ya que muchas aplicaciones como el correo electrónico, la web y servicios de mensajería instantánea no pueden funcionar sin él.

El DNS consta de tres componentes. En primer lugar, el espacio de nombres de dominio y los recursos de registros que crean una estructura de árbol con los nombres y datos asociados. Segundo, los servidores de nombres que almacenan el espacio de nombres de dominio denominados árbol de una forma distribuida, cada servidor de nombres contiene solo una parte del árbol y apunta a otros servidores de nombres. El servidor de nombres que mantiene la raíz del árbol de espacio nombres se denomina el servidor raíz de nombres. El servidor raíz de nombres contiene información sobre el servidor de nombres del siguiente nivel que son los servidores de dominio de nivel superior. Estos son los servidores autorizados para servir a los dominios de nivel superior como .com, .edu, .org, .uk, .es, .gr, etc. Más abajo en el árbol están los servidores de nombre de organización o empresa. Por último, los solucionadores son programas cuya función es extraer información de la infraestructura DNS. El solucionador recibe consultas de seres humanos o de otros programas (clientes de correo, navegadores web) por nombres de dominio que ellos desean traducir y se comunica con el servidor de nombres para obtener la respuesta. Cada solucionador debe tener acceso al menos a un servidor de nombres y pasearse entre ellos para encontrar la respuesta a una consulta.

El proceso de traducir un nombre de dominio a una dirección ip se denomina resolución. Como el espacio de dominio es jerárquico y descentralizado, el proceso de resolución implica la consulta a un servidor de nombres cerca de la parte superior del árbol y a continuación, consulta otros servidores de nombres mientras se recorre el árbol hacia el servidor de nombres con la información necesaria.

Ataques DNS

Un ataque de denegación de servicio (DoS) es un intento de negar el recurso de un computador y que no esté disponible para los usuarios legítimos. El DNS puede ser el destino, sino también la herramienta para tales ataques. Un ataque que busque dejar el sistema de nombres no disponible estaría dirigido a los servidores de nombres. Un tipo de ataque se centraría en colapsar los servidores. Paquetes especialmente diseñados pueden aprovechar las vulnerabilidades del software, como el desbordamiento de buffer (buffer overflow), que puede provocar el bloqueo del servidor. No es necesario que el atacante centre su ataque en el software DNS, todos los servicios que se ejecutan en el mismo host que el servidor DNS, incluso el propio sistema operativo puede ser el objetivo del ataque. Otro tipo de ataque de denegación de servicio en los servidores de nombre apunta a consumir todos los recursos disponibles del servidor, haciendo que las respuestas del servidor sean más lentas o incluso no responda a solicitudes legítimas.

El DNS también puede utilizarse para realizar un tipo de DoS denominado amplificación de ataque a otros hosts. Un atacante puede aprovechar la enorme diferencia de tamaños entre una solicitud de transferencia de zona y la respuesta. Asumiendo que el servidor DNS acepta solicitudes de transferencias de zona de todo el mundo, un atacante puede enviar dicha solicitud a través de la dirección de origen del blanco. El servidor de nombres DNS responderá a la solicitud inundando el insospechado destino con datos. Si el destino es una red en lugar de un único host, entonces el atacante puede solicitar una transferencia de zona spoofing (suplantando) varias ips de la red víctima.

Ataque del tipo hombre en el medio

Las consultas de DNS son usualmente transmitidas mediante el protocolo UDP para baja sobrecarga. La mayoría de las veces, la consulta y la respuesta caben en un único datagrama que viaja a través de la red sin firma y sin encriptar. Dado que el protocolo DNS no autentica el origen de las solicitudes, un atacante puede interceptar una consulta que viaja desde el solucionador hacia el servidor de nombres DNS y responder con una traducción maliciosa antes que el verdadero servidor de nombre. Las probabilidades generalmente favorecen a los atacantes porque ellos residen con frecuencia en la misma LAN que

la víctima, mientras que el servidor DNS normalmente no. Además, el servidor DNS que recibe la consulta puede tener que buscarla de forma recursiva lo que aumentaría aún más el tiempo de respuesta. El solucionador que solicita la traducción aceptará como válida cualquier respuesta que reciba por dos razones. En primer lugar, no puede verificar que el que responde es quien dice que es y segundo que no puede verificar que el que responde es delegado para controlar esa parte del espacio del dominio. Este tipo de ataque, llamado hombre en el medio, puede utilizarse para redirigir un usuario benigno a sitios diferentes de lo que solicitó para phishing y otras actividades maliciosas.

Ingeniería social

El usuario malintencionado puede intentar explotar las características de los usuarios y las relaciones entre ellos para controlar el sistema de nombres. Estos ataques no van dirigidos contra el protocolo, pero pueden causar una gran frustración y pérdidas económicas a la víctima. El secuestro de dominios es la transferencia de la propiedad de un nombre de dominio desde el legítimo propietario a uno malicioso. El atacante intenta convencer al registrador de dominios para modificar la información de registro del nombre de dominio o transferirlo a otro registrador. Para ello, el atacante utiliza todo tipo de técnicas de ingeniería social para suplantar al propietario del dominio. Si el ataque tiene éxito, el atacante normalmente inicia una transferencia a otro registrador en un país diferente para hacer que la devolución al propietario legítimo sea aún más difícil. Este tipo de ataque puede tener enormes repercusiones financieras para el propietario, ya que los ingresos generados por el sitio en su dominio son dirigidos hacia el atacante.

Ataques al cloud computing

El concepto emergente de la computación en nube es un fenómeno extendido y desconcertante. El cloud computing permite a las organizaciones ejecutar aplicaciones (a menudo denominadas servicios) sobre una base de pago por uso, muy confiable, altamente disponible, con infraestructura de hardware y software escalable, conocidos como nubes. En cierto sentido, una nube puede ser vista como un gran y moderno mainframe con recursos prácticamente infinitos y el término cloud computing se refiere a la utilización de estos recursos para ofrecer servicios web.

La seguridad en cloud computing cuenta con una definición vaga. Las iniciativas comunitarias y organizaciones como la Cloud Security Alliance persiguen el objetivo común de reunir conocimientos y unir esfuerzos para idear medidas de seguridad apropiadas para el cloud computing. El rápido crecimiento de la Cloud Security Alliance sugiere que la comunidad está realmente preocupada por la seguridad. Aunque el concepto de cloud computing sin duda plantea nuevos desafíos, sin embargo, puede ser difícil distinguir entre cuestiones específicamente causada por los sistemas informáticos, y cuestiones que, por casualidad, se producen en un sistema implementado en una nube.

Los proveedores de servicios en la nube intentan vender "cloud security" simplemente como otro ejemplo del problema de la seguridad en la virtualización, ofreciendo seguridad como servicio de soluciones de monitorización.

En realidad, los desafíos de seguridad en la nube van más allá de los retos de los entornos virtualizados en al menos tres formas. La medida más obvia y efectiva en general para proteger la confidencialidad de los datos es el cifrado o encriptado. Sin embargo, el cifrado no siempre es una solución viable, especialmente para aplicaciones con uso intensivo de datos que requieren un alto rendimiento de entradas y salidas. El cifrado no es sencillo cuando los datos se distribuyen. Como la mayoría de los usuarios se abstiene de cifrar el disco duro de sus laptops por sobrecarga técnica y computacional, también puede molestar a los usuarios cifrar sus unidades virtuales de almacenamiento remoto. Además, si un almacenamiento remoto es cifrado de forma transparente (es decir por el proveedor), ¿a quién le pertenecen los datos?, ¿al usuario, al proveedor? y, ¿este hecho es demostrable? ¿Cómo?

Los problemas de seguridad típicos de entornos de hospedaje compartido se acentúan en el caso de las nubes, porque la complejidad adicional, no-percibida debido a la asignación dinámica de recursos, la replicación y la optimización, ofrecen a cada usuario la idea de ser únicos.

La ola de delincuencia que vemos en la web hoy en día es bastante diferente de la de los ataques de red más tradicionales. Nuestros adversarios cambiaron de táctica alejándose del ruido del escaneo

hacia ataques más furtivos, porque sus motivaciones cambiaron. Los ciberatacantes modernos buscan incentivos económicos, en contraposición a las exposiciones de la superioridad técnica. El rápido crecimiento de la economía subterránea ya ha abrazado el modelo de cloud. De hecho, puede aducirse que las botnets son un estado embrionario de una infraestructura maliciosa distribuida tipo cloud. Algunos investigadores incluso cuantifican la amenaza de navegadores que son controlados por sitios web malintencionados que les ordenan que ataquen de forma remota a terceros (por ejemplo, ataques de denegación de servicio, la propagación de gusanos y escaneos de reconocimiento), creando un potente ataque tipo cloud a la infraestructura del cliente.

No se debe perder de vista que finalmente lo que se pretende proteger es información. Y la información propiamente tal se enfrenta a amenazas de distinto tipo, pudiendo ser mayor o menormente afectada según la naturaleza de la amenaza que pueda enfrentar. Las amenazas a la información se pueden clasificar en tres tipos distintos, siendo estos primeramente la amenaza representada por la naturaleza. Efectivamente la primera amenaza es el factor natural reflejado por los desastres naturales que pueden ocasionar grandes pérdidas de información por medio de inundaciones, incendios, terremotos y tormentas eléctricas. Un segundo tipo de amenaza son de origen técnico muy vinculado a la obsolescencia del hardware, los softwares y las mismas redes, debido a que en la medida que la información esté contenida físicamente en dispositivos que tienen su vida útil cumplida, el riesgo de que por fallas o por capacidad, la información no pueda ser recuperada es alto. El tercer tipo de amenaza y el más sensible es el propio ser humano que puede generar las peores consecuencias en contra de la información. Dentro de la clasificación de amenazas humanas se encuentran las no maliciosas, que se refieren a personal operador de sistemas de información que debido a su ignorancia o falta de capacitación, por errores involuntarios causan la pérdida de información o daños a esta debido a su desconocimiento de la operación de esos sistemas. Paralelamente, la amenaza humana mal intencionada es de mayor riesgo que la anterior debido principalmente a la intención que es definidamente ofensiva con intensión de causar daños a la información contenida en un sistema informático. Este tipo de amenaza puede clasificarse como externa cuando se refiere a la acción de ciberespionaje, hackers, y la explotación de vul-

nerabilidades de una red y otros. Pero la amenaza más dañina es la amenaza humana, mal intencionada (maliciosa) que es causada por personal desafecto de la misma organización que pueda generar desde un sabotaje hasta robar la información clasificada de un sistema. Lo mismo con el personal corrupto que puede generar tanto o más daño a la información. Esta clasificación puede verse representada en la siguiente figura.

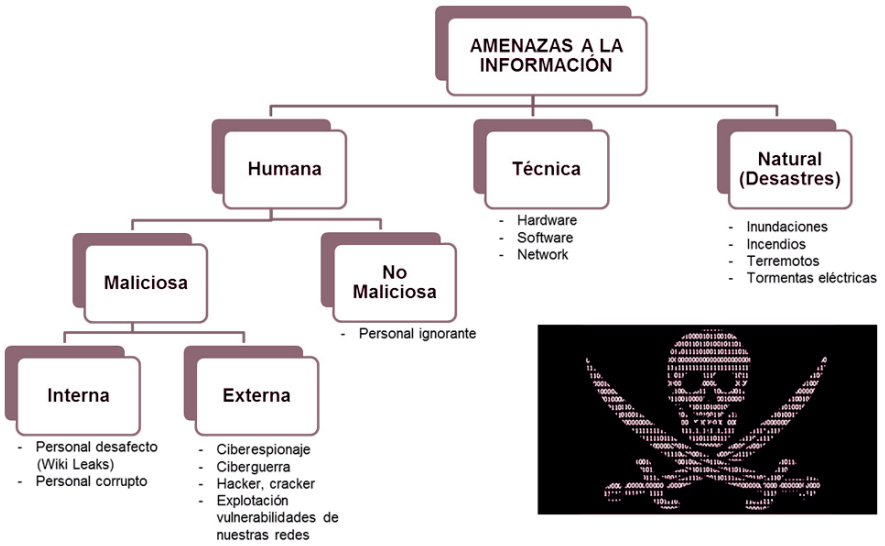

Figura 2.7: Amenazas a la Información. Fuente: Elaboración propia.

Capítulo III
De Ciberseguridad a Ciberguerra

La revolución tecnológica más significante en la guerra y en la vida actual, está en el rol de la información y el conocimiento, y en particular en el grado de la alerta situacional que se le presenta a los comandantes, gracias al incrementado número de sistemas de comunicaciones e información que apoyan a las fuerzas de combate. Sin embargo, no todos los ejércitos están capacitados para tomar ventaja de esta revolución y en la "era de la información" actual, los ejércitos deben estar preparados para enfrentar un amplio espectro de amenazas inherentes a esta era.

La era de la información con la asociación de las tecnologías de la información, favorece a las redes más que a las jerarquías; difunde y redistribuye el poder; cruza y redibuja fronteras físicas y responsabilidades y expande horizontes. Esto es particularmente verdadero en el ambiente civil, donde las organizaciones han llegado a ser más democráticas en la distribución de la información y han logrado una mejor eficiencia.

Para la guerra, la mayor lección del mundo comercial es que el conflicto de la era de la información es acerca del conocimiento y la habilidad de las redes y de las organizaciones en red, para proveer una mayor ventaja o la superioridad definitiva en el conflicto. Sin embargo, los comandantes militares tienden a ver el mando y la información (incluso las comunicaciones en muchos ejércitos), según las mismas líneas jerárquicas o de mando. En un modelo en red no jerárquico, el flujo de mando y de información debe ser necesariamente divergente. Los sensores, los comandantes y los sistemas de armas están conectados por una grilla en red que asegura que la data de alerta situacional puede ser compartida por todos los elementos, sin importar si pertenecen a la misma unidad. Las líneas de mando no necesitan ser compartidas con los flujos de información. La información se comparte a través de la red; el mando y el control son dirigidos de acuerdo con el orden de batalla preestablecido. Por

lo tanto, la adopción de estas tecnologías no afecta solamente la manera en que los ejércitos son dirigidos y controlados, sino que también deben cambiar la forma en que estos son organizados, entrenados y dirigidos.

En la última década el ciberespacio ha surgido como una nueva dimensión en la que pueden materializarse a su vez nuevas amenazas. Esto ha modificado el escenario tradicional de la defensa, que consideraba solo las dimensiones de tierra, mar, aire y el espacio, al incluir al ciberespacio como una dimensión adicional más intangible que las anteriores.

Diversas naciones han hecho pública su intención de crear organismos especiales de defensa para desarrollar y desplegar todo un arsenal de nuevas ciberarmas. Así el presidente de Estados Unidos, Barack Obama, el día 11 de julio de 2012 estableció a través de un decreto, medidas para cautelar el uso de internet durante emergencias de seguridad o desastres naturales. Bajo el nombre de Asignaciones de Seguridad Nacional y Preparación de Funciones de Comunicaciones en Emergencia (Assignment of National Security and Emergency Preparedness Communications Functions), dándole más poder al Estado y a sus agencias de control sobre las telecomunicaciones y la web durante estados de emergencia.

Este decreto se basa en que el gobierno federal debe tener la capacidad de comunicarse en todo momento, inclusive cuando las circunstancias no son del todo favorables. La intención es poder hacerlo cuando las situaciones son críticas. Tener una comunicación efectiva, confiable y disponible a todo evento, a escala local e internacional, es esencial para que el ejecutivo pueda comunicarse con los otros dos poderes, los gobernadores de los Estados, el sector privado y sus aliados en otros países. A juicio del gobierno de Estados Unidos, poder hacerlo es afianzar la seguridad nacional porque facilita la capacidad del Estado para comunicarse en emergencias.

Atendiendo la naturaleza de las amenazas que caracterizan al ciberespacio, es que muchos expertos consideran que las capacidades en el ámbito de la ciberguerra, que se desarrollen en el futuro por parte de algunos Estados y/o grupos de interés, atendiendo la sofisticación alcanzada por las ciberarmas y el nivel de desarrollo de las operaciones de ciberguerra, constituirán una amenaza concreta para la seguridad de los Estados y de las personas, tal como lo dejan en evidencia los malwares y operaciones identificadas en algunos conflictos modernos.

La superioridad de la información puede entonces ser definida como aquel grado de supremacía en el dominio de la información que permite la conducción de las operaciones sin una oposición efectiva. De este modo, la superioridad de la información se convierte en conocimiento superior que, combinado con una doctrina organizacional, entrenamiento, experiencia y un apropiado mecanismo y herramientas de mando y control, alcanza la superioridad en la toma de decisiones.

Tal vez el impacto mayor de las tecnologías de la información se encuentra en el concepto emergente de guerra centrada en redes (Network-Centric Warfare, NCW). En la guerra centrada en redes, los sistemas de armas y los sensores están conectados por redes desplegadas a través de las cuales las armas pueden enfrentar blancos basándose en la alerta situacional que es compartida con otras plataformas. De tal forma se puede aplicar una capacidad de combate con menos sistemas de armas que con los que son normalmente requeridos. El hecho de que los sistemas de armas estén interconectados, no significa que los blancos puedan ser enfrentados aleatoriamente o sin una autorización; el control todavía es esencial para asegurar que los blancos sean atacados de acuerdo con el plan operacional.

Aunque puede continuar existiendo algún rol para los enlaces directos desde los sensores hacia los sistemas de armas, el objetivo final de la NCW es que el empleo de las armas de precisión se basa en información. Ningún sensor por si solo tiene la capacidad de dirigir las aplicaciones de las armas de precisión, la data debe ser integrada desde un número de sensores y bases de datos, de tal forma que, en el campo de batalla moderno, las redes se transforman en un multiplicador de fuerza considerable. Bajo esta condición, los comandantes se encuentran desencadenados gracias a las comunicaciones y no se ven forzados a permanecer en los centros de información (puestos de comando y control). La red de información debe estar presente a través del campo de batalla y debe ser fluida, flexible, robusta, redundante y en tiempo real, tener integridad y seguridad, tener capacidad y accesibilidad, ser conjunta y capaz de apoyar una coalición.

El empleo de redes tácticas basadas en enlaces inalámbricos, sin nodos de comunicaciones tiene la ventaja que las fuerzas pueden dispersarse a requerimiento y aumentar su efectividad rápidamente en tiempo y espacio. De esta forma se tiene menos dependencia de los centros de pro-

cesamiento de información, que ahora pueden ser distribuidos para incrementar la supervivencia física sin sacrificar poder de procesamiento.

El término "digitalización del campo de batalla" se refiere a la automatización a través de redes y procesos digitales de las operaciones de mando y control a través de todo el ámbito del espacio de batalla. Esta integración de nodos terrestres, aéreos y marítimos (nodos de sensores, de comunicaciones, de mando y de sistemas de armas) en redes digitales continuas, requiere un intercambio digital compatible de data y situaciones operativas comunes a todos los nodos. La seguridad, compatibilidad e interoperabilidad son factores dominantes de conducción hacia la digitalización total a través de todo el espacio de batalla.

Finalmente, la implementación de sistemas de información y la tecnología de la información son esenciales para entregar la automatización necesaria para transferir, procesar y almacenar grandes volúmenes de data en el campo de batalla futuro. El desarrollo de la tecnología jugará un rol significativo en el apoyo a los comandantes para permitirles planificar y maniobrar más rápido que sus adversarios. Los sistemas de información y las tecnologías en los próximos años incrementarán considerablemente el alcance, volumen, exactitud y velocidad de la información disponible para la toma de decisiones (función del comandante).

Guerra de la información

Con la "Era de la Información" se produce una revolución en las operaciones militares que entrega una ventaja decisiva en el campo de batalla moderno, permitiendo a los comandantes obtener y explotar información de una forma más efectiva, aunque esto tiene su vulnerabilidad. Así como los sistemas de comunicaciones y de información son vitales para la sociedad civil y militar, estos pueden llegar a ser considerados como blancos principales en guerra y también pueden servir como medios principales para conducir operaciones ofensivas. Consecuentemente, la adopción de las tecnologías de la información por parte de los militares crea una nueva vulnerabilidad. La misma tecnología de la información que provee las mayores ventajas para las redes que apoyan a los comandantes modernos, también provee uno de los principales medios para su destrucción, esto porque una alta dependencia de los sistemas de comunicaciones y de información incrementa su vulnerabilidad. Entonces, mientras

los sistemas automatizados de comando incrementan la alerta situacional del comandante, estos también pueden volverse contra ellos y ser utilizados para contribuir a su incertidumbre respecto del campo de batalla.

El objetivo de la guerra de la información es alcanzar una ventaja significativa en la información que permita el rápido dominio y control de un adversario, incluyendo todas las acciones tomadas para preservar la integridad de los propios sistemas de información ante la explotación, corrupción o interrupción que el adversario pueda ejercer sobre ellos, mientras que al mismo tiempo se intenta explotar, corromper, interrumpir o destruir los sistemas de información adversarios, así como el proceso de alcanzar una ventaja de información en el empleo de las fuerzas.

La aplicación de la guerra de la información en las operaciones militares se llama Guerra de Mando y Control (GC2). El objetivo de la GC2 es influir, negar información, degradar o destruir las capacidades de C2 del adversario, mientras se protegen las capacidades de mando y control (C2) propias contra tales acciones.

Por otro lado, hablando de sistemas C2 y entendiendo a estos como redes de mando y control desplegadas en un teatro de operaciones, principalmente inalámbricas, hoy se utilizan protocolos de comunicaciones que encontramos en las redes civiles, sin ir más lejos el formato ip de internet está presente en un buen porcentaje de las redes de los sistemas C2. En otras palabras, las vulnerabilidades de este protocolo o de las aplicaciones que pueden operar sobre el, hoy afectan por igual a las redes civiles y militares y dentro de las militares incluidas las de sistemas C2. Es decir, el desarrollo de malwares, virus informáticos y todo tipo de vulnerabilidades informáticas explotadas y atacadas por los denominados hackers, hoy pueden tener víctimas tanto en redes civiles como militares. Cuando esta actividad se desarrolla con capacidades organizadas por un Estado para enfrentar a otro Estado y es conducida ya no por un grupo de hackers locales, sino que, por un grupo de profesionales dedicados a explotar vulnerabilidades de redes adversarias por medio del ataque coordinado, se le denomina Ciberguerra y toma lugar en el Ciberespacio. Se entiende el ciberespacio como toda red de computadores que transmiten data digital de voz, videos o archivos, siendo estas redes físicas o inalámbricas, de formato ip o de cualquier otro protocolo,

pudiendo por ejemplo ser redes telefónicas, de televisión, de radio transmisión, la misma internet, pero no exclusivamente, y otras más.

Por otro lado, el ciberespacio no puede existir sin el libre empleo del espectro electromagnético, medio natural de la propagación de su data y naturalmente los problemas de ciberseguridad son más factibles de ser experimentados por un ciudadano normal, cosa que vemos a diario en vulneraciones a las redes civiles o el simple robo de información desde bases de datos residentes en redes supuestamente protegidas, como es el caso de los fraudes bancarios que han afectado a un número considerable de ciudadanos a través de la violación de sus cuentas bancarias y tarjetas de crédito. Así, la ciberguerra se hace más notoria porque tiene cobertura civil y mediática (por ejemplo, el colectivo anonymous, el caso WikiLeaks y otros), que expone esta actividad a los noticieros y los medios en general, con la consecuente realidad de los ataques registrados a nivel internacional también. No se puede pretender que la guerra se ganará simplemente por el hecho de tener una ventaja tecnológica, sino más bien por cómo se integra y utiliza la tecnología.

La ciberguerra está comprendida dentro de las Operaciones de Información (IO). En su sentido militar, se define como las acciones tomadas de forma deliberada para obtener la superioridad en la información y denegarle esta al enemigo. La superioridad en la información también es un elemento clave en el concepto NEC (Network Enabled Capability). En estas operaciones se realizan las acciones ofensivas y defensivas necesarias para controlar la información, afectando los procesos y sistemas de información del adversario, y protegiendo los sistemas y procesos de información propios.

Operaciones de información

Las cinco capacidades básicas que se logran y se mantienen a través de la IO son las siguientes:

- Las Operaciones Psicológicas PSYOP, para lograr el dominio de la información.

- Operación de Contrainteligencia (CI), la propaganda contra las operaciones y los asuntos públicos.

- Operaciones de Engaño o Decepción (MILDEC), para inducir a error al enemigo.

- Operaciones de Seguridad (OPSEC), para evitar por ejemplo la liberación en internet de información militar pertinente y sensible.

- Guerra Electrónica (EW), muy importante y de amplio efecto sobre los sistemas de telecomunicaciones y de información, así también como sobre los sistemas de armas.

- Operaciones de Redes de Computadores (CNO), que le dan el marco a la ciberguerra y pueden ser divididas en tres. Computer Network Attack (CNA); Computer Network Explotation (CNE) y Computer Network Defense (CND).

En la siguiente figura se puede apreciar la relación de las diferentes cinco funciones de las operaciones de información mencionadas anteriormente y las tres actividades de las operaciones de redes de computadores.

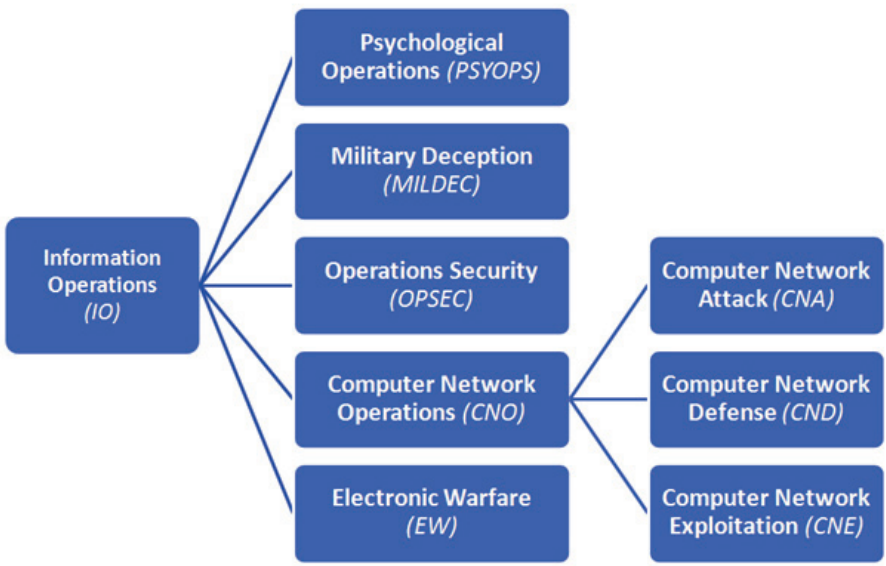

Figura 3.1: Las cinco funciones de operaciones de información y las tres actividades de las operaciones de red de computadores.
Fuente: https://www.infosecinstitute.com/

Operaciones de ciberguerra

Con el fin de determinar los efectos de la ciberguerra en un conflicto, a continuación se detallan los diferentes tipos de Operaciones de Redes de Computadores (CNO) que constituyen las estrategias básicas de operación en la ciberguerra.

Computer Network Operations (CNO)

Junto a la guerra electrónica se utiliza para interferir, perturbar, inutilizar, degradar o engañar los sistemas de mando y control del adversario. Anulando así su capacidad de tomar decisiones, preservando esa capacidad para los medios propios. Las CNO, según lo la Joint Doctrine for Information Operations de EE.UU., se divide en Computer Network Explotation (CNE), Computer Network Atack (CNA) y Computer Network Defense (CND).

Operaciones de Explotación de Redes de Computadores (CNE)

Las CNE comprenden acciones de recolección de información para inteligencia sobre sistemas adversarios. La mayoría de estos ciberataques se pueden clasificar como DDoS. Estos se caracterizan por la utilización de inyección de códigos únicos a través del lenguaje estructurado de consultas (SQL), junto con ataques DDoS de gran volumen, que explota las deficiencias de seguridad de las codificaciones de aplicaciones SQL Server. Se estima que los ataques de inyección SQL que se producen contra distintos sistemas pueden comprometer la totalidad de los datos almacenados en bases de datos, los que pueden ser robados o alterados. La información almacenada en estas bases de datos muchas veces consiste en combinaciones de nombre de usuario y una contraseña que pueden ser robados y utilizados más adelante durante la recolección de inteligencia dentro de otros sistemas.

Operaciones de Ataque a Redes de Computadores (CNA)

Las CNA considera acciones tendientes a perturbar, degradar, denegar o destruir información soportada por y en los sistemas información adversarios. Son originalmente operaciones de interrupción de servicios. La inmensa mayoría de los ataques son en forma de ata-

ques de DDoS contra sitios web de gobiernos, generando el cierre de hosting (sitios web) durante horas o días en un conflicto. Debido a esto, y a que los gobiernos se basan en la capacidad de internet para el control de la información, los ataques contra los sitios web de gobierno en la práctica afectan la capacidad de difundir información a través de la web a la ciudadanía y a la comunidad internacional, así como a algunos sistemas de comunicaciones que se basaban en telefonía e internet para su funcionamiento. Los ataques DDoS afectan significativamente las comunicaciones a través de correos electrónicos, teléfonos fijos y teléfonos móviles. Así entramos de lleno al campo de la guerra de la información a través de las ciberoperaciones.

También las modificaciones no autorizadas de las páginas y sitios web (defacement) se manifiestan en actos de cibervandalismo a modo de generar distracción, confusión y retrasos.

Operaciones de Defensa de Redes de Computadores (CND)

Son acciones de protección, monitoreo, análisis, detección, respuesta y recuperación frente a ataques, intrusiones u otras acciones no autorizadas que puedan comprometer la información y los sistemas críticos que la soportan. Son las acciones de preparación para hacer frente a la ciberguerra. Considera, en respuesta a los ciberataques el traspaso de la mayor parte de los sitios web corporativos a servidores ubicados en el extranjero, lo que facilita filtrar el tráfico malicioso hacia los sitios web. De igual forma, muchos sitios web atacados cambian su formato desde páginas web interactivas a blogs, lo que impide que muchos ataques DDoS puedan ser efectivos, ya que no existe servicio que denegar.

Las CNO, en combinación con las de guerra electrónica, se utilizan principalmente para interrumpir, perturbar, inutilizar, degradar o engañar los sistemas de mando y control del enemigo, anulando su capacidad para tomar decisiones con eficacia y oportunidad, preservando a la vez los sistemas de mando y control propios y amigos.

Como la guerra es el conflicto entre dos Estados, se tiende a poner en tela de juicio si existe realmente la ciberguerra como tal, así como si puede ser materializada como un conflicto independien-

te, ya que para la existencia de un conflicto y posteriormente una guerra se requiere al menos de dos actores con intereses contrapuestos. En caso contrario se trataría solo de un ciberataque, sobre todo teniendo en cuenta la dificultad que existe respecto de la identificación del atacante. Asimismo, se destaca en el desarrollo de este concepto, la necesidad de proteger los sistemas propios, junto con garantizar la libertad de acción para las fuerzas propias. De esta forma la ciberguerra se concibe como una actividad integral y solidaria, y no un concepto militar independiente. Además, el concepto incluye los componentes defensivos y ofensivos.

Como consecuencia, la ciberguerra se lleva a cabo como una acción común de los seres humanos y los computadores, generalmente representada en un grupo de actividades secuenciales y paralelas, y no un solo golpe, que incluso dependiendo de si se trata de una acción sorpresiva, puede dar inicio a una guerra.

Para EE.UU., la ciberguerra es el componente de las ciberoperaciones (CyberOps) que comprende el concepto de Global Information Grid (GIG) o Red de Información Global, que extiende el ciberpoder más allá de los límites defensivos del concepto de GIG para detectar, impedir, negar y derrotar a los adversarios. Las capacidades de ciberguerra típicamente se orientan a atacar computadores y las redes de telecomunicaciones, así como los procesadores y controladores embebidos en los equipos, sistemas e infraestructura. La ciberguerra no se limita a la internet, sino que incluye todo tipo de tecnologías digitales. Además, la ciberguerra es solo una parte de las ciberactividades militares.

Así el término ciberguerra es una combinación del término guerra y ciberespacio, que designa al conflicto militar en función de los medios de la tecnología de la información. En la práctica, este es el ataque a los computadores y sus datos, la red informática y los sistemas que dependen de las computadoras. Sin embargo, la mayoría de los autores consideran que los grandes ciberataques no se pueden llevar a cabo sin el apoyo gubernamental, debido a los recursos necesarios y las posibles consecuencias políticas. Por lo tanto, algunos de los ciberataques a gran escala se presentan en la literatura como ciberguerra, incluso cuando el agresor no pudo ser claramente identificado.

Igualmente, si el ataque tiene un trasfondo terrorista, al ataque se llama de manera regular ciberterrorismo; si el objetivo principal es la adquisición ilegítima de la información, se le llama el ciberespionaje. El ciberterrorismo y el ciberespionaje son ilegales, sin embargo, el término cibercrimen se utiliza sobre todo para los que se consideran delitos normales, tales como el robo de dinero a través del uso indebido de los datos bancarios en línea.

En contraste con la ciberguerra, el ciberespionaje trata de evitar daños en el sistema atacado para evitar ser detectado y garantizar el flujo de información después de la intrusión, es decir, se trata de una forma más pasiva de ataque. Sin embargo, a gran escala el ciberespionaje puede generar problemas o daños significativos en los equipos y redes, por lo que a menudo también es definido en la literatura como ciberguerra.

En síntesis, hay una superposición entre los términos y definiciones, por lo que la atribución de un incidente a un cierto tipo de ataque o agresor puede ser muy difícil. Por ello, sin las pruebas pertinentes, es una práctica regular entre los países el evitar acusar a otros Estados o gobiernos de dichas acciones.

Ciberataques

Los ataques surgen al mismo tiempo que las tecnologías de la información lo hacen, en estas tecnologías no solo se engloban los computadores sino cualquier dispositivo electrónico, como es el caso de los teléfonos móviles, laptops, tablets, GPS, etc., así como las comunicaciones. Estos ataques pueden afectar a cualquier nivel, ciudadanos, empresas, administración, infraestructuras críticas, sector bancario, etc. Se habla incluso de amenazas avanzadas, entendiéndose por ellas a las metodologías empleadas para evadir las medidas de protección de una compañía con el fin de desencadenar una variedad de ataques con un objetivo concreto, las que cada vez son más numerosas y difíciles de detectar, ya que las organizaciones en general carecen de medios, tecnología y personal para abordarlas apropiadamente.

La mayoría de los ataques se aprovechan de vulnerabilidades de los sistemas informáticos, sistemas operativos, aplicaciones y otros que generan agujeros de seguridad que surgen de una deficiente progra-

mación que no tiene en cuenta la seguridad en el ciclo de vida del desarrollo del software y los diversos protocolos de comunicación. Con el tiempo muchos protocolos han avanzado hacia versiones más seguras, por ejemplo, Telnet y SSL, http y https, ftp y sftp, entre otros.

Los tipos de atacantes

Los atacantes se pueden clasificar atendiendo a su motivación, como puede ser la búsqueda de un cambio social o político, un beneficio económico, político o militar o satisfacer el propio ego; su objetivo, ya sean individuos, empresas, gobiernos, infraestructuras, sistemas y datos de tecnologías de la información, ya sean públicos o privados; el método empleado, código dañino, virus, gusanos, troyanos y otros.

De esta forma, atendiendo a su autoría los ataques se pueden clasificar en:

- Ataques patrocinados por Estados. Referidos a cuando los conflictos del mundo físico o real tienen su continuación en el mundo virtual del ciberespacio. En los últimos años se han materializado ciberataques contra las infraestructuras críticas de países o contra objetivos muy concretos, pero igualmente estratégicos. Aquí también puede incluirse el espionaje industrial.

- Servicios de inteligencia y contrainteligencia. Regularmente empleados por los Estados para realizar operaciones de información. Suelen disponer de medios tecnológicos avanzados.

- Terrorismo, extremismo político e ideológico. Los terroristas y grupos extremistas utilizan el ciberespacio para planificar sus acciones, publicitarlas y reclutar adeptos para ejecutarlas, así como herramienta de financiamiento. Estos grupos ya han reconocido la importancia estratégica y táctica del ciberespacio para sus intereses.

- Ataques de delincuencia organizada. Las bandas de delincuencia organizada han comenzado a trasladar sus acciones al ciberespacio, explotando las posibilidades de anonimato que este ofrece. Este tipo de bandas tienen como objetivo la obtención de informa-

ción sensible para su posterior uso fraudulento y conseguir grandes beneficios económicos.

- Ataques de bajo perfil. Este tipo de ataques son ejecutados, normalmente, por personas con conocimientos TIC que les permiten llevar a cabo ciberataques de naturaleza muy heterogénea y por motivaciones fundamentalmente de índole personal.

La estrategia regular para un ataque típico a equipos y sistemas se inicia cuando la persona o grupo agresor intenta obtener acceso al equipo y/o red; luego, una vez que se ha logrado el acceso, se procede a instalar el malware que puede utilizarse para manipular el equipo, los datos o para robar los datos. Esto permite a su vez iniciar nuevas acciones en pro de la consecución de los objetivos del ataque. De esta forma los siguientes pasos constituyen la estrategia típica seguida para materializar un ataque a equipos y sistemas:

Primer paso: obtención de acceso

Algunos de los métodos comunes para obtener el acceso son los siguientes:

- Explotación de las brechas de seguridad en los sistemas operativos y software de aplicación (por ejemplo, Adobe y Windows), acción conocida también como explotación de vulnerabilidades. A través de scanner de puertos se puede realizar también el sondeo de computadores y redes, en busca de vulnerabilidades que permitan su ingreso.

- Mediante el uso de fuerza bruta se realiza de manera automática el hacking de contraseñas.

- A través de la ingeniería social se busca engañar intencionalmente a los usuarios. Un ejemplo de esto es cuando un falso administrador le pide a los usuarios de un sistema sus contraseñas.

- La manipulación de mensajes de correo electrónico con archivos adjuntos maliciosos y enlaces a sitios web que contienen código malicioso.

- El phishing es un método donde los usuarios son engañados y llevados a un sitio web malicioso, haciéndose pasar por una entidad de confianza para adquirir información sensible como nombres de usuario, contraseñas y detalles de tarjetas de crédito.

- La simulación o "Spoofing" es una situación en donde una persona o un programa se disfraza de otro para la falsificación de los datos.

- El Cross-site-scripting es un tipo de vulnerabilidad típico de las aplicaciones web, que permite a una tercera parte inyectar en páginas web vistas por el usuario, código JavaScript o en otro lenguaje script similar, evitando medidas de control como las políticas de seguridad del mismo origen. Este tipo de vulnerabilidad se conoce en español con el nombre de secuencias de comandos en sitios cruzados.

- Una manera más física de ser infectado es a través de la infección de medios de almacenamiento de datos, tales como discos duros externos, DVDs, USB Sticks y otros.

- La instalación intencional de brechas de seguridad o "backdoors", que permitan el acceso a los servicios secretos de un Estado. Microsoft Alemania, por ejemplo, confirmó en enero de 2007 una cooperación oficial con la Agencia de Seguridad Nacional Estadounidense (NSA), en relación con el sistema operativo Windows Vista, pero negó la existencia de puertas traseras. Además, Microsoft ha puesto en marcha el Programa de Seguridad de Gobierno (SGP), donde los gobiernos pueden acceder a cerca del 90% del código fuente. Sin embargo, EE.UU. también teme de puertas traseras, en particular en el hardware, por lo tanto, se evita el uso de chips asiáticos en tecnologías de seguridad relevantes. Por la misma razón, el Departamento de Estado de EE.UU., evita el uso de computadoras chinas en sus redes. Sin embargo, la defensa y el gobierno no pueden producir por sí solos todo el hardware y software que requieren, por lo que el uso de tecnologías COTS (Commertial off the Shelf Technologies) no puede ser evitada, siendo una fuente de vulnerabilidad. La cadena de suministro global de estos productos es también una fuente potencial de vulnerabilidades.

- Drive-by-download es la descarga involuntaria de programas maliciosos de internet durante una visita a un sitio web.

Segundo paso: instalación del malware y comienzo de la manipulación

El ciberespionaje se puede realizar por razones privadas, comerciales, penales o políticas, con el fin de intentar obtener información confidencial tal como contraseñas, números PIN, etc. En cambio, la ciberguerra trata de manipular los sistemas informáticos de manera activa.

En general, son tres los tipos de malware más relevantes: los virus (programas que infectan a los computadores), troyanos o caballos de Troya (programas que proporcionan información a otros equipos), y los gusanos (programas que son capaces de difundirse activamente a otros sistemas).

Típicamente, un programa de malware consiste en dos partes, una parte la infección, la que instala el programa en un computador y otras partes que contienen las instrucciones del atacante. Ejemplos de este tipo de programas son los keyloggers, que registran y reportan cualquier tecla que se pulse a otro computador, que permite tener una perspectiva general de todas las actividades, así como registrar todas las contraseñas. Otro ejemplo son los rootkits, que corresponden a herramientas que permiten el inicio de sesiones y manipulaciones por parte del atacante sin el conocimiento del usuario legítimo.

Ejecución de la ciberguerra

Los ataques de Denegación de Servicio Distribuidos (DDoS) desempeñan un papel clave en la ciberguerra. Como ya vimos previamente, un ataque DDoS corresponde al intento de hacer que un recurso no esté disponible para sus usuarios a través de ataques concertados de otros equipos. La herramienta más importante para un ataque DDoS es una botnet. En una botnet, los computadores pueden ser controlados a través de un software distribuido (Distribute Software o sistema distribuido,) que les permite cooperar entre sí para llevar a cabo una acción que requiere grandes capacidades de computación (bot se deriva de robot = trabajadores).

Normalmente, un gran número de máquinas son necesarios para generar el volumen de tráfico para saturar una red. Esto se llama de negación de servicio distribuido (DDoS), debido a que el ataque se lleva a cabo por múltiples máquinas que juntas pueden generar ese tráfico. Además, para ocultar el origen del ataque, estas máquinas son parte de redes diferentes, de modo que una sola red no puede ser identificada como la fuente generadora del bloqueo.

Normalmente consiste en la utilización de inyección de códigos únicos a través del lenguaje estructurado de consultas (SQL), que explota las deficiencias de seguridad de las codificaciones de aplicaciones SQL Server. Eso significa que, si un sistema no es efectivo para validar a un usuario, el usuario puede introducir comandos dentro de parámetros que se pasan de la aplicación web a la base de datos de respaldo. De esta forma, una inyección SQL efectivamente pone en peligro el servidor que soporta la base de datos atacada. Cabe señalar que a diferencia de un ataque DDoS que utiliza una red de miles de bots para saturar un sistema objetivo y hacer que se apague, la inyección SQL puede lograr el mismo efecto con solo unos pocos sistemas.

Los comandos inyectados se pueden utilizar para que el sistema se vincule asimismo con diferentes ciclos de comandos que lo afectan, o pueden ser utilizados para la obtención de información desde la base de datos afectada (espionaje). Cabe destacar que la mayoría de los expertos concuerdan que los ataques de SQL son extremadamente difíciles de detectar cuando están cubiertos por un ataque DDoS a gran escala.

Una forma más reciente de ciberataque es la denegación del servicio distribuido reflejado (Distributed Reflection Denial of Service o DRDOS), que corresponde a solicitudes automatizadas que se envían a un gran número de equipos, los que remiten a su vez su respuesta a las peticiones. A través de la suplantación de protocolos de internet se entrega una dirección ip errónea como dirección de origen de todas las respuestas, las que irán al computador de la víctima (que normalmente tiene esta dirección) y la sobrecargan. Este tipo de ciberataque hace que la identificación del atacante sea aún más difícil que en la DDoS.

Una red coordinada de robots se denomina botnet, la que permite dirigir a miles de computadores contra otros sistemas. Redes de bots pueden ser ilegales, aunque incluso es posible arrendarlas en la ac-

tualidad. El predominio de las redes de bots en la ciberguerra se basa en los siguientes aspectos:

- Las botnets a menudo no se encuentran en el país del atacante, lo que hace difícil la localización y atribución de un ataque, y por ende un contraataque inmediato casi imposible.

- Las botnets proporcionan grandes capacidades de computadores (procesadores) necesarios para un ataque con éxito.

- Las botnets permiten los ataques dirigidos, mientras que los virus y los gusanos pueden propagarse sin control e incluso afectar a los sistemas propios o aliados.

- Las botnet, teóricamente, pueden ser ubicadas en cualquier computador, por lo que no es posible proteger un sistema mediante la exclusión de ciertos grupos de computadores.

- En resumen, para una determinada maniobra, las redes de bots pueden ser utilizadas para un ataque masivo, sorpresivo, eficiente y manejable.

Otros métodos de ataques utilizados:

- Desfiguración de un sitio web (website defacement), cuando se modifica el aspecto y contenido de un sitio web por razones de propaganda.

- La infiltración y la manipulación de las infraestructuras críticas, como sistemas de radar, las redes eléctricas y sistemas de control de plantas de energía y el sabotaje de sistemas informáticos, que a menudo son un efecto secundario del espionaje masivo y los posteriores fallos del sistema. Las nuevas tecnologías pueden cambiar el escenario y las estrategias de forma súbita y por completo, por ello la historia de la ciberguerra no permite predecir la evolución futura de ella. Sin embargo, se puede esperar que las botnets serán utilizadas en el futuro como instrumento básico para ataques a gran escala.

De manera general un ciberataque se caracteriza primero por la presencia del atacante, luego por la ejecución de actividades de sondeo

de los equipos y redes con el propósito de acceder a estas. Cabe señalar que en esta etapa es donde se materializa la denegación del servicio, previamente abordada.

Una vez obtenido el acceso, se interviene en los equipos y redes con el fin de crear las condiciones que le permitan incrementar los privilegios de usuario y poder explotar de esta forma en su beneficio los equipos y redes atacados. Finalmente, se configuran puertas de acceso traseras que permitan el acceso y explotación posterior del sistema afectado de manera encubierta, en la oportunidad y frecuencia que se requiera.

La autoría de los ataques

La determinación de la autoría, es decir, la identificación y localización de un atacante para iniciar las contramedidas es un objetivo relevante y prioritario, pero difícil de lograr. Sin embargo, como la investigación para determinar la autoría está en curso, en lugar de apagar inmediatamente un equipo infectado, regularmente se mantiene encendido con el fin de ser utilizado para saber qué información se envía y a quién, a pesar de que a menudo el flujo de información va a través de servidores intermedios.

Además, los hackers crean huellas digitales, que son los códigos típicos de programas o ciertos patrones de acceso que permiten la caracterización de un determinado grupo de atacantes. Sin embargo, esto no permite aclarar si un atacante está trabajando en nombre propio, de otro Estado o autoridad específica.

Las ciberarmas

Las ciberarmas se pueden definir como herramientas de software que pueden atacar, invadir, realizar espionaje y manipulación de computadores, así como controlar la autorreplicación y distribución. Idealmente, esto debe incluir la opción de autodesactivación (que va en silencio). El uso de este tipo de software es cada vez más común y la diferenciación convencional entre virus, gusanos y troyanos es cada vez menos relevante.

El término ciberarma no se refiere solamente a una herramienta militar, ya que como los principios técnicos son esencialmente los mismos, el software puede ser utilizado también para ciberdelitos.

Los objetivos de la ciberguerra

Los objetivos más probables en una ciberguerra son las redes que controlan la infraestructura crítica. Así las redes críticas son aquellas que si se interrumpen de manera significativa por un período determinado (varios días o varias semanas o indefinidamente), o se afecta su funcionamiento de manera irregular o intermitente, pueden afectar la vida cotidiana de las personas y el funcionamiento normal de un Estado.

Las redes afectadas pueden ser de diferente naturaleza y alcance, a menudo integrada incluso con otras redes en una cadena redundante. Sin embargo, hay sistemas que no cuentan con sistemas redundantes en cuya operación podrían verse afectados por la interrupción o denegación, así como la desinformación, lo que podría eventualmente poner fin a todas las actividades relacionadas con la red, tales como:

- El sistema de emergencias 911 en Estados Unidos, o en caso de Chile los diferentes números de emergencias tales como el 131, 132, 133 o 134, entre otros.

- Los sistemas de transporte aéreos y terrestres, tales como el metro y el aeropuerto de Santiago, respecto de sus sistemas de control automático de tráfico, de emisión de tickets y control de pasajeros.

- Sistemas de información médica de control de datos sensibles, tales como los requerimientos de donantes, dosis y registros de pacientes críticos.

- Las funciones de las Isapres respecto de la emisión de bonos y atenciones médicas.

- Las AFP respecto de los fondos previsionales de cada cotizante o pensionado en el sistema.

- Los principales bancos nacionales respecto de la gestión de créditos, cobranzas y movimientos en las cuentas corrientes de sus clientes.

- El Banco Central de Chile o la Reserva Federal de EE.UU., así como las compañías de tarjetas de crédito y otras instituciones financieras, respecto de sus operaciones de captación y colocación de fondos.

Considerando los aspectos referidos a ciberguerra abordados en este capítulo, queda en evidencia el gran dinamismo, crecimiento, evolución, complejidad y vulnerabilidad simultánea asociada con las tecnologías que sustentan el dominio de la ciberguerra. De esta forma, las operaciones de redes computacionales (CNO) son capaces de afectar redes o sistemas críticos de los Estados a nivel nacional, pudiendo potencialmente interferir en la vida diaria de las personas, socavar la confianza de la sociedad en sus instituciones y provocar daños significativos en los principales sectores económicos de un país, con repercusiones nacionales o multinacionales, incluso potencialmente más perjudicial que cualquier acontecimiento de carácter local.

Asimismo, se establece que el término ciberguerra es una combinación de los conceptos de guerra y ciberespacio, que designa al conflicto militar en función de los medios de la tecnología de la información que utiliza en pro de la consecución de sus fines. Destacándose que la velocidad de los cambios que permite el ciberespacio, implica que se requiere de poco tiempo para realizar un ataque o para implementar nuevas defensas, comparado con lo que sucede en el espacio físico, respecto de operaciones convencionales durante conflictos armados tradicionales.

Respecto de la estrategia típica de un ciberataque, la mayoría de los ataques aprovechan las vulnerabilidades de los sistemas informáticos, particularmente de las redes críticas; que la naturaleza del conflicto diferirá de la naturaleza y objetivos de los participantes; y que el alcance, dirección, duración y propósito de los ciberataques observados, son difíciles de identificar ya que a menudo resulta complejo detectar y diferenciar los hilos de las diversas relaciones de causa y efecto que los caracterizan.

En tal sentido se destaca que un adversario puede emplear diversas técnicas de encubrimiento para ocultar el origen de la acción, lo que complica su trazabilidad. Por ello, la determinación de la autoría, es decir, la identificación y localización de un atacante para iniciar las contramedidas, es un objetivo relevante y prioritario, pero sin lugar a dudas difícil de lograr.

Así, de acuerdo a las diferentes concepciones descritas de ciberespacio y ciberguerra, resulta pertinente destacar que la información y la capacidad para gestionarla, se han constituido en factores relevantes para la articulación y progreso de la sociedad, y por esta razón, han contribuido al desarrollo y consolidación del ciberespacio y de la ciberguerra, como dimensión y medio relevante para la defensa y la seguridad de los Estados y las personas.

Si se considera la ciberguerra como un ciberataque en contra de un Estado con efectos perjudiciales para este, que se lleva a cabo presumible o supuestamente con el apoyo de uno o más Estados, atendiendo su extensión y/o complejidad, es necesario considerar que a diferencia de los conflictos convencionales, la información sobre el incidente o los incidentes es regularmente presentada solo por una de las partes afectadas, la mayoría de las veces por la víctima y en casos excepcionales por el atacante. Esta información unilateral, hace extremadamente difícil poder estructurar pruebas y análisis objetivos.

A continuación, se describen algunos de los principales conflictos contemporáneos, en los que se utilizaron las capacidades de la ciberguerra, ya sea para defender y/o afectar determinados intereses de algunos Estados y organizaciones.

Guerra de Yugoslavia en 1999

Para diversos autores corresponde al primer conflicto en el que se utiliza la ciberguerra de manera concreta en las acciones bélicas, como lo fue el bloqueo de las redes telefónicas de Yugoslavia por la OTAN durante el conflicto de Kosovo en 1999. Cabe destacar que, tras el bombardeo de la embajada china en Belgrado, los hackers chinos atacaron sitios web del gobierno de EE.UU., tales como el sitio web de la Casa Blanca, el que permaneció fuera de línea por tres días debido a precauciones de seguridad ante la persistencia de los ataques de Denegación de Servicio Distribuidos (DDoS).

Ataques masivos a gobiernos occidentales e industria

Existe consenso entre los expertos de que una "ciberguerra fría" entre EE.UU. y China ha estado ejecutándose desde hace años, en donde las redes civiles y militares han sido los objetivos principales de China, así

como las empresas fabricantes de armas. Se estima por ejemplo que China en el año 2007 logró obtener entre 10 y 20 terabytes de datos de los respectivos equipos y sistemas de Estados Unidos. Ese mismo año el Departamento de Seguridad Nacional informó de la detección de más de 117.000 ataques a sus equipos y sistemas. A estos se le sumaron una serie de ataques durante un par de años, denominados "Titan Rain" por EE.UU. Asimismo, el gobierno federal de Alemania informó de ataques a sus sistemas informáticos a un ritmo similar.

El análisis de "Titan Rain" reveló que el patrón típico de los ataques era que un equipo de entre 6 a 30 hackers tomaba el control de las computadoras y sistemas, luego copiaba todos los archivos del disco duro en período de 30 minutos, para posteriormente enviar la información obtenida a través de una botnet hacia servidores ubicados en la provincia china de Guangdong, sin embargo, esto no pudo finalmente ser comprobado.

Otros grandes ciberataques

GhostNet y Aurora fueron otros grandes ataques ocurridos en el año 2009. GhostNet fue un ataque informático a gran escala en contra de embajadas en EE.UU., entre otras las de India, Corea del Sur, Indonesia, Tailandia, Taiwán, Alemania y Pakistán, así como de los ministerios de Relaciones Exteriores de Irán, Bangladesh, Indonesia, Brunei y Bután. El virus permitía activar la webcam y micrófonos de los equipos, dando la posibilidad de monitorear la habitación en donde se encontraba el computador infectado. A través de la Operación Aurora en el año 2009, los ciberatacantes presumiblemente chinos, trataron de acceder a los programas informáticos y códigos fuente de las compañías del sector de TI de EE.UU., tales como Google y Adobe, entre otras, así como a otras empresas de alta tecnología del sector de seguridad y defensa.

La Operación Dragón Nocturno es otra de las operaciones de ciberataques a gran escala que se han realizado. Esta se llevó a cabo en contra de diferentes empresas de la industria del petróleo, energía y petroquímicas a nivel mundial. Asimismo es posible destacar la Operación "Shady RAT", llevada a cabo presumiblemente por China en contra de 72 organizaciones de nivel mundial por más de 5 años a contar de julio del 2006. Cabe destacar que China niega rotundamente alguna vinculación con esta y otras operaciones.

Ataque realizado contra Estonia en el 2007

Entre el 29 de abril y el 11 de mayo de 2007 diversos sistemas de Estonia fueron afectados masivamente por un ataque de denegación de servicio distribuido (DDoS), a consecuencia de la decisión del gobierno de remover un monumento ruso que representa para Rusia la liberación de Estonia de Hitler, el que era percibido por Estonia como símbolo de represión por parte de Rusia. Las redes de Estonia fueron saturadas de datos procedentes de Rusia, sin embargo, probablemente no por el Estado sino por las organizaciones patrióticas. Algunos equipos tuvieron un incremento de 1.000 solicitudes por día a 2.000 solicitudes por segundo y el ataque se prolongó durante semanas. Las páginas web del gobierno, los partidos políticos y los bancos fueron atacadas y colapsaron.

La agresión provocó que Estonia pidiera la intervención de la OTAN y, en agosto de 2008, se puso en marcha el Centro de Excelencia para la Cooperación en Ciberdefensa (CCD) de la OTAN en Tallinn, capital de Estonia.

Este ataque es uno de los más documentados y estudiados internacionalmente, y debido a que la OTAN apoyó a Estonia es que pudo ejecutarse una acción forense exhaustiva sobre las redes y computadores afectados. En la siguiente figura se expone una representación gráfica y cronológica de los diferentes tipos de ataque que allí ocurrieron y las consecuencias que generaron sobre la infraestructura crítica de ese país.

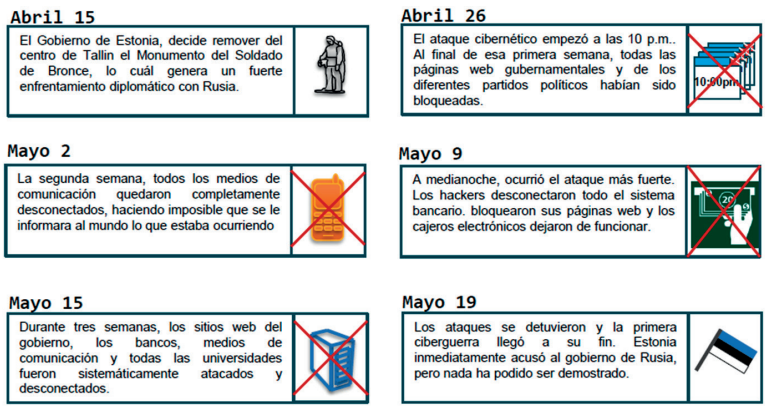

Figura 3.2: Cronología del ataque y consecuencias inmediatas contra Estonia, 2007.
Fuente: www.mindefensa.gov.co

Ataque contra Siria en el 2007

El 6 de septiembre de 2007, una planta considerada como nuclear por Israel fue bombardeada y destruida en Siria por la Fuerza Aérea israelí. Este ataque requería para su éxito de un extenso sobrevuelo por el espacio aéreo sirio sin ser detectado. Israel fue técnicamente capaz de afectar los sensores sirios y ocultar la presencia de sus aeronaves, simulando un cielo libre de tráfico para los sistemas de defensa aérea, pudiendo así realizar este ataque sin perturbación. Este conflicto representa de manera clara, la forma en cómo la ciberguerra puede ser utilizada como una capacidad que incrementa y multiplica el poder de las fuerzas y una herramienta adicional en apoyo a ataques convencionales.

Ataque a Georgia en el 2008

De manera previa al comienzo de la guerra convencional entre Georgia y Rusia en 2008, Georgia denunció ciberataques masivos en contra de sus sistemas de infraestructura crítica, por ejemplo, los medios de comunicación, la banca y el transporte. Algunas semanas antes del inicio del conflicto, el 20 de julio de 2008, la página web del presidente de Georgia fue bloqueada por un ataque de denegación de servicio distribuida (DDoS). Además, se ejecutó la modificación no autorizada del sitio web (defacement), en el cual fotos de Hitler se pusieron al lado de las fotos del presidente georgiano. Asimismo, un día antes del inicio del ataque convencional, un ataque masivo de DDoS afectó seriamente los sistemas TI del país.

Ataque con virus a UAV de EE.UU., 2009-2011

Durante los años 2009 al 2011, los insurgentes iraquíes utilizaron softwares disponibles en el mercado para acceder al sistema de control a distancia de los UAV empleados por Estados Unidos en sus operaciones en Irak y Afganistán, permitiéndoles obtener a través de sus laptops, información de inteligencia en función de grabar y visualizar los videos obtenidos por estas plataformas. En el año 2011, la Base Creech de la USAF en Nevada, que sirve como base de operación de los sistemas MQ-1 Predator y MQ-9 Reaper, informó que sus sistemas habían sido infectados por un virus, pero negó cualquier impacto en la disponibilidad y operatividad de los aviones no tripulados.

Ataque a Irán por el virus Stuxnet en 2009-2010

Stuxnet fue el primer virus informático específicamente diseñado para causar daño en el mundo real, en lugar del mundo virtual. A diferencia de otros malwares previos, este es capaz de causar problemas físicos secundarios, afectando de manera específica el software que controla los sistemas industriales de Siemens denominado SCADA (Supervisory Control And Data Adquisition); es un software que permite controlar y supervisar procesos industriales a distancia. En concreto, Stuxnet fue diseñado para dañar la maquinaria en las instalaciones de enriquecimiento de uranio iraní en Natanz.

De acuerdo a datos de la Agencia Internacional de Energía Atómica, los expertos consideran que Stuxnet destruyó un número importante de centrífugas de Irán, esencialmente plataformas gigantes utilizadas para enriquecer uranio, haciéndolas girar fuera de control hasta autodestruirse. Cabe señalar que Stuxnet es un gusano, es decir, un programa que es capaz de propagarse activamente a otros sistemas, explotando vulnerabilidades del sistema Windows. A pesar de que fue descubierto en el año 2010, se estima que durante el año 2009 ya habría infectado los primeros computadores en Irán a través de una memoria USB infectada.

Es pertinente señalar que, a diferencia de otros conflictos, este no se enmarca en una guerra formal entre dos Estados, pero si forma parte de un conflicto entre dos o más Estados, como lo es el que ha sostenido Irán respecto de su programa nuclear, de manera general con Naciones Unidas y en forma específica con EE.UU. e Israel.

En el año 2010, el actual presidente de EE.UU. Barack Obama decidió retomar un plan iniciado por el presidente George Bush para boicotear los sistemas informáticos de Irán e intentar frenar así su programa nuclear. Entre las campañas de ciberarmas que Obama aprobó se encuentra Stuxnet, virus que se desarrolló con la colaboración de Israel [15].

En el año 2011, los sistemas informáticos de Irán, en especial los relacionados con su programa energético, sufrieron varios ataques informáticos importantes. Este malware atacó específicamente las instalaciones nucleares iraníes en Natanz, el que realizó una acción

de sabotaje (CNA) no detectado contra los variadores de frecuencia de las centrífugas de enriquecimiento de uranio, interrumpiendo su funcionamiento.

El malware fue detectado en varios lugares del mundo y plantas nucleares de Irán, sin embargo, solo causó daños en la planta nuclear de Natanz. Stuxnet es un gusano informático que afecta a equipos con el sistema operativo Windows, es el primer malware conocido que espía y reprograma sistemas industriales, es considerado un prototipo funcional de un ciberarma, que puede conducir a la creación de una nueva carrera armamentista en el ciberespacio a nivel mundial.

Stuxnet atacó equipos con Windows empleando vulnerabilidades de día cero o de origen de este sistema operativo. Su objetivo son sistemas que emplean los programas de monitorización y control industrial (SCADA) WinCC/PCS de Siemens.

Stuxnet fue introducido a la planta nuclear de Natanz, a través de un doble agente que trabajaba para Israel. Este agente introdujo el virus al sistema de control industrial mediante una memoria USB. Una vez dentro del sistema, el virus comenzó a infectar las computadoras del sistema de control central, reprogramando las computadoras, y por lo tanto el software, el que comenzó a dar nuevas instrucciones a las máquinas industriales que controlaba. Permaneció inactivo durante períodos de 35 días para, de forma imprevista y durante apenas siete minutos, acelerar los rotores de las centrífugas hasta el límite de la destrucción o desacelerarlo hasta llegar prácticamente a la inactividad. Sumado a lo anterior, y en forma paralela, el virus enviaba falsas señales al sistema de control para que el sistema considerara que todo seguía funcionando sin observaciones.

En concreto, según la empresa Symantec, Stuxnet verifica la existencia en el objetivo de cierto número de motores de las centrífugas fabricadas por dos empresas concretas, una iraní y otra finlandesa, estableciéndose rutinas distintas según la cantidad de centrífugas de uno y otro fabricante. Ante la falta de reportes formales, las evidencias existentes sobre el ataque de Stuxnet a la planta nuclear Iraní de Bushehr por ejemplo, muestra que el malware fue diseñado para sabotear lentamente la planta. El código debía implantar órdenes para acelerar y ralentizar la maquinaria física durante un par de semanas.

De esta forma se buscó que el programa pasara inadvertido dentro del sistema, incubándose por un largo tiempo y cambiando paulatinamente el proceso sin llegar a descomponerlo. Inicialmente al ser detectado, se consideró que era un gusano más creado con la finalidad de robar información. Sin embargo, los expertos pronto determinaron que contenía códigos diseñados específicamente para atacar los sistemas Siemens SCADA, encargados de controlar el manejo de tuberías, plantas nucleares y otros equipos industriales. De manera concreta en este caso los investigadores determinaron que Stuxnet fue diseñado para interceptar órdenes enviadas desde un sistema SCADA para controlar cierta función dentro de una instalación. Aunque el último análisis de Symantec no ha encontrado qué función en específico debía ser atacada, la información sugiere que Stuxnet apuntaba a las instalaciones nucleares de Bushehr o Natanz, en un claro intento por sabotear el naciente programa nuclear iraní. De acuerdo con Symantec, Stuxnet ataca los variadores de frecuencias, los que son usados para controlar la velocidad de un dispositivo -como un motor.

Stuxnet intercepta las órdenes del software de Siemens SCADA, y las reemplaza con comandos maliciosos para modificar la velocidad del motor, de modo que este varíe de manera significativa a intervalos intermitentes. Sin embargo, Stuxnet no sabotea cualquier variador de frecuencia. El programa revisa la red de la planta, y solo se activa si la instalación tiene cuando menos 33 variadores hechos por la empresa iraní Fararo Paya, o por la finlandesa Vacon. Específicamente, Stuxnet solo ataca dispositivos diseñados por estas dos compañías si están corriendo a alta velocidad (entre 807Hz and 1210Hz). Ese rango de celeridad solo se utiliza en aplicaciones selectas, tales como en los procesos de enriquecimiento de uranio. De hecho, la exportación de variadores de frecuencia que pueden superar los 600Hz está controlada por la Comisión Regulatoria Nuclear de Estados Unidos. Su grado de sofisticación es tal que, si el número de variadores de la firma iraní supera la de la firma finlandesa, el malware libera una secuencia. Si ocurre el caso opuesto, entonces el virus activa una secuencia diferente. Estos detalles hacen pensar que los desarrolladores de Stuxnet tenían en mente una instalación específica a la cual atacar, así como un conocimiento extenso sobre el sistema.

Para el éxito de Stuxnet, se necesita de un proceso continuo que corra durante un mínimo de un mes de forma ininterrumpida. El

enriquecimiento de uranio cumple perfectamente esta premisa. Las centrífugas necesitan girar a una velocidad precisa durante largos periodos para extraer el material puro. Si esas centrífugas cambian su aceleración, se puede interrumpir el proceso de aislamiento de los isótopos más pesados. El resultado es un uranio de muy pobre calidad. En tal sentido, se estima que el gusano incluye dos componentes importantes. Uno se diseñó para hacer que las centrífugas nucleares de Irán giraran fuera de control. Otro vinculado directamente con las operaciones CNE, destinado a que el programa registre de manera encubierta el tipo de operaciones normales que se realizaban en la planta nuclear, para luego volver a introducir esos resultados en los operadores de la planta, como una cinta pregrabada de seguridad en un asalto bancario, con el fin de que pareciera que todo funcionaba normalmente, cuando en realidad las centrífugas estaban fuera de control hacia su destrucción.

Cabe señalar que los ataques no fueron totalmente exitosos ya que, según los informes de inspectores nucleares internacionales, solo algunas de las operaciones de Irán se detuvieron mientras que otras se estima continuaron de manera casi normal. Tampoco existe certeza que los ataques se hayan terminado, debido a que algunos expertos que han examinado el código creen que contiene las semillas para más versiones y ataques posteriores.

Tanto las actas de la Agencia Internacional de Energía Atómica (OIEA) [16], así como, diversas fotografías y videos que circularon por la red, dejaron en evidencia los daños provocados por el ciberataque más importante sufrido por una instalación nuclear. Estos reportes señalan las dificultades que tuvo Irán para hacer frente a la importante falla en el equipo de su principal planta de enriquecimiento de uranio, mientras estaba siendo atacada por Stuxnet. Sin embargo, los reportes de la OIEA también muestran el febril esfuerzo por parte de los científicos iraníes para contener el daño y reemplazar las piezas dañadas, a pesar de las limitaciones que les representa las sanciones internacionales que prohíben a Irán la compra de equipos nucleares.

La reacción del gobierno de Irán a los ataques en contra de sus capacidades nucleares, denota que las operaciones de ciberguerra no generaron en la práctica efectos en el ámbito político de su poder nacional. Prueba de ello, es que Irán en un período de seis meses

entre finales de 2009 y principios de 2012, de acuerdo a reportes de funcionarios de la ONU, desmanteló más del 10% de las máquinas centrífugas de enriquecimiento de uranio utilizados en la planta de Natanz. De esta forma, nuevas máquinas llegaron a la planta para reemplazar a las que se perdieron.

Asimismo, a pesar de los contratiempos que significó Stuxnet en su programa nuclear, se aprecia que, a instancias del gobierno, los científicos iraníes trabajaron activamente para mantener una producción constante y estable de uranio de bajo enriquecimiento.

Queda claro entonces, que el mayor efecto en el ámbito militar generado por las operaciones de ciberguerra en contra de Irán, es el retraso del reloj nuclear de Irán ocasionado por Stuxnet. Asimismo, que la línea entre la acción encubierta y el acto de guerra, están desapareciendo en la historia actual y en una de las regiones más volátiles del mundo.

Es evidente el efecto concreto de Stuxnet en este ámbito del poder nacional de ambos países; en el caso de EE.UU., incrementó su poder militar y logró afectar de manera concreta el potencial militar de Irán, sin tener que llegar a una campaña de bombardeo en su contra para destruir las capacidades más importantes de Irán para producir uranio con fines militares. Entonces una campaña de bombardeo que no destruya totalmente esas capacidades dejaría a Irán en condiciones de reconstruir rápidamente su programa nuclear y lo motivaría incluso a llevar a cabo un programa intensivo para construir una bomba, lo que solo haría más peligrosa e inestable a la región. Finalmente, si bien la Casa Blanca y la CIA se han negado a comentar tanto sobre Stuxnet como Flame, el Viceprimer Ministro de Israel en una entrevista con el diario The Washington Post en junio de 2012, dio a entender que los ciberataques ahora forman parte de las buenas prácticas de un juego justo, cuando se trata de Estados agresores. Como resultado, se estima que las próximas guerras en el medio oriente están cada vez más cerca de ser desarrolladas de manera intensiva en el ciberespacio, a través de redes y computadores, en lugar de las dimensiones tradicionales de la guerra, como lo son la tierra, el mar, el aire y el espacio.

De lo discutido hasta ahora, la velocidad de los cambios en el ciberespacio, comparado con los cambios factibles de alcanzar en el espacio

físico, es una cualidad fundamental del medio que contiene a la ciberguerra, ya que determina el poco tiempo que se necesita para realizar un ataque o para implementar nuevas defensas. Asimismo, el gran potencial que tiene el desarrollo de acciones ofensivas y defensivas muy rápidas y breves, en función de los efectos que se puede alcanzar, tanto en conflictos entre particulares como entre Estados. De esta forma, ante el dinamismo del ciberespacio y la ciberguerra, las capacidades y vulnerabilidades de los actores tienden a ser temporales, así como las estrategias para explotarlas.

Por ello, las vulnerabilidades de los sistemas son un elemento primordial en los ciberataques ya que corresponde a la esencia de las capacidades ofensivas, defensivas y de inteligencia que cada actor puede y debe desarrollar en el ciberespacio, con el fin de explotarlo y protegerse. En este contexto, la globalización es una fuerza que permite ampliar el alcance y profundidad del ciberespacio y por lo tanto los efectos de la ciberguerra. Factor cada vez más gravitante que motiva a algunos líderes políticos y militares a considerar a las ciberarmas como armas de destrucción e interrupción masiva.

Por ello, tal como lo demuestra el ataque a las capacidades nucleares de Irán primero a través del Stuxnet y luego Flame, la preparación de un ciberconflicto requiere desarrollar capacidades específicas y permanentes, pero en constante evolución, que permitan conocer el terreno de la zona potencial del conflicto, las capacidades defensivas y ofensivas de los actores, así como establecer la posibilidad real de generar daños colaterales y escaladas no planificadas.

Con lo descrito en el presente capítulo se puede comprender que más allá de la diversidad que caracteriza a las operaciones de ciberataques, ya sea en función de la región del mundo en el que se desarrollan, de las características y sofisticación de los actores involucrados, así como del propósito que persiguen, todos los tipos de ataques utilizan medios tecnológicos y métodos similares, lo que hace muy difícil o incluso imposible la identificación del agresor y sus motivos.

Los Estados, y particularmente los organismos responsables de su seguridad y defensa, deben asumir que el mapa de la ciberguerra está en constante evolución y los esfuerzos de vigilancia y reconocimiento del ciberespacio deben ser constantes, atendiendo que la

posibilidad de un conflicto en el ciberespacio es cada vez más latente y de implicancias insospechadas para los Estados.

La mayor contribución de la ciberguerra en los conflictos modernos está vinculada principalmente con su capacidad para obtener información del adversario de manera encubierta y con menores niveles de riesgo, debido a la complejidad existente para la detección y trazabilidad de sus operaciones. Por esta razón, la identificación y localización de un atacante para iniciar las contramedidas es un objetivo relevante y prioritario, pero sin lugar a dudas difícil de lograr para todos los Estados.

El nivel de desarrollo de capacidades de ciberguerra de un Estado, y el balance de estas entre ofensivas y defensivas están directamente relacionados. De esta forma, mayores capacidades de ciberguerra le permiten a un Estado ser menos vulnerable a las CNO que se desarrollen en su contra, junto con incrementar los potenciales beneficios de su utilización en su favor.

Los efectos de la ciberguerra en los conflictos modernos son directamente proporcionales a las capacidades de ciberguerra con que cuente un Estado y directamente proporcionales también a las vulnerabilidades que en este ámbito caractericen a un blanco. De esta forma, Estados con un mayor nivel de desarrollo y penetración de las TICs, tenderán a estar más expuestos a operaciones de redes de computadores, y sus efectos podrían ser más significativos en el desarrollo y consecución de un conflicto con otro Estado.

No existen sistemas que estando vinculados a internet o que trabajen en red, a pesar de la magnitud y sofisticación de las medidas de seguridad que se implementen, sean absoluta y totalmente seguros e inmunes a las operaciones de ciberguerra. La ciberseguridad es un desafío permanente y cada vez mayor para todos los países, sobre todo para aquellos en vías de desarrollo, los que por una parte están escasamente preparados, en particular en materias de inteligencia y son altamente vulnerables debido a su creciente nivel de desarrollo e incorporación de las TIC.

Capítulo IV
El Futuro de las Amenazas

Un computador o una red de computadores no monitoreados genera una incertidumbre total respecto de su seguridad. Se puede invertir mucho en seguridad para un computador, para una red y para sus usuarios (firewalls, antivirus, encriptación, etc.), pero si no se monitorea esa red… no existe certeza de su seguridad y/o vulnerabilidad. Esto es lo que un CSIRT realiza, monitorea las redes de su responsabilidad en términos de la seguridad de los flujos de información tanto internos como las comunicaciones de entrada y salida con el exterior, evitando que se genere fuga de información por canales no autorizados, ya sea voluntaria o involuntariamente, deteniendo el flujo de esta cuando no obedezca a conductas autorizadas y esperadas por parte de sus componentes y/o contactos externos.

Entonces, el equivalente a un CSIRT es el cuerpo de guardia de una unidad militar, que como tal tiene muros muy altos o al menos cercos con serpentín de alambre con púas (equivalente a un firewall), con cámaras en un circuito cerrado de televisión para tener imagen las 24 horas del día del perímetro evitando de esta forma el ingreso no autorizado y habilitando un pórtico de acceso donde existe un control positivo de quien ingresa o se retira de la unidad, impidiendo de esta forma el ingreso de personas no autorizadas a la unidad e impidiendo que salga material de esta a la vía pública. En el mismo sentido opera un CSIRT, pero su foco es la comunicación de las redes y la información que se gestiona internamente y que se envía y se recibe del exterior.

Amenazas futuras

Según lo expuesto hasta aquí en este ensayo, se puede hacer una predicción respecto a las posibles tendencias de ciberamenazas para el futuro próximo:

- **Ciberespionaje**
  Es altamente probable que se experimente un aumento en el empleo del ciberespacio para la obtención de inteligencia y se incrementará por todos los países de nuestro entorno por su eficacia y dificultad de atribución. Debido a la publicación de campañas de ciberespionaje realizada por compañías de seguridad, los países emplearán más recursos en la seguridad de sus operaciones, aislando infraestructuras y diversificando las técnicas, tácticas y procedimientos de ataque.

- **Ataques como servicio**
  Es altamente probable que, a través de grupos con conocimiento y capacidad técnica avanzada, se contrate sus servicios y se planifiquen ataques a medida, con garantías de éxito. Requerirá ampliar el conocimiento de las redes Deep Web, incrementar la cooperación público-privada y armonizar la legislación internacional. (Deep Web o Hidden Web es la web profunda u oculta, no accesible a través de navegadores convencionales. Usualmente se utilizan herramientas como TOR [The Onion Router] para acceder a ella).

- **Fusión de técnicas, tácticas y procedimientos utilizados por el ciberespionaje y la ciberdelincuencia**
  Es de esperar una alta y rápida evolución de la actividad cibercriminal en técnicas, tácticas y procedimientos empleados en el ciberespionaje usando herramientas del tipo APT (Advance Persistant Threat) y dirigidas especialmente contra el sector financiero persiguiendo la sustracción de dinero.

- **Herramientas de ataque para dispositivos móviles (principalmente Android)**
  Se estima que en un lapso no superior a cinco años se duplicará el número de amenazas contra dispositivos Android y las vulnerabilidades en los dispositivos móviles, plataformas y aplicaciones. Los datos comprometidos se usarán para otros ataques o para su venta en el mercado negro.

- **Incremento de ataques contra cajeros automáticos y procedimientos de pago**
  Se espera un incremento y evolución de los ataques contra estos

dispositivos, empleando técnicas de ataques persistentes (APT) para, a través de ellos, penetrar en la red de la entidad financiera responsable.

- **Nuevas vulnerabilidades en software y protocolos habituales**
  Como es de esperar, con la permanente evolución en el desarrollo de software basados en protocolos y estándares de comunicación, el desarrollo de nuevas vulnerabilidades continuará siendo algo inherente a toda esta tecnología. Así como hasta hoy vemos como nuevas aplicaciones, softwares y dispositivos nacen con vulnerabilidades a los mercados en donde se comercializan.

- **Ataques contra infraestructuras críticas**
  Muchos Estados estarán preparándose para atacar los sistemas de control industrial SCADA y otros sistemas críticos, como las redes de energía eléctrica. Esto ha quedado demostrado con el desarrollo de malwares como Stuxnet.

- **Ataques contra Linux y OS-X**
  Aumentarán este tipo de ataques, fomentados por el incremento en su uso, la desactivación de determinadas medidas de seguridad por defecto al objeto de permitir la instalación de software pirata y el escaso desarrollo de herramientas de seguridad, dada la imagen de seguridad que tenían. Linux es un sistema operativo de software libre, similar a Unix y OS-X o Mac OS X que es un sistema operativo basado en Unix y desarrollado por Apple Inc. Para dispositivos móviles existe una versión específica llamada iOS.

- **Ataques contra el internet de las cosas**
  El internet de las cosas (IoT, por sus siglas en inglés) se refiere a la interconexión de objetos cotidianos (dispositivos, sistemas y servicios) con internet a través de redes fijas e inalámbricas, permitiendo al usuario un control y manejo de forma remota. La expansión del internet de las cosas llevará consigo un mayor debate sobre los problemas de seguridad y, especialmente, de privacidad derivados de su conexión y contacto cercano permanente con los usuarios. También se conocerán vulnerabilidades de los dispositivos que permitirán la inclusión de código dañino que monitoree la actividad de los usuarios.

Defensa de sistemas informáticos

Los esfuerzos se deben centrar en incrementar las capacidades de prevención, detección, análisis, respuesta y coordinación, unido a una política de investigación y de cambio en la mentalidad. Trabajar como si se estuviera comprometido y por lo tanto proteger los activos fundamentales en un medio comprometido. Entonces algunas de las medidas necesarias serán las siguientes:

1. Incremento de la capacidad de vigilancia: se deben desplegar sistemas que potencien las capacidades de detección e investigación de incidentes en redes y sistemas, facilitando su contención y eliminación. Desplegando sistemas de gestión centralizada de eventos de seguridad y complementar con herramientas capaces de detectar anomalías de manera temprana.

2. Intercambio de información de ciberamenazas: se deben desplegar sistemas que permitan el intercambio automático de reglas de detección e indicadores de compromiso para su integración en los sistemas de defensa.

3. Protección frente a ciberataques de tipo DDoS: mediante la aplicación de configuraciones de seguridad y servicios de filtrado de conexiones.

4. Implantación segura de IPv6: soporte a la migración de la nueva versión del protocolo base de internet.

5. Uso de medidas criptográficas: con la finalidad de otorgar confidencialidad e integridad a la información que se transmita y almacene por las redes y sistemas.

6. Protección y vigilancia de servicios esenciales para la organización: el correo y los servicios web son parte de estos servicios esenciales.

7. Impulso de la I+D+i en ciberseguridad: mantener una constante investigación de los aspectos de seguridad de los productos impulsando los correspondientes procesos de certificación. Desarrollo de nuevos proyectos que mejoren las capacidades de

vigilancia e intercambio de información ágil para su empleo en los sistemas de detección. Innovar para hacer más eficientes los procesos y procedimientos de seguridad.

8. Sensibilización a todos los niveles: es necesario que directivos, empleados, profesionales y ciudadanos sean todos conscientes y responsables de las amenazas y vulnerabilidades en el empleo de las tecnologías de la información.

9. Formación en ciberseguridad: se debe incrementar la formación y certificación de profesionales de ciberseguridad.

10. Adecuación de la legislación: desarrollar periódicamente la normativa legal y apoyar el desarrollo e implantación de una "estrategia de ciberseguridad".

Si nos concentramos en el marco regulatorio y legal, más allá de la existencia o no de decretos y leyes se hace muy notoria la falta de un documento superior del Estado de Chile que canalice y oriente los esfuerzos en proteger los sistemas de información críticos. Es realmente notoria la falta de visión país respecto de la seguridad de los sistemas de información. En una sociedad que se compara permanentemente con las estadísticas y rankings de la OCDE, seguramente en este tema debemos ser uno de los países más distantes del primer nivel internacional. Hoy se necesita a todas luces una Estrategia Nacional de Ciberseguridad que entregue los lineamientos, visión y objetivos en materia de seguridad para sistemas de información en el Estado y con un marcado enfoque de protección de la Infraestructura Crítica (IC), la protección de los datos y la privacidad de las personas.

Entendiendo a la IC como el conjunto de servicios básicos, estructura vial y plataformas de soporte que sustenta el normal funcionamiento y desarrollo de la vida diaria de una sociedad, se debe poner especial atención en proteger sus sistemas de información. Esto porque gran parte de la industria y la IC del país es controlada remotamente por tecnologías de la información, las que si no son protegidas quedan expuestas a ataques perpetrados a través del ciberespacio.

Se han generado instancias de coordinación a nivel internacional que han agrupado a un gran número de países en desarrollo y en vías

de desarrollo. Estas instancias han buscado que los países adopten una política de seguridad tendiente a satisfacer los requerimientos de protección de su IC. Pero unos en mayor o menor medida se han venido quedando relegados por decisión propia o por ignorar la real relevancia de este aspecto en la seguridad del país. Este último parece ser el caso de Chile.

Si bien la seguridad de un Estado tiene como objetivos la protección del territorio y la protección de sus ciudadanos, hoy no se puede obviar la protección de las IC. Así muchos de los países desarrollados han optado por adoptar estrategias o planes de seguridad que abarcan estos tres objetivos, para posteriormente descomponer esa estrategia en planes específicos de protección civil, de protección del territorio (a nivel interno y externo) y de protección de infraestructura y bienes críticos. Entonces, sabiendo la penetración que han tenido las tecnologías de la información en todo ámbito (estatal, industrial, personal, etc…), no es extraño que distintos países hayan desarrollado planes y estrategias específicas tendientes a segurizar el empleo del ciberespacio tanto para sus ciudadanos, su industria y el Estado en sí mismo. A continuación, veremos algunas iniciativas implementadas por algunos países en este sentido.

Estados Unidos es un caso de seguridad mayor, por cuanto a raíz de los hechos del 11 de septiembre del año 2001 creó el "Department of Homeland Security – DHS" [18]. El DHS está encargado, entre otros aspectos, del desarrollo de la legislación relativa a seguridad nacional, la que en aspectos de ciberdefensa ha emitido los siguientes documentos:

- La ley sobre información de Infraestructuras Críticas.

- La directiva de Identificación, Priorización y Protección de Infraestructuras Críticas.

- La directiva sobre la iniciativa de Ciberseguridad Nacional.

- La Estrategia Nacional para la Seguridad del Ciberespacio.

La estrategia de Seguridad Nacional en el Ciberespacio de febrero 2003 asigna la responsabilidad de la protección al DHS y reconoce

que debe ser un esfuerzo coordinado de los gobiernos federal, estatal y local, del sector privado y de los ciudadanos. Establece 5 líneas estratégicas prioritarias a las que asigna responsables y acciones de detalle a realizar para alcanzarlas [19]. Estas son:

- Sistema de respuesta nacional de seguridad en el ciberespacio. Para ello propone diversas acciones, entre las que destacan la mejora de la gestión de incidentes, ampliar el sistema de alerta ante ciberataques, realizar ejercicios de coordinación o mejorar el intercambio de información público-privado.

- Programa de reducción de amenazas y vulnerabilidades. Para ello propone diversas acciones, entre las que destacan, la mejora de las capacidades de las fuerzas de seguridad como el FBI y otras agencias policiales, la mejora del control de los sistemas SCADA o profundizar en el conocimiento sobre amenazas y vulnerabilidades.

- Formación y concienciación en el ciberespacio. Este programa estaba preparado para cinco tipos de audiencias, tales como los ciudadanos y pequeñas empresas, empresas consideradas estratégicas (especialmente las que gestionan infraestructuras críticas), universidades y centros de investigación (especialmente los que dispongan de gran capacidad de cálculo), sector privado (especialmente el que disponga de sistemas SCADA) y gobiernos locales y estatales.

- Asegurar el ciberespacio gubernamental. Las acciones a realizar en el gobierno federal fueron el seguimiento de la evolución de las amenazas y vulnerabilidades y la implementación de las mejoras de seguridad adaptadas a estas, el impulso de la alianza nacional para asegurar la información, la mejora de la seguridad de las redes inalámbricas, la mejora de los requisitos de seguridad en la subcontratación y en las adquisiciones y la mejora en la realización de los procesos de auditoría o inspección. Además, se debe impulsar la seguridad en los gobiernos locales y estatales.

- Cooperación nacional e internacional. Como líneas de actuación destacan el refuerzo de las actividades de contrainteligencia, la mejora de las capacidades de prevención y atribución de un

ataque y la coordinación entre las diferentes agencias. Internacionalmente se intentará mejorar los canales de comunicación y que se adopten en las legislaciones nacionales los acuerdos sobre cibercrimen.

La estrategia de Seguridad Nacional en el Ciberespacio del 2003 asigna responsabilidades que descansan en su mayoría en el DHS y dispone de un completo anexo con las acciones recomendadas para cada línea estratégica. Para el desarrollo de esta estrategia, dentro del DHS, se impulsa el US-CERT [20] que proporciona apoyo en la respuesta ante ciberataques contra la parte civil del gobierno federal (.gov) y tiene la responsabilidad de relacionarse con los gobiernos locales, estatales y la industria. Destaca que el DHS tiene, además, la misión de protección de infraestructuras críticas nacionales definida en el acta del 2002 (Critical Infrastructure Information Act) [21].

En el ámbito del Ministerio de Defensa (DoD) existen muchas iniciativas tanto de las tres fuerzas como de las agencias de inteligencia que tienen misiones en la protección de las redes sensibles y clasificadas como la Agencia de Seguridad Nacional (NSA). Esta agencia tiene un departamento encargado del aseguramiento de la información (NSAIAD [22]) que se focaliza en el análisis permanente de nuevas amenazas y vulnerabilidades, en el desarrollo de guías, productos y soluciones de seguridad, en el desarrollo de productos de encriptación y gestión de claves de los mismos y en la formación y concientización de seguridad. El DoD financia el CERT-CC [23] que tiene como una de sus misiones principales establecer un foro de coordinación entre los CERTs nacionales. Está operado por la Universidad Carnegie Mellon y su misión principal es la relación con otros CERT's (especialmente gubernamentales) para intercambiar información y colaborar ante incidentes de seguridad.

El Reino Unido en su Estrategia Nacional de Seguridad prioriza la protección de las IC del país y especifica que internet es parte de ellas y que puede ser tanto un objetivo como un medio para terroristas, delincuentes o naciones hostiles. El Reino Unido emitió entre otros documentos relacionados, la Estrategia Nacional de Seguridad de la Información y tiene como objetivo asegurar las ventajas de este país en el ciberespacio mediante tres líneas estratégicas:

- Reducción del riesgo del uso del Ciberespacio por el Reino Unido actuando sobre la amenaza (disminuyendo su motivación y capacidad), sobre sus vulnerabilidades y sobre el impacto de cualquier ataque en los intereses nacionales.

- Aprovechar las oportunidades en el ciberespacio mediante la obtención de inteligencia que apoye las políticas nacionales y actúe contra los adversarios.

- Incrementar las actividades de concientización, desarrollar una doctrina sobre el ciberespacio y sus políticas derivadas y mejorar las capacidades humanas y técnicas.

Igualmente, el Reino Unido creó el Centro para la Protección de la Infraestructura Nacional.

Francia, por su parte, publica su estrategia sobre ciberseguridad y la promulga en el Libro Blanco de la Seguridad y Defensa Nacional [24], aprobado por el presidente de la república en junio de 2008, donde se resalta que la ciberamenaza tiene una probabilidad muy alta de que se produzca y su impacto en las infraestructuras críticas y en los sistemas gubernamentales es considerado alto. Este libro blanco contempla cinco funciones estratégicas que las fuerzas de defensa y seguridad francesas deben dominar que son el conocimiento y la previsión (con la necesidad de mejorar las capacidades técnicas de las Agencias de Inteligencia), la prevención (con la necesidad de una defensa proactiva en profundidad que realice una vigilancia permanente), la disuasión, la protección y la respuesta.

Anteriormente a esta estrategia se había desarrollado un plan de mejora de la Seguridad de los Sistemas de Información del Estado. En Francia la Secretaría General de la Seguridad y Defensa Nacional dependiente del Primer Ministro y recientemente reestructurada, es la encargada de tratar todos los asuntos de ciberdefensa y dentro de esta se creó la Autoridad Nacional de Seguridad de los Sistemas de Información (ANSSI) [25] con las siguientes misiones:

- La detección y reacción urgente ante ciberataques mediante la vigilancia continua de las redes gubernamentales sensibles y la implementación de mecanismos de defensa en estas redes.

- El desarrollo de productos y servicios de confianza para su uso en los gobiernos y en los sectores críticos.

- Proporcionar asesorías de seguridad a organismos gubernamentales y operadores de infraestructuras críticas.

- Proporcionar información a empresas y ciudadanos sobre las nuevas amenazas a la seguridad de la información y el procedimiento de protección mediante una política activa de comunicación.

España, sin ser menos, creó el Centro Nacional de Protección de Infraestructuras Críticas. Sus mayores esfuerzos en ciberseguridad han sido canalizados por el Centro Criptológico Nacional para incrementar la seguridad de la información en la administración pública y la participación del Ministerio de Defensa como miembro del centro de excelencia de ciberdefensa cooperativa de la OTAN, que se encuentra en Estonia.

Argentina ya publicó el Programa Nacional de IC de Información y Ciberseguridad, que crea un marco regulatorio que propicia la identificación y protección de las infraestructuras estratégicas y críticas. De igual forma creó el ICIC-CERT (Equipo de Respuesta a Emergencias Computacionales) y normas de seguridad en sistemas y tecnologías informáticas del sector público, entre otras.

La OTAN ha centrado sus esfuerzos de ciberdefensa en las siguientes instancias:

- La creación de un CSIRT, el NATO-CSIRT.

- La Política de Seguridad en Ciberdefensa de la OTAN.

- El documento de acuerdo sobre el concepto de Ciberdefensa de la OTAN.

- La asignación de responsabilidades en ciberdefensa y creación de estructuras organizacionales para la implementación de la Política de Ciberdefensa, por medio de la designación de la Autoridad de Gestión de la Ciberdefensa de la OTAN y la creación del Centro de Excelencia Cooperativa de Ciberdefensa a raíz de los ataques sufridos por Estonia.

A modo de análisis de las estrategias mencionadas podemos concluir que todas realizan una aproximación global al problema tratando de forma conjunta todos los niveles sobre los que se debe actuar en ciberdefensa, estos son en primera instancia los gobiernos centrales, regionales y locales; como segunda instancia las infraestructuras críticas; como tercera instancia las fuerzas y cuerpos de seguridad del Estado y, finalmente, los ciudadanos.

A propósito de una organización del ámbito de la defensa, como es el caso de la OTAN, surge de inmediato la pregunta respecto de ¿cuál es el verdadero estatus de nuestra defensa nacional en aspectos de ciberseguridad?

Sin duda las instituciones de la defensa han desarrollado capacidades de ciberdefensa, pero la respuesta a la pregunta del párrafo anterior es materia de seguridad nacional, razón por la cual en este ensayo no profundizaremos en ella. Sin embargo, no deja de ser llamativo el hecho de que a la fecha no exista una organización conjunta visible entre las FF. AA. del país, que aborde la responsabilidad en los temas de ciberdefensa. Si bien actualmente existe consenso en que el dominio de la guerra se desenvuelve en cuatro campos distintos, siendo estos el terreno (de responsabilidad del Ejército), el mar (de responsabilidad de la Armada), el aire y el espacio (de responsabilidad de la Fuerza Aérea), surge definitivamente un quinto elemento de dominio de la guerra… el ciberespacio.

Entonces, así como hace ya casi un siglo, los servicios aéreos de la Armada y el Ejército se fusionaron y crearon la Fuerza Aérea como una nueva rama de la defensa (en Chile y todo el mundo), tal vez estamos en condiciones de reunir las potencialidades y capacidades de ciberdefensa de las tres instituciones actuales y crear una nueva fuerza cuyo ámbito de acción sea la defensa del ciberespacio para el país… ¿por qué no?

La verdad es que ya existe una figura que aborda esta situación y se concretó en EE.UU., donde por disposición de su actual presidente se creó el Cibercomando cuya misión es velar por los intereses de ese país en la protección directa de sus sistemas informáticos, dar respuesta rápida frente a ataques o incluso ejecutar ataques para proteger sus intereses. Todo esto gatillado por el incidente que hizo públicos un sin número de documentos diplomáticos y militares de ese país (WikiLeaks).

A todas luces vemos países tan cercanos como Argentina y países tan desarrollados como Estados Unidos, ambos formando parte del eje de conciencia en temas de ciberseguridad y la protección de las IC. Entonces surge la pregunta: y… ¿Chile cuándo?

La respuesta es relativamente difícil de abordar. Algunas ideas de las razones se han expuesto en este ensayo, pero mientras nuestras autoridades no tomen conciencia de la verdadera importancia y vulnerabilidades involucradas en nuestra IC, no veremos una Política Nacional de Protección de ellas, ni mucho menos una Estrategia Nacional de Ciberseguridad.

Según el Ministerio del Interior y Seguridad Pública de nuestro país, la Secretaría General de la Presidencia y la Subsecretaría de Telecomunicaciones son los principales organismos nacionales llamados a contribuir en la conformación de la política de cibeseguridad a nivel gubernamental. Aunque el país no ha emitido una estrategia nacional de ciberseguridad, la toma de conciencia entre las instituciones de gobierno es generalizada. Las funciones de la infraestructura gubernamental han actualizado la tecnología de seguridad, y los interesados discuten regularmente acerca de las capacidades y niveles de seguridad de las redes y sistemas de información activos, así como también de las vulnerabilidades que estos han demostrado. El Estado también coordina la planificación de la gestión de crisis y ha puesto en marcha algunas medidas de redundancia.

Las ramas de las Fuerzas Armadas de Chile, comparten información y ciber-responsabilidades de Defensa, pero no tienen una estructura de mando y control central. Uno de los principales desafíos de Chile para el futuro es fortalecer sus capacidades de respuesta a incidentes, las que se podrían abordar a través del CSIRT del Ministerio del Interior, en funcionamiento desde el año 2004, que ofrece para los sitios web de gobierno respuesta a incidentes, pero no ha sido formalmente institucionalizado a nivel nacional para hacer frente a todo tipo de ciberincidentes.

Según la Organización de Estados Americanos (OEA), Chile ha establecido un marco jurídico amplio para hacer frente a la ciberdelincuencia. El Decreto Supremo Nº 1.299 describe las normas y define los roles para el manejo de la ciberdelincuencia, la Ley Nº 19.223 introduce ci-

berdelitos al Código Penal, y la Ley Nº 19.628 abarca la protección de datos y privacidad. A pesar de que el sector privado no está obligado por la ley a revelar incumplimientos, el gobierno trabaja en estrecha colaboración con las empresas para informar y responder a ciberincidentes. Según las autoridades chilenas, phishing, malware y hacking son los tipos más frecuentes de los ciberataques en el país. Las organizaciones policiales como la Brigada del Cibercrimen de la Policía de Investigaciones y el Departamento de Criminología de Carabineros de Chile, llevan a cabo investigaciones y análisis forense digital, respectivamente.

Esas unidades han aclarado numerosos cibercrímenes en los últimos años. Por último, los tribunales tienen una muy relativa capacidad para manejar las pruebas electrónicas. Sin embargo, la mentalidad de ciberseguridad es incoherente en la sociedad chilena. Para sensibilizar a la población, en el 2013 el Ministerio de Educación inició la internet Segura, campaña para educar a los jóvenes sobre la privacidad y el uso seguro de internet. Una campaña para que los ciudadanos tomaran conciencia de los riesgos del comercio electrónico y entendieran sus derechos como consumidores, esta campaña fue titulada como Derechos del Consumidor Digital. La Universidad de Chile ofrece grados avanzados en materia de ciberseguridad, junto a diversos cursos en línea y capacitación para sus empleados. El sector privado, en comparación, se ha vuelto cada vez más consciente de los riesgos de ciberseguridad y ha implementado planes para ocuparse de ellos.

Considerando el ciberespacio como una colección de recursos, los actores implicados (incluyendo Estados, industrias, organizaciones, grupos o individuos) competirán por controlarlo. Esto conduce inevitablemente a conflictos en el ciberespacio. Se puede definir el ciberconflicto como una confrontación entre dos o más partes, donde al menos una parte utiliza los ciberataques contra el otro. La naturaleza del conflicto diferirá de la naturaleza y objetivos de los participantes. Los delincuentes buscarán ingresos ilegales, de modo que secuestran parte del ciberespacio. Los servicios de inteligencia buscan información útil para atacar a sus adversarios del ciberespacio a fin de obtener acceso a esa información. Los militares buscan interrumpir las operaciones del enemigo, por ello atacan sistemas de sensores, logísticos, de comunicaciones y de mando y control en el ciberespacio enemigo. Los conflictos pueden ser tan simples como disputas civiles sobre la propiedad de

un nombre de dominio o más complejos como campañas deliberadas de ciberataques como parte de la guerra convencional entre Estados avanzados tecnológicamente.

Dando por supuesto que los ciberconflictos son inevitables, se pueden establecer varias implicancias desde la variable tiempo de la que depende el ciberespacio. Esta dependencia del tiempo se puede explicar como el cambio en la estructura y contenido del ciberespacio a lo largo del tiempo. El tiempo en el ciberespacio puede ser relativamente corto, minutos a menudo incluso segundos o fracciones de segundo. Basándonos en esto se pueden deducir implicancias como el potencial de los rápidos desarrollos de acciones ofensivas y defensivas, la viabilidad de trazar el mapa del ciberespacio y la necesidad de monitorearlo y reconocerlo constantemente. Los rápidos cambios en el ciberespacio implican que se necesita poco tiempo para realizar un ataque o para implementar nuevas defensas, comparado con el espacio físico. Un gusano de red que se autorreplica puede infectar enormes partes del ciberespacio en cuestión de minutos. Por ejemplo, en 2003 el gusano SQL Slammer infectó aproximadamente el 90% de los computadores vulnerables conectados a internet en unos 10 minutos de un total de 75.000 máquinas en todo el mundo. La única comparación con esto en el espacio físico es el lanzamiento simultáneo de cientos o miles de misiles balísticos armados con cabezas convencionales. Ninguna otra cosa tendría estas consecuencias globales en un intervalo de tiempo similar.

En el lado defensivo, en el ciberespacio es posible mejorar las defensas en segundos o minutos implementando nuevas reglas de cortafuegos, por ejemplo. Construir un nuevo búnker en el espacio físico consume mucho más tiempo. Esto no significa que levantar defensas en el ciberespacio se haga siempre en minutos. Simplemente es posible desplegar medidas defensivas preparadas en menor tiempo (reglas más restrictivas de firewalls, routers, servidores y hosting, etc.).

Al preparar un ciberconflicto es necesario conocer el terreno de la zona potencial de conflicto, las capacidades defensivas y ofensivas de los actores y la posibilidad de daños colaterales y escaladas no planificadas. Por la naturaleza del ciberespacio, es difícil hacer esto, ya que el entorno es complejo y está en constante evolución. Los vectores de entrada potenciales, los objetivos críticos, los usuarios y la información clave

pueden cambiar en segundos. Como resultado, el mapa solo puede ser cercano al tiempo real y no hay forma de asegurar que será el mismo al día planificado del ataque (o defensa). Basándose en esto se puede sacar otra conclusión. Si el mapa está cambiando constantemente, entonces los esfuerzos de monitoreo y reconocimiento deben ser también constantes, de igual manera que se es consciente de la posibilidad de un conflicto en el ciberespacio. Esto significa vigilancia asidua y operaciones encubiertas en el lado defensivo e investigaciones habituales en el lado ofensivo. Sin ello, un ataque puede pasar desapercibido o, en el caso ofensivo, el ataque puede frustrarse por un simple cambio en la posición del objetivo. Esta necesidad de actividad constante, sin embargo, eleva el riesgo de detección por los atacantes y puede delatar los planes y rutinas de los defensores.

Existe una tendencia creciente de cibercampañas que se fijan en los conflictos políticos, económicos o militares en el ciberespacio. El caso de Estonia del 2007 mostró que una nación entera puede verse afectada por ciberataques, mientras que el caso de Georgia del 2008 es un ejemplo de cibercampaña que apunta a un conflicto armado. En ambos casos, al menos parte de los ataques fueron cometidos por hackers patriotas voluntarios que usan los ciberataques para tomar parte en conflictos internos o internacionales. En estos ciberconflictos comúnmente solo los objetivos son conocidos mientras que los agresores permanecen en el anonimato.

A menudo es difícil averiguar dónde termina la capacidad de un Estado y dónde empiezan los grupos de hackers patriotas independientes. Además, es relativamente fácil formar una nueva cibermilicia de personas que tiene poca experiencia con computadores. Se entiende por cibermilicia como un grupo de voluntarios que pueden y son capaces de usar los ciberataques para alcanzar un objetivo político. Una cibermilicia online se define como un grupo donde los miembros se comunican principalmente vía internet y como norma, esconden su identidad. Lo que estos ciberguerreros puedan carecer en formación y recursos, lo suplen con su número de integrantes.

Sin embargo, incluso una cibermilicia ad-hoc que no está bajo control directo de un Estado puede ser una extensión útil del ciberpoder de un Estado. Por otra parte, ellos también pueden convertirse en una amenaza a la seguridad nacional. Debido a la naturaleza global de in-

ternet, esta amenaza proviene probablemente de múltiples jurisdicciones, lo que limita la aplicación de la ley o las opciones defensivas del Estado. Por tanto, ambos enfoques deberían ser considerados.

Conclusiones Finales

- El empleo del ciberespacio es transversal al Estado (incluida la defensa), los privados y ciudadanos y es utilizado por la Infraestructura Crítica para su operación.

- Las amenazas son difíciles de dimensionar, muy tecnológicas y acompañadas de explosiones sociales gatilladas por eventos mediáticos. Por tal razón se requiere un monitoreo centralizado permanente de las redes nacionales.

- Nos enfrentamos a nuevos escenarios para el delito, el terrorismo y la guerra, lo que exige la creación de nuevas herramientas de prevención, reacción y defensa. Para consolidar una capacidad suficiente de ciberseguridad y ciberdefensa, es necesaria una Estrategia Nacional de Ciberseguridad.

- Los desafíos son definir una autoridad central de ciberseguridad, mejorar el marco regulatorio legal, mejorar la infraestructura de ciberseguridad, la capacitación, el monitoreo y la cooperación a nivel nacional e internacional.

REFERENCIAS

[1] El Proyecto OPTE. www.opte.org/

[2] SEGURINFO. Congreso y feria interamericana de seguridad de la información. www.segurinfo.org/

[3] Patrick Traynor, William Enck, Patrick McDaniel, and Thomas F. La Porta. Mitigating attacks on open functionality in sms-capable cellular networks. In MOBICOM, 2006.

[4] Lei Liu, Guanhua Yan, Xinwen Zhang, and Songqing Chen. Virusmeter: Preventing your cellphone from spies. In Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection, RAID '09, Berlin, Heidelberg, 2009. Springer-Verlag.

[5] M. Lesk. The new front line: Estonia under cyberassault. Security Privacy, IEEE, 2007.

[6] John Markoff. Before the gunfire, cyberattacks, Aug. 2008 www.nytimes.com/2008/08/13/technology/13cyber.html?em

[7] Georgios Loukas and Glay ke. Protection against denial of service attacks: A survey. The Computer Journal, 2009.

[8] CERT CC. Code Red II. www.cert.org/incidentnotes/IN–2001–09.html.

[9] Anonymous wikileaks supporters explain web attacks, Dec. 2010. www.bbc.co.uk/news/technology-11971259

[10] Directive on the identification and designation of european critical infrastructure and the assessment of the need to improve their protection. In Commission of the European Communities, Brussels, Belgium, May 2008.

[11] Communication from the commission on a european programme for critical infrastructure protection. In Commission of the European Communities, Brussels, December 2006.

[12] Integrated Risk Reduction of Information-based Infrastructure Systems. In IRRIIS project, Deliverable D 1.2.1" Scenario analysis", Jun 2006. www.irriis.org/File.aspx?lang=2\&oiid=8661\&pid=572.

[13] Sophos Facebook ID Probe. 2008. http://www.sophos.com/pressoffice/news/ articles/2007/08/facebook.html

[14] Open Web Application Security Project (OWASP). www.owasp.org/index.php/Main_Page

[15] Sanger, D. (2012). Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. USA.

[16] International Atomic Agency (2012). IAEA & IRAN. www.iaea.org/newscenter/focus/iaeairan/index.shtml

[17] Guerra Electrónica. Pedro Jarpa Martínez. Colección Academia Politécnica Militar del Ejército de Chile, ACAPOMIL, 2013.

[18] Department of Homeland Security (DHS). www.dhs.gov.

[19] The National Strategy to Secure Cyberspace. White House. www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

[20] US-CERT. http://www.us-cert.gov/

[21] Critical Infrastructure Information Act of 2002. www.dhs.gov/xlibrary/assets/CCI_Act.pdf

[22] National Security Agency. Information Assurance Directorate (IAD). www.iad.gov

[23] CERT-CC. Centro de coordinación de CERT. De la Universidad Carnegie Mellon. www.cert.org

[24] Livre blanc sur la défense et la sécurité nationale. www.livreblancdefenseetsecurite.gouv.fr/information

[25] Agence nationale de la sécurité des systèmes d'information (ANSSI). www.ssi.gouv.fr

[26] Entidad Acreditadora – Ministerio de Economía Fomento y Turismo. www.entidadacreditadora.gob.cl/norma-chilena-oficial-nch-iso-27002-of2009/