CARRERA DE TECNICATURA EN DESARROLLO DE APLICACIONES WEB

MATERIA: Tecnología de Redes

“Elementos de Ciberguerra en Redes WAN de alta seguridad”

**Líder de Proyecto:**

Mauro Gabriel Ledesma

40391692

**Integrantes:**

Sergio Fabian Balanda 31732808

Mauro Gabriel Ledesma 40391692

Nicolás Sierra 28642247

Nicolás Orlando 31656029

Hernán Protto 36819223

**Título**

**Escenario de la Ciberguerra.**

En este texto se analiza el escenario conflictivo de la ciberguerra, que, aparecido recientemente con la llegada de las tecnologías de la información, que hoy en día están presentes en todos los ámbitos del mundo moderno y cada vez con más frecuencia.

Se definen los conceptos básicos para luego continuar con la situación, casos de análisis, conflicto, metodologías y ataques, Ciberdefensa, y capacidad de defensa.

**Objetivo del Trabajo:**

Analizar el creciente escenario conflictivo de la ciberguerra. La ciberguerra como nuevo campo de batalla, los ataques, y las contramedidas.

Contenido

[**1-Introducción y conceptos básicos 4**](#_gjdgxs)

*Responsable Balanda, Sergio Fabian.*

[1.1 Conceptos básicos 4](#_30j0zll)

[1.2 Definiciones. 7](#_1fob9te)

[1.3 Amenaza, impacto, implicaciones. 9](#_3znysh7)

[**2-Situacion, casos de análisis, escenario de conflicto 12**](#_2et92p0)

*Responsable: Orlando, Nicolás.*

[2.1 Contexto geopolítico, principales actores y hechos destacados: 12](#_tyjcwt)

[2.2 Los cinco escenarios de ciberguerra: 13](#_3dy6vkm)

[2.3 La lucha por el control de Internet 19](#_1t3h5sf)

[2.4 Casos 21](#_4d34og8)

[**3-Metodologías y ataques. 24**](#_17dp8vu)

*Responsable: Ledesma, Mauro Gabriel.*

[3.1 Conceptos y Metodologías Principales. 24](#_3rdcrjn)

[3.2 Ataques. 26](#_26in1rg)

[3.4 Ciberataques Globales. 29](#_lnxbz9)

[**4-Defensa, Ciberdefensa y capacidad de respuesta 30**](#_35nkun2)

*Responsable: Sierra, Nicolás.*

[4.1 Técnicas de Ciberdefensa. 30](#_1ksv4uv)

[4.2 La mejor defensa es el ataque – Defensa Legal. 31](#_44sinio)

[4.3 Situación en Argentina. 39](#_2jxsxqh)

[**5-Concluciones 40**](#_z337ya)

*Responsable: Protto, Hernán.*

1-Introducción y conceptos básicos

*1.1 Conceptos básicos*

A través de la historia las nuevas tecnologías han revolucionado la guerra, a veces abruptamente, a veces sólo gradualmente; pensemos en el combate, en la pólvora, el avión, el radar o la fusión nuclear. Igual que ha sucedido con las Tecnologías de la Información. Las computadoras e Internet han transformado la economía y han dado grandes ventajas a los ejércitos occidentales tales como la capacidad de enviar aviones controlados remotamente para capturar inteligencia o atacar a objetivos. Sin embargo, la expansión de la tecnología digital tiene sus riesgos al exponer a los ejércitos y a la sociedad a los ciberataques (ataques digitales). La amenaza es compleja, en múltiples aspectos y potencialmente muy peligrosa. Al igual que ha sucedido con el control de las armas convencionales y nucleares, los países deben comenzar a pensar en el modo de reducir las amenazas de la ciberguerra con el objetivo de intentar evitar los ataques antes de que sea demasiado tarde o afrontarlas con éxito si se realizan.

En el mundo surge una nueva dimensión con el llamado ciberespacio. Es un nuevo campo de batalla en el siglo XXI, sin fronteras y asimétrico. Así surgen nuevos términos con el prefijo ciber.

*Palabras clave: Seguridad, ciberespacio, tecnologías, información, comunicaciones, amenaza, estrategia, ataques, redes, internet, ciberseguridad, ciberdelincuencia, ciberataque, ciberdefensa, ciberterrorismo, ciberarma, vulnerabilidad, infraestructura crítica.*

Los conceptos de seguridad nacional y ciberespacio son de uso generalizado por parte de amplios sectores de nuestra sociedad. La palabra seguridad se puede aplicar a muchos ámbitos. Así se habla de seguridad física, seguridad vial, seguridad ciudadana, seguridad jurídica, seguridad económica, seguridad energética, seguridad financiera, seguridad de las tecnologías de la información, etc., cuya gestión es la responsabilidad de diferentes ministerios, sin embargo, en este contexto, la seguridad nacional es aquella encargada de proteger los intereses nacionales.

Tradicionalmente la seguridad nacional se ha concebido como el elemento garante de la identidad y supervivencia nacionales o, dicho de otra forma, de su independencia e integridad. No obstante, este concepto se ha ido ampliando incluyendo actualmente un mayor número de riesgos, entre los que figuran, por ejemplo, los desastres naturales, el cambio climático, las tecnologías de la información y las comunicaciones. Todo ello según la apreciación de su dimensión por la población.

En el mundo actual ha surgido una nueva dimensión donde pueden materializarse las amenazas: el ciberespacio. Dentro de la comunidad TIC (Tecnologías de la Información y Comunicaciones) el ciberespacio se refiere al conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos. El ciberespacio puede también puede definirse como un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con estos sistemas.

Otra posible definición de ciberespacio es: un ámbito caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura física asociada. El ciberespacio se puede considerar como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física.

Muy frecuentemente se identifica Internet con ciberespacio, aunque, el ciberespacio es un concepto mucho más amplio. Por tanto, resulta más adecuado referirse, por ejemplo, al ciberterrorismo con expresiones como terrorismo por medios informáticos, teleterrorismo o terrorismo digital. Sin embargo, la utilización de expresiones como ciberdelincuencia o ciberterrorismo como sinónimas, en el primer caso de delincuencia vía internet o en el caso de la segunda, de terrorismo a través de la red, han generado en el colectivo la identificación de ciberespacio e Internet como ese mismo lugar intangible al que anteriormente se hacía mención.

La principal característica que ha contribuido al desarrollo y a la dependencia del ciberespacio es el tratamiento de la información. En la llamada sociedad de la información o ciber sociedad, la premisa es que la información por sí misma tiene un valor susceptible de generar poder (político, económico, social, etc.). Cuanto mayor sea la eficacia con que sea manejada y tratada aquélla, mayores serán los beneficios.

El ciberespacio ha experimentado un enorme y veloz desarrollo, así como la

dependencia que nuestra sociedad tiene de él, lo que contrasta con el menor y lento avance en materias de ciberseguridad. Por este motivo, los actores (tanto estatales como no estatales) que decidan operar en el ciberespacio, obtendrán una serie de ventajas asimétricas, como:

• El ciberespacio es un campo de batalla de grandes dimensiones y donde resulta relativamente fácil asegurar el anonimato. Los ataques se pueden lanzar desde casi cualquier parte del mundo.

• Los efectos de los ataques son desproporcionados con respecto a su coste. Las operaciones se pueden realizar sin necesidad de efectuar fuertes inversiones en recursos humanos y materiales.

• La naturaleza de los ciberataques fuerza a la mayoría de las víctimas, tanto reales como potenciales, a adoptar una actitud defensiva.

• Esta amenaza tiene un alcance global, en la cual el actor (ya sea ciberdelincuente, ciberterrorista, etc.), puede operar desde cualquier parte del mundo con el único requisito de tener acceso al ciberespacio. La conexión al ciberespacio de cualquier sistema lo convierte en un objetivo susceptible de ser atacado.

• Proporciona las herramientas necesarias para que los más pequeños puedan enfrentarse, incluso vencer y mostrarse superiores a los más grandes, con unos riesgos mínimos para ellos.

Por tanto, al movernos en la sociedad de la información o también llamada cibersociedad, surgen nuevos términos con el prefijo ciber para denominar eventos que se producen en el ciberespacio. De ahí surgen los términos: ciber entorno, ciberactivismo, ciberdelincuencia, ciberterrorismo, ciber amenaza, ciberguerra, ciber rebelión, ciber ejército, ciberarma, etc.

Nos enfrentamos a un nuevo campo de batalla dentro de la seguridad que es el ciberespacio, donde se producen comportamientos o fenómenos ya conocidos, pero empleando técnicas nuevas; y también fenómenos nuevos que surgen de la propia idiosincrasia del ciberespacio y en donde, en ocasiones, no están claras las fronteras entre activismo y delincuencia.

El ciberespacio no tiene fronteras, es un nuevo campo de batalla del siglo XXI, aunque ya se intuyó a finales del siglo XX. El campo de batalla o teatro de operaciones es el ciberespacio, los atacantes son los hackers que utilizan un armamento no siempre sofisticado que es el código dañino.

1.2 Definiciones.

En los últimos años el término ciber se ha usado para describir casi todo lo que tiene que ver con ordenadores y redes y especialmente en el campo de la seguridad. Un campo de estudio emergente está mirando a los conflictos en el ciberespacio, incluyendo las ciberguerras entre estados, el ciberterrorismo, los ciber ejércitos, etc. Desafortunadamente, sin embargo, no existe un consenso sobre qué es el ciberespacio, por no decir de las implicaciones de los conflictos en 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 ciber entorno y ciberseguridad. El ciber entorno 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. 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 ciber entorno. 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 ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber entorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y la confidencialidad.

Un delito informático o ciberdelincuencia, es toda aquella acción ilegal que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet. Muchos de estos delitos, se definen como abusos informáticos.

La criminalidad informática o cibercrimen tiene un alcance mayor, donde se incluyen delitos como el fraude, el robo, el chantaje, la falsificación y la malversación de caudales publico utilizando ordenadores y redes como medio para realizarlos.

Básicamente el ciberterrorismo podría definirse como:

El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos.

También el ciberterrorismo, es denominado terrorismo electrónico, podemos definirlo como la forma de terrorismo que utiliza las tecnologías de información para intimidar, coaccionar o para causar daños a grupos sociales, con objeto de lograr una serie de fines políticos o religiosos.

Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra propiedad privada, o al menos causar el daño suficiente como para generar miedo. Como ejemplo de ataques serían los que provocan muertos o heridos, así como los ataques lanzados contra las infraestructuras críticas de un país, dependiendo de su impacto.

Por el contrario, ataques que irrumpen servicios no esenciales o que causan una molestia costosa, no se catalogan como ciberterrorismo.

La ciberguerra o guerra informática es aquel conflicto bélico que utiliza como campo de operaciones, en vez de los campos de batalla convencionales, el ciberespacio y las tecnologías de la información y como armas las aplicaciones, comandos y herramientas diversas que proporcionan la informática y las telecomunicaciones. Los objetivos más comunes son la inhabilitación de los sistemas informáticos del enemigo o la obtención de información.

Estos actos tanto los incluidos en el cibercrimen, en la ciberguerra o en el ciberterrorismo se denominan ciberataques.

Dependiendo de la meta que se desee alcanzar o el daño que se desee provocar, veremos que los ciberataques pueden presentarse de diferentes maneras. Para alcanzar sus objetivos, el ciberdelincuente utiliza una serie de técnicas básicas, las cuales se aplican individualmente o de forma combinada. Algunas de ellas son:

Los virus informáticos, el envío masivo de correo no deseado o spam, suplantación de remitentes de mensajes mediante spoofing, él envió o instalación de archivos espías o keyloggers, uso de troyanos para el control remoto de los sistemas o la sustracción de la información, archivo BOT del IRC (Internet Relay Chat), uso de rootkits, cambios en las direcciones de dominio (DNS), instrucciones no autorizadas, DDoS (denegación de servicio), interferencia electrónica de comunicaciones, BlindRadars bloqueo de tráfico aéreo, robo de información, anulación de equipos, etc.

Con el termino ingeniería social se define el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces predeterminada para la obtención de información para el acceso no autorizado a sistemas informáticos.

No existe una limitación en cuanto al tipo de información y tampoco en la utilización posterior de la información obtenida. Puede ser ingeniería social el obtener de un profesor las preguntas de un examen o la clave de acceso de la caja fuerte de un banco. Sim embargo, el origen del termino tiene que ver con las actividades de obtención de información de tipo técnico utilizadas por hackers (claves de acceso, password, IPs, tipos de sistemas, sistemas de seguridad, etc.).

Un hecho importante es que el acto de ingeniería social acaba en el momento en que se ha conseguido la información buscada. Las acciones que esa información pueda facilitar o favorecer no se enmarcan bajo este término.

1.3 Amenaza, impacto, implicaciones.

Considerando el ciberespacio como un espacio o una colección de recursos, los actores implicados (incluyendo Estados, negocios, organizaciones, grupos o individuos) competirán por controlarlo. Esto conduce inevitablemente a conflictos en el ciberespacio. Se puede definir el ciber conflicto 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 partes enemigas, amistosas o neutrales del ciberespacio para obtener acceso a esa información. Los militares buscan interrumpir las operaciones del enemigo, por ello atacan sistemas de sensores, logísticos, de comunicaciones 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 ciber conflictos son inevitables, se pueden establecer varias implicaciones desde el variable tiempo de la que depende el ciberespacio. Esta dependencia del tiempo se puede explicar cómo 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. Basándose en esto, se pueden deducir implicaciones como el potencial de los rápidos desarrollos de acciones ofensivas y defensivas, la viabilidad de trazar el mapa del ciberespacio y la necesidad de patrullarlo y reconocerlo constantemente. Los cambios rápidos 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 auto-replica puede infectar enormes partes del ciberespacio en cuestión de minutos. Por ejemplo, en 2003 el gusano SQL Slammer infectó aproximadamente el 90% de los ordenadores 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 unas 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 señala que es posible desplegar medidas defensivas preparadas (reglas más restrictivas de cortafuegos, enrutado y alojamiento alternativo, etc.) en menor tiempo. Al preparar un ciber conflicto 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 cambio. Los vectores de entrada potenciales, los objetivos críticos, los usuarios y la información clave pueden cambiar en segundos. Como resultado el mapa sólo puede ser cercano al tiempo real y no hay forma de asegurar que será el mismo el día planificado de ataque (o defensa). Basándose en esto se puede sacar otra implicación. Si el mapa está cambiando constantemente, entonces los esfuerzos de patrulla 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 con trampa 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.

Hoy día y los próximos años, nos encontramos con la implantación creciente del Internet móvil y la consiguiente proliferación de dispositivos móviles (acceso mediante todo tipo de dispositivos, teléfonos inteligentes, tabletas, libros electrónicos, microordenadores netbooks, ordenadores think (con poca memoria y capacidad de proceso conectados a La Nube) videoconsolas, acceso desde todo tipo de medios de comunicación, automóviles, trenes, aviones, autobuses, barcos, …), de las tecnologías cloud computing, la virtualización, o el avance imparable de las redes sociales y de los restantes medios sociales como blogs, wikis, mashups (de modo autónomo o

integrados en redes sociales). Todo esto unido a la difusión también cada día mayor de las nuevas tecnologías en torno a la Geolocalización, Realidad Aumentada, la Web en tiempo real o el Internet de las cosas (acceso a la Red mediante todo tipo de cosas, sensores, electrodomésticos, herramientas tecnológicas, etc.) están configurando grandes cambios sociales que afectarán significativamente a la capacidad de los departamentos de TI para mantener la seguridad de la Red.

Si nos centramos en las organizaciones y empresas, la imagen clásica del puesto de trabajo está variando completamente. Los trabajadores escriben en los ordenadores portátiles que se llevan a casa, escriben, ver la prensa o consultan sitios relacionados con el trabajo en los teléfonos móviles, realizan llamadas privadas y profesionales desde los mismos dispositivos.

Los cibercriminales están aprovechándose de las innovaciones tecnológicas para agilizar sus propias operaciones delictivas; por ejemplo, el uso creciente de las redes sociales y como los terroristas se están sumando a dichas redes sociales que se han convertido en terreno de juego para los cibercriminales con un creciente número de ataques.

En cuanto al de las amenazas, la ingeniería social y la mezcla de tecnologías por parte de los usuarios son cada vez más peligrosas para la ciberseguridad. Está cada vez más al alza los ataques multivector que combinan diferentes soportes (correo-e, web, voz, vídeo.) para encontrar fisuras. Los cibercriminales y, por ende, los ciberterrorista siguen atacando sitios web legítimos de forma planificada, a la vez que gestionan ataques de spam controlados (ataques multivectoriales) preparados para actuar en un momento concreto y enfocados en establecer keyloggers (programas capturadores de teclado), bots y puertas traseras. Todo esto hace que la situación actual, con las nuevas tecnologías e internet sean un campo de operaciones magnifico para la ciberguerra.

2-Situacion, casos de análisis, escenario de conflicto

2.1 Contexto geopolítico, principales actores y hechos destacados:



**Rusia y EEUU**

La política agresiva de Rusia en contra de la ONU genera una constante tensión nuclear con EEUU y Rusia.

El estado ruso ha estado tomando acciones que perjudican los intereses de EE. UU y sus aliados de la OTAN en el báltico (Letonia y Estonia). Vladimir Putin ha manifestado que no va a dudar en usar la fuerza militar si cree que la seguridad de Rusia puede ser atacada.

Por su parte el presidente Barack Obama ha sancionado a Rusia por ciberataques para influir en las elecciones presidenciales a favor de Donald Trump.

**Corea del Norte**

Corea del norte y sus reiteradas demostraciones de fuerza han sido vistas por el mundo occidental como una provocación. Pruebas nucleares y lanzamientos de misiles balísticos han demostrado capacidad de miniaturizar una ojiva en un misil balístico.

Por su parte Corea del sur Japón y demás aliados de EE.UU. en el Pacífico concordaron nuevos tratados defensa con escudos antimisiles en la región.

Corea del Norte ha sido acusada en los últimos años de realizar diversos ataques cibernéticos, mayormente contra redes financieras en EE.UU., Corea de Sur u otros países.

Estado Islámico

La mayor preocupación del mundo occidental son los recientes ataques terroristas en Europa y la posibilidad de este grupo de hacerse con un arma nuclear, ya que han demostrado tener recursos financieros, materiales y logísticos en mayor proporción que cualquier otro grupo terrorista en la historia.

Se han adjudicado el ciberataque contra bases de datos de militares en EEUU.

**Europa**

Europa se encuentra amenazada por las tensiones internas tras el Brexit y ataques terroristas recurrentes.

En cuanto a ciberataques, recientemente en Reino Unido se atacaron los servicios del NHS que paralizó 16 hospitales en todo el país.

2.2 Los cinco escenarios de ciberguerra:

**1. EEUU y China.**

La curiosa relación entre China y los Estados Unidos, les ha llevado a una constante tensión que ni puede ser declarada abiertamente ni se manifiesta más allá de esa guerra oculta que se libra en las redes. Mientras tanto, lugares públicos como el "Foro de la Industria de Internet China y Estados Unidos", acogen calurosas declaraciones de intenciones en las que la colaboración contra el crimen y el espionaje son la clave.

Casos como el de Huawei, acusado el año pasado de mantener abiertas puertas traseras en sus Reuters que permitirían un eventual espionaje y acceso a sus infraestructuras por parte del país de origen de estos dispositivos, desató una polémica comercial que pasaría a primer plano informativo al formalizarse la queja por parte de la embajada China a propósito de la campaña contra una de sus mayores empresas tecnológicas.

Según un informe de Akamai, China supuso a lo largo del último trimestre de 2012 un 41% del tráfico global de los ataques de denegación de servicio (DDoS). EEUU representó el 10% de estos. El crecimiento de estos ataques y la multiplicación de sus orígenes hacen que las estrategias de seguridad de empresas no directamente vinculadas a la red, como bancos y medios de comunicación, queden expuestas. La escalada en la complejidad evidencia cada vez más que sin un claro patrocinio y el respaldo de una infraestructura cada vez mayor no es posible llegar a la escala actual que adquieren estos ataques.

En 2009, se produciría el ataque conocido como Aurora, que tendría como principal objetivo un Google que se negaba por aquel entonces a aplicar las cláusulas de censura que el Gobierno chino pretendía imponer al buscador. Las cesiones parciales a la censura no serían suficientes para Pekín. Finalmente, Google decidiría abandonar China, que desde entonces elevaría a Baidu como la gran opción de un internet debidamente fiscalizado por las autoridades.

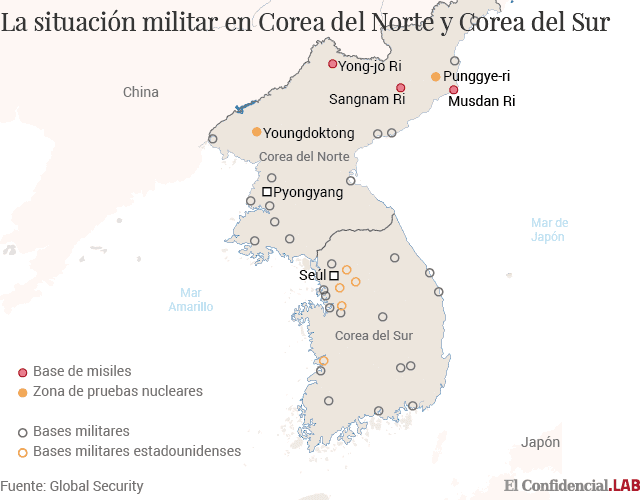
Otro momento comprometido para las autoridades chinas sería la filtración en un documental de corte propagandístico en el que se mostraba la interfaz de un software de ataque que solicitaba una dirección IP desde la que encubrir el origen real de este. En el fotograma, se empleaba la dirección de la Universidad de Alabama, lo que dejaba en mala posición un reportaje que pretendía mostrar a China como víctima.

Esclarecedor ejemplo ha sido también el nuevo centro de operaciones ubicado en Shangai, que se ha revelado como una de las fuentes de buen número de intervenciones en la red. Si bien ha sido complicado revelar la procedencia de estos ataques, dado que la mayor parte empelan como plataforma la multitud de equipos zombies (operados remotamente por un software de control remoto) que operan como una BotNet (red de ordenadores infestados), finalmente el origen apunta a este centro de operaciones.

La sombra de los ciberataques procedentes de China parece siempre seguir unos parámetros que difícilmente podrían apuntar a hackers individuales. Así los sucesivos ataques a empresas, prensa y organismo gubernamentales como la NASA, no dejan de apuntar, aunque si pruebas concluyentes, hacia miembros apoyados por el propio gobierno. La contraparte es aún más oscura. China, apenas reporta casos en los que su seguridad haya sido comprometida, a pesar de la constancia de que no dejan de sucederse casos en ambas direcciones. Así, el ministerio de Defensa chino y otros sitios militares han llegado a contabilizar mensualmente un promedio de 144.000 a lo largo de 2012, de cuyo origen parece que un 62,9% partía de EEUU según una de las pocas informaciones suministradas.

Ciertamente, las informaciones que se deslizan en los medios apuntan a un espionaje organizado y constante por parte de EEUU. La revelación de todo un arsenal de nuevas armas secretas chinas, directamente recogido en informes públicos del Pentágono, no deja lugar a dudas del espionaje que este mantiene. La exactitud de los datos acerca de armas como misiles balísticos orbitales, cazas y sobre todo nuevas herramientas orientadas al ciberespionaje revelan una actividad importante en este sentido.

**2. Guerra cibernética contra "Estados enemigos” como Irán o Corea del Norte**

Irán, pasando por Siria en su camino, se ha convertido para EEUU e Israel en el próximo objetivo geoestratégico. La aparición de Stuxnet y la intrusión informática en la planta de enriquecimiento de uranio iraní de Natanz en 2010, ha sido uno de los momentos más señalados de todo este proceso. No se trata solamente de que se haya podido acceder desde el exterior al corazón de los sistemas de control de unas instalaciones críticas, sino que el método planteaba una novedad inquietante. Así Stuxnet abría el camino a toda una nueva generación de virus espía capaz de actuar de forma casi autónoma y con un potencial aterrador.

No sería hasta bastante después, cuando el propio Gobierno estadounidense confirmara la existencia de un arsenal informático preparado para eventuales ataques preventivos, cuando sabríamos que se confirmaba, de forma tácita, que Stuxnet formaba parte de dicha infraestructura. Posteriormente conoceríamos que sería concretamente parte de una colaboración entre EEUU e Israel. Tanto Stuxnet como Duqu, siguen un mismo patrón. El peligro de ambos es la casi independencia con la que estas armas cibernéticas operan. Una eventual "mutación" o una deriva inesperada podría hacerlas operar a una escala no prevista o incluso volverlas contra sus creadores, como tantas obras de ciencia ficción nos han adelantado.

Por su parte, Hezbollah también ha comenzado a crear una estructura desde la que realizar incursiones en el ciberespacio. El frente abierto contra Israel, nos ha ofrecido otro capítulo curioso. De forma independiente operaciones de miembros de Anonymous han confluido en ataques a infraestructuras informáticas expuestas sobre todo tras los últimos episodios contra palestina por parte del estado hebreo. En este contexto, deberemos estar atentos a cómo se desenvuelve la llamada OpUSA. Entre las acusaciones más destacadas, la de volver a entrenar y equipar a yihadistas contra el gobierno sirio.

El escenario del conflicto sirio también ha aportado sus particulares operaciones como la llevada adelante por la Syrian Electronic Army, que se atribuye los ataques de esta semana pasada a medios occidentales, como la BBC, France 24 TV, diversas radios públicas estadounidenses, Al-Jazeera, el Gobierno de Qatar y diversas cuentas de Twitter desde las que se difundirían informaciones falsas que llevarían a la caída de 145 puntos al índice Down Jones. Parece que en este sentido Siria puede ser el prólogo de una intervención contra su socio iraní.

Mientras, Corea de Norte y sus supuestas instalaciones nucleares se han convertido en otro de los objetivos prioritarios tanto de su vecino del sur como de EEUU. La reciente entrada de hackers en las redes norcoreanas, aisladas del resto de internet, ha sido posible gracias a un despliegue de antenas Wifi amplificadas que pudieron captar la señal y establecer un punto de entrada desde lugares próximos a la frontera. La intrusión terminaría por afectar a diversas infraestructuras, aunque no alcanzara a ordenadores con información acerca del programa nuclear. Tal infraestructura difícilmente pasaría desapercibida en una de las fronteras más vigiladas del mundo. La reacción del norte fue cortar la línea de enlace existente desde 2006 para evitar confusiones militares y enfrentamientos fronterizos y declarar nulos los términos del armisticio entre ambos coreas.

En paralelo a las amenazas y bravatas norcoreanas, EEUU y Corea del Sur establecen las bases para colaborar en un eventual escenario de conflicto en la red. Esto se traduce en que el pretexto del ataque por parte de hackers se sostiene con dificultades y las próximas intrusiones en el sistema del norte serán ya confirmadas sin excusa, como métodos de "defensa".

Por otro lado, parece que los ataques "de vuelta" pueden tener su origen en la propia China, aunque Corea del Sur se guarda bien las espaldas y acusa a sus compatriotas del norte de las recientes infecciones que afectaron a bancos, ordenadores personales y canales de televisión.

Por su parte, los EEUU han descrito entre sus prioridades estratégicas la intrusión en las redes que controlen el programa militar de Corea del Norte. La información pública que se conoce al respecto, advierte que podrían estar en disposición de manejar una variedad de herramientas de ataque que, aunque no de la sofisticación del gusano israeloestadounidense Stuxnet podrán comenzar a comprometer sectores estratégicos en poco tiempo.

**3. Rusia, la ciberdelincuencia y el espionaje**

El caso más famoso de ataque de supuestos hackers a una nación fue el de 2007 a Estonia. Por aquel entonces, el país báltico era una de las naciones de mayor penetración digital de occidente. Diversos sistemas fundamentales, entre los que destacaban el sistema bancario y las infraestructuras públicas, desde saneamiento hasta los mismos semáforos, fueron bloqueados durante cerca de dos semanas a consecuencia de la retirada de un monumento identitario para la población rusa que habita el país. Expertos de la OTAN tendrían que acudir para tratar de hacer cesar dicho ataque cuyo origen se ubicaría finalmente en la Federación Rusa.

Ninguno de estos ataques "políticos" ha sido en ningún caso reconocido, como viene siendo pauta habitual, por autoridad alguna. Las especulaciones posteriores apuntarían a una suerte de "encargo" a hackers con capacidades de movilizar enormes Botnets para llevar adelante estos.

La afirmación que el negocio ilícito es el modelo de empresa capitalista más perfecto podemos trasladarla al ámbito de la red. El empresario delictivo busca un nicho de mercado y lo explota de la mejor forma posible. Para ello, la red se ha convertido en un nuevo lugar donde poder difundir su mercancía mejor.

En el caso ruso también parece ser más cierto que en ningún otro que existen múltiples operadores independientes que se dedican al delito informático sin relación con el Estado. Informes como es de Russian Underground 101, a cargo de Max Goncharov, detalla todas las actividades ilícitas que se realizan en la red y los precios a los que estos cibercriminales profesionales, prestan sus servicios en el mercado negro del hacking ilícito, en foros como antichat.ru, xeka.ru y cardingcc.com.

Grandes estructuras de ciberespionaje como la recientemente desvelada "Octubre Rojo" apunta a nuevas formas de espionaje netamente delictivo con origen ruso. La sofisticación de este software espía es muy grande. Con un periodo de operación de más de cinco años, este software utiliza distintos módulos independientes, con pautas similares al malware Flame, capaz de replicarse de forma oculta y descifrar códigos como ACID, desarrollado por el Ejército francés y que emplea la OTAN y la Unión Europea.

**4. Anonymous y el Hacktivismo**

Las sucesivas detenciones de diversos individuos que se atribuyen a redes de Anonymous o miembros de LulzSec apenas han conseguido poner freno a las constantes campañas que estos colectivos agrupados bajo un nombre común realizan.

Desde sus primeras operaciones surgidas de 4Chan contra emisoras racistas o la Cienciología, El colectivo Anonymous ha evolucionado hacia una mayor concienciación de su papel como activista por los derechos en Internet. Su apoyo a Wikileaks, en la llamada Operación PayBack, con las primeras acciones contra su bloqueo financiero, los llevarían a saltar definitivamente al primer plano informativo. También aumentarían su base de simpatizantes agregando un perfil mucho más activista y comprometido.

Desde entonces las operaciones de grupos de Anonymous irían incrementándose, sobre todo contra países con censura, organismos, políticos e incluso empresas. Ni siquiera la pederastia quedaría fuera de los ataques del grupo, que realizaría un masivo bloqueo al servidor de la red oculta que más páginas de este tipo empleaba.

El grupo LulzSec, impulsaría un ataque contra la compañía Sony que culminaría con la caída de PlayStation Network y la revelación de buena parte de nombres y claves de usuarios de sus clientes, como consecuencia de la denuncia de Sony contra George Hotz, creador del Jailbreak para iPhone que luego realizaría igualmente para la PlayStation 3. Los cambios de la política de uso de su consola y las restricciones que trataban de imponer a su este volverían a tener consecuencias para esta con sucesivos ataques que culminarían con la apertura final de esta a ser "pirateada" y la consiguiente puesta a disposición de juegos para su descarga.

La legislación que pretendía limitar la piratería y de paso buena parte de las libertades ciudadanas en la red, denominada SOPA, agruparía a buena parte del sector tecnológico. Acompañando a la línea cívica, que finamente conseguiría tumbar la ley, las operaciones de Anonymous tomarían el nombre de Operación BlackOut y pasarían por ataques a empresas y organismo gubernamentales que apoyaran dicha legislación.

**5. Una difusa guerra contra el terrorismo**

Podemos afirmar que el yihadismo internacional ha comenzado a ver cómo la actividad en la red puede ser empleada más allá de fuente de reclutamiento y comunicación entre sus miembros. Así grupos como la ciberguerilla Izz ad-Din al-Qassam, han comenzado a emplear metodologías muy similares a las que emplean grupos como Anonymous para realizar sus acciones en la red. Una de sus formas más recurrentes de ataque ha sido contra bancos estadounidenses. Estos ataques constantes se han sucedido a lo largo de un periodo de ocho meses. Al igual que apuntábamos respecto al caso iraní, parece que grupos vinculados a este país son los dan soporte a este nuevo "comando" que también suele aparecer como QCF (Izz ad-Din al-Qassam Ciber Fighters).

En este sentido, podemos encontrar paradojas al estilo de la OpUSA, anunciada para el próximo día 7 de mayo por parte de Anonymous, como forma de protesta de las violaciones de derechos humanos en las que los EEUU pueden ser responsables. Podría darse el caso que, aunque de forma autónoma, converjan los intereses de grupos completamente divergentes en este ataque. Como hemos explicado más arriba, el caso de Siria e Irán no deja de colmar de contradicciones a un occidente capaz de apoyar a los mismos yihadistas que persigue en sus propias fronteras.

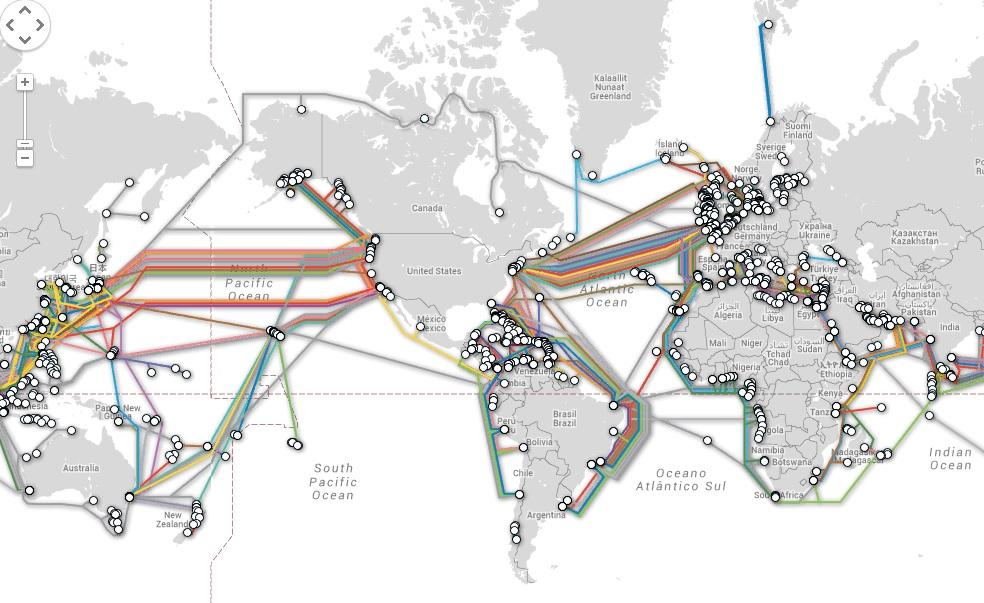
La "lucha contra el terrorismo" se ha convertido en el nuevo comodín del populismo conservador capaz de justificar cualquier legislación una vez modelada oportunamente la opinión pública. La realidad ha demostrado que la mayor parte de las líneas de actuación que se han anunciado públicamente han terminado por tener un empleo bien distinto. Las diversas unidades surgidas a partir de la Patriot Act, después del 11S, demostraron una escasa eficacia a pesar de la ingente cantidad de recursos destinados a estas. El espionaje del activismo dentro de los propios EEUU ha terminado por ser una de las mayores actividades de dichos grupos. En este sentido la ciberyihad parece ser el placebo necesario para mantener una tensión pública lo bastante asustada como para comulgar con una sustracción de derechos de otro modo intolerable.

La propia legislación que supuestamente persigue controlar las comunicaciones terroristas no deja de ser un brindis al sol al respecto. Sin embargo, legislaciones como CISPA permitirán que el espionaje ciudadano pueda realizarse no solo por agencias estatales autorizadas para ello, incluso extrajudicialmente al tratarse de la supuesta persecución del terrorismo, sino por las mismas compañías que prestan servicios de Internet.

Intentar orientarnos entre los múltiples escenarios de la ciberguerra y el cibercrimen resulta tan complejo como relatar el nuevo orden mundial que se está conformando. Quizás lo más interesante es que estos movimientos soterrados son las muestras de mayores despliegues y pueden apuntar la dirección geoestratégica del futuro. La ciberguerra en la actualidad no es más que la escaramuza inicial de futuros conflictos. Aun así, en un futuro próximo su importancia la llevará a un primer plano. De cualquier manera, conocer su desarrollo dice mucho más que los discursos oficiales, teñidos de la diplomacia falsaria que nos revelara Wikileaks.

2.3 La lucha por el control de Internet

El control de la infraestructura

Tanto los medios masivos de comunicación tradicionales como los nuevos, basados en las Tecnologías de la Información y la Comunicación, son herramientas claves e imprescindibles en las nuevas estrategias en la lucha por el control hegemónico y son la base de los nuevos modelos de guerras, basadas en desgastes, difusión de información falsa o generación de masa crítica tras la difusión de noticias falsas o tendenciosas más los ataques cibernéticos concretos.

La propiedad y el control de las fibras ópticas submarinas que comunican al mundo entero, está en manos de corporaciones que responden a los diferentes ejes de poder político centrales. Entre ellas Telefónica, Google, China Telecom, etc. Las mismas potencias centrales poseen, por ejemplo, submarinos no tripulados capaces de realizar ataques físicos (cortar los cables) en pocos minutos lo que incomunicaría parcial o totalmente a millones de personas: el equipamiento industrial o médico, por ejemplo, depende de computadores y conexión a internet, el sistema financiero va camino a abandonar el papel moneda y manejarse exclusivamente con “dinero electrónico” que no es otra cosa que millones de transacciones por redes informáticas, desde dispositivos electrónicos, dependiendo en forma exclusiva de las redes informáticas y

software para ello.

La guerra de nuestro tiempo se hace en el mundo virtual. Los ejércitos cibernéticos de Estados Unidos, Rusia y otras potencias como China pugnan, con grandes presupuestos y ejércitos cada vez más numerosos de cibersoldados, por lograr una posición hegemónica en internet. Éste, sin embargo, no es un territorio, sino más bien un marco dinámico en el que diariamente surgen fragilidades y desafíos a los que hacer frente.

Por eso, la actuación de estos países en la red de redes es una combinación de amurallamiento cibernético, asedio informático, robo de datos y espionaje. Hacer caer una página web utilizada por los ciudadanos para llevar a cabo gestiones administrativas, robar a gran escala datos de tarjetas bancarias, acceder a bases de información de servicios gubernamentales, irrumpir en registros de información de servicios sensibles, tanto públicos como privados, obtener datos de proyectos científicos.

Ése es el catálogo más común de actividades de cualquier batallón de ciberguerra. Hacen, por lo general, un incansable trabajo cotidiano que consiste en diagnosticar las grietas propias para subsanarlas y en localizar las del contrario, para penetrar por ellas y obtener ventaja estratégica o para causar el mayor daño posible. Y lo hacen generalmente en el más críptico de los silencios.

**¿Qué se ataca en un ciberataque?**

El más habitual es el ataque de Denegación de Servicio y su hermano aún más complicado, el ataque de Denegación Distribuida de Servicio (DoS y DDoS, por sus siglas en inglés). Es el más sencillo.

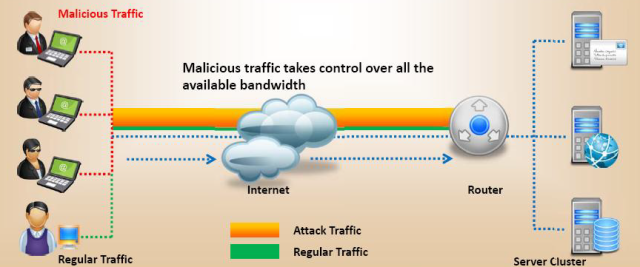
El ejemplo más simple es el de querer acceder a un sitio web de un determinado servicio y encontrarse con que no funciona por mucho que refresque el sitio con la tecla F5. Quizá este sitio está siendo víctima de un ataque DDoS.

Esto Consiste básicamente en saturar los recursos de un servicio cualquiera en internet, mediante el envío de una cantidad de peticiones que no puede asimilar. Esto, fácil de hacer contra usuarios particulares o páginas web de empresas pequeñas, tiene mucha más dificultad cuando se trata de atacar recursos de una administración, en este caso la estadounidense.

Por ello, en esos casos, el ataque que suele primar es el conocido como de Amplificación y Reflexión. Con una pequeña línea de código, generas una respuesta masiva.

¿Para qué sirve esto?

Para privar a los usuarios de los servicios temporalmente y demostrar fuerza de hackeo. Un ataque DDoS de ese tipo suele ser el paso previo a una ofensiva mayor. Hacer caer un servicio por saturación puede dejar al descubierto sus vulnerabilidades de programación. Y eso se aprovecha para, por ejemplo, acceder a las bases de datos y robarlos. Son los datos que se utilizan para acceder a cuentas bancarias o para chantajear a las empresas y sus usuarios.



2.4 Casos

**Stuxnet**

Stuxnet es un gusano informático que afecta a equipos con Windows, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad ubicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares.

Stuxnet es capaz de reprogramar controladores lógicos programables y ocultar los cambios realizados. También es el primer gusano conocido que incluye un rootkit para sistemas reprogramables PLC.4

La compañía europea de seguridad digital Kaspersky Lab describía a Stuxnet en una nota de prensa como "un prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial". Un ejecutivo de Symantec, advirtió que el 60% de los ordenadores contaminados por el gusano se encuentran en Irán, sugiriendo que sus instalaciones industriales podrían ser su objetivo.

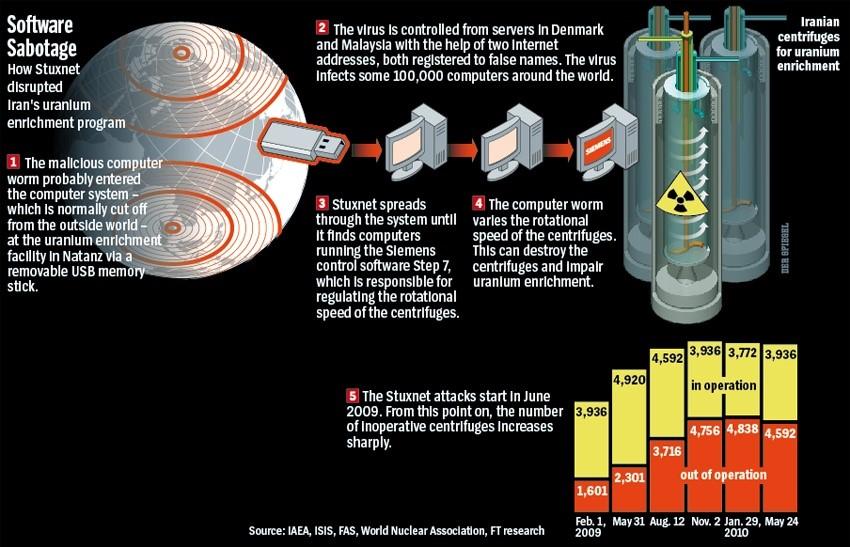
Kaspersky concluye que los ataques sólo pudieron producirse "con el apoyo de una nación soberana", convirtiendo a Irán en el primer objetivo de una guerra cibernética real.

El objetivo más probable del gusano, según corroboran medios como BBC o el Daily Telegraph, pudieron ser infraestructuras de alto valor pertenecientes a Irán y con sistemas de control de Siemens. Medios como India Times apuntan que el ataque pudo haber retrasado la puesta en marcha de la planta nuclear de Bushehr. Fuentes iraníes han calificado el ataque como "guerra electrónica" aunque minimizan el impacto de los daños en sus instalaciones. Algunos medios como el norteamericano New York Times han atribuido su autoría a los servicios secretos estadounidenses e israelíes. Stuxnet busca sistemas de control industriales y luego modifica el código en ellos para permitir que los atacantes tomen control de los sistemas sin que los operadores lo noten. En otras palabras, esta amenaza está diseñada para permitir a los hackers manipular equipamiento físico, lo cual lo hace extremadamente peligroso.

Esta amenaza no es parecida a nada de lo visto anteriormente, no sólo en lo que hace, sino en cómo se descubrió. Es el primer virus informático que permite hacer daño en el mundo físico. Es sofisticado, requirió importantes fondos económicos para ser desarrollado y no existen en la actualidad muchos grupos que puedan desarrollar una amenaza de este tipo. Es también el primer ataque cibernético que hemos visto que ataca específicamente a sistemas de control industrial.

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

“Realmente nunca hemos visto algo así antes y el hecho de que pueda controlar el funcionamiento de una maquinaria física es inquietante”, comentó Liam O’Murchu, investigador de Symantec Security Response.

Industrie

**Industroyer**

Dos firmas de ciberseguridad revelaron que existe un poderoso programa malicioso capaz de detener el funcionamiento de los sistemas de distribución de electricidad y otras infraestructuras claves.

La compañía con sede en Eslovaquia ESET dijo que este software es la amenaza más poderosa desarrollada desde el descubrimiento de Stuxnet, la herramienta de hacking utilizada para sabotear el programa nuclear de Irán que se creía que estaban desarrollando los servicios de inteligencia de Estados Unidos e Israel.

ESET dijo que este programa, apodado Industroyer, podría estar detrás del apagón de una hora y media que sufrió la capital ucraniana, Kiev, el pasado mes de diciembre.

La compañía señalo que el poder de la amenaza de Industroyer radica en que funciona utilizando protocolos de comunicación diseñados hace décadas e incorporados en sistemas de energía, transporte, agua y gas de todo el mundo.

Utilizando uno de esos protocolos, débilmente protegidos, Industroyer puede tomar directamente el control de los interruptores de subestaciones eléctricas y de circuitos, lo que da a los hackers la posibilidad de cortar la distribución de energía y dañar los equipos.

Este malware es la "mayor amenaza a los sistemas de control industrial desde Stuxnet", estimó ESET sin indicar quién estaba detrás.

Sin embargo, en un informe separado divulgado este lunes sobre el mismo programa malicioso, una segunda compañía de seguridad, Dragos, lo vinculó con un grupo ruso de hackers llamado Sandworm que ha sido relacionado con el gobierno ruso.

Dragos ha apodado a este virus CrashOverride y considera también que se trata del segundo malware desplegado para interrumpir procesos físicos industriales después de Stuxnet.

"CrashOverride no es específico de un comerciante o de una configuración, en su lugar hace uso de operaciones de redes eléctricas y comunicaciones en red para causar impacto", dijo Dragos.

La empresa añadió que el malware podría usarse en varias subestaciones eléctricas al mismo tiempo pudiendo crear un extenso apagón que podría permanecer horas e incluso días.

3-Metodologías y ataques.

3.1 Conceptos y Metodologías Principales.

Según la RAE, un ataque es la “acción de atacar, acometer o emprender una ofensiva”, por lo tanto, se podría definir un “ciberataque” como la acción de atacar, acometer o emprender una ofensiva en el ciberespacio.

Los ataques cibernéticos o ciberataques aprovechan las vulnerabilidades, ya estén asociadas al software, a los dispositivos informáticos o a las personas que los administran y utilizan. Con el aumento de la complejidad de los sitios web y el rápido desarrollo de aplicaciones, aumenta la posibilidad de sufrir ataques. Mientras tanto, los piratas informáticos y ciber mercenarios crean, distribuyen y utilizan sofisticadas herramientas de exploit y malware para robar o destruir datos empresariales fundamentales, comprometer sitios web e interrumpir estructuras operativas.

Tanto si el motivo es el espionaje como el sabotaje, los ciberdelincuentes emplean distintos métodos de ataque, como el "spear-phishing", el ataque de inyección SQL, el filtro de scripts de sitios (XSS) y los ataques de fuerza bruta, adaptándolos o usándolos de forma combinada para llevar a cabo elaborados ciberataques. Uno de las tácticas más perturbadora utilizada en los ciberataques es el ataque distribuido de denegación del servicio (DDoS), en el que se utilizan botnets para congestionar un sitio web o una aplicación web hasta el punto que los usuarios legítimos no pueden acceder a él, algo que cuesta a las empresas millones de dólares en ingresos, pérdida de productividad y daños en la reputación.

A continuación, se nombran las metodologías y elementos principales de los Ciberataques.

**Los virus informáticos**

Son programas que infectan, o pretenden infectar, a otros archivos con el objetivo de infectar y producir daños en el sistema informático en el que se han introducido. Como un virus en el cuerpo humano, éste se va a transmitir a otros archivos y así se va a ir propagando e infectando nuevos archivos.

**Los Troyanos**

También llamados Caballos de Troya, son una especie de virus que se caracteriza por engañar a los usuarios disfrazándose de programas o archivos habituales, como fotos, archivos de música o de correo entre otros, para de esta forma infectar y causar daño. El principal objetivo es dar acceso al sistema informático infectado para poder robar información personal e incluso confidencial.

**El envío masivo de correo no deseado o SPAM**

Se denomina “SPAM” a los mensajes enviados por correo electrónico y que son no deseados, no solicitados o de remitente desconocido, habitualmente con publicidad. Se califica de “envío masivo” ya que generalmente son enviados de forma masiva a un servidor o cuenta, de tal forma que éste se sature por la gran cantidad de datos que recibe y que llegan al límite de su capacidad de procesamiento, impidiendo así la recepción de emails e información necesarios.

**Rootkits**

Es un conjunto de herramientas que consiguen ocultar un acceso ilícito a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema. Al estar diseñados para pasar desapercibidos, no pueden ser detectados.

**El uso de archivos BOT del IRC (Internet Relay Chat)**

Es un programa que permite que el sistema sea controlado remotamente sin el conocimiento ni el consentimiento del usuario. Se suelen utilizar en webs de conversación online, como los chats o programas IRC.

**Interferencia electrónica de comunicaciones**

La interferencia electromagnética es la perturbación que ocurre en cualquier circuito, componente o sistema electrónico causada por una fuente de radiación electromagnética externa al mismo. Esta perturbación puede interrumpir, degradar o limitar el rendimiento del sistema, causando así interferencias con el propósito expreso de producir una disfunción en los sistemas de comunicaciones.

**Blind Radars:**

Se trata de una técnica de interferencia electrónica de los radares de las torres de control y de los sistemas de seguimiento de los aviones, con el fin de bloquear el tráfico aéreo y que puede llegar a producir choques en el aire o que un avión se estrelle.

**El envío o instalación de virus espías o “Keyloggers” en inglés**

Es un programa que registra y graba las pulsaciones de las teclas. De esta forma, la persona que haya instalado el programa, podrá utilizar la información recolectada.

3.2 Ataques.

**Keylogger**

Es un programa de ordenador, o elemento de hardware que graba cada pulsación del teclado y guarda estos datos en un archivo. Una vez que reúne la cantidad de datos necesaria, la transfiere a través de Internet a un host remoto predeterminado. Puede también realizar capturas de pantalla y usar otras técnicas para controlar la actividad del usuario. Un Keylogger puede causar la pérdida de contraseñas, datos de autentificación y similar información.

Keylogger con Hardware

Los Keyloggers físicos son pequeños dispositivos que se instalan entre nuestra computadora y el teclado. Son difíciles de identificar para un usuario inexperto, pero si se presta atención es posible reconocerlos a simple vista. Tienen distintas capacidades de almacenamiento, son comprados en cualquier casa especializada y generalmente son instalados por empresas que desean controlar a ciertos empleados. Adaptadores en línea que se intercalan en la conexión del teclado, tienen la ventaja de poder ser instalados inmediatamente. Sin embargo, mientras que pueden ser eventualmente inadvertidos se detectan fácilmente con una revisión visual detallada.

1. Dispositivos que se pueden instalar dentro de los teclados estándares, requiere de habilidad para soldar y de tener acceso al teclado que se modificará. No son detectables a menos que se abra el cuerpo del teclado.

2. Teclados reales del reemplazo que contienen el Keylogger ya integrado. Son virtualmente imperceptibles, a menos que se les busque específicamente.

Keylogger con Software

Contrariamente a las creencias populares, el código de un Keylogger por software es simple de escribir, con un conocimiento básico de la API proporcionada por el sistema operativo objetivo. Los Keylogger de software se dividen en:

1. Basado en núcleo: este método es el más difícil de escribir, y también de combatir. Tales keyloggers residen en el nivel del núcleo y son así prácticamente invisibles. Derriban el núcleo del sistema operativo y tienen casi siempre el acceso autorizado al hardware que los hace de gran alcance. Un Keylogger que usa este método puede actuar como driver del teclado, por ejemplo, y accede así a cualquier información registrada en el teclado mientras que va al sistema operativo.

2. Enganchados: estos keyloggers registran las pulsaciones de las teclas del teclado con las funciones proporcionadas por el sistema operativo. El sistema operativo activa el Keylogger en cualquier momento en que se presione una tecla, y realiza el registro.

3. Métodos creativos: aquí el programador utiliza funciones como GetAsyncKeyState, GetForegroundWindow, etc. Estos son los más fáciles de escribir, pero como requieren la revisión del estado de cada tecla varias veces por segundo, pueden causar un aumento sensible en uso de la CPU y pueden ocasionalmente dejar escapar algunas pulsaciones del teclado.

El ejemplo más común de Keylogger de software Los Troyanos, los daños o violaciones de privacidad que puede causar este virus es el uso de la webcam sin permiso, borrar el disco, modificar la agenda de contactos, efectuar llamadas y enviar SMS, hasta geolocalizar al usuario por GPS.

Existen dos métodos principales usados por keyloggers para entrar en el sistema:

• Un Keylogger legítimo puede ser instalado manualmente en el sistema por su administrador o cualquier otro usuario que tenga privilegios para hacerlo. Un hacker puede entrar en el sistema y configurar su Keylogger. En ambos casos, la amenaza a la privacidad se instala en el sistema sin el conocimiento y consentimiento del usuario.

• Los keyloggers maliciosos pueden ser instalados en el sistema con la ayuda de otros parásitos, como virus, troyanos, backdoors y otros malwares. Entran en el sistema sin el conocimiento del usuario y afectan a todos los usuarios que usan el ordenador comprometido. Estos keyloggers no tienen funciones de desinstalación y pueden ser controlados solo por sus autores o por los atacantes.

En la mayoría de los casos, los keyloggers afectan a ordenadores que ejecutan el sistema operativo Microsoft Windows. Sin embargo, todos los virus son constantemente actualizados, por lo que no hay garantía de que no sean capaces de hacker otras plataformas populares.

**Malware Cherry Blossom**

Se enfoca en Servicios inalámbricos como routers y Access points, involucrando dispositivos wifi tanto hogareños como en espacios públicos.

Funciona modificando la configuración de los dispositivos como por ejemplo los servidores DNS especificados e inyectando contenido malicioso para explotar vulnerabilidades.

**Pandemic: Falsas aplicaciones**

El proyecto Pandemic es un implante persistente para las máquinas con Microsoft Windows que comparte archivos con usuarios en una red local.

Pandemic ofrece un acceso remoto a los usuarios al reemplazar una aplicación mediante código con una versión troyana del programa.

Como su nombre sugiere, tan sólo hace falta que una sola computadora de una red local comparta los archivos sea infectada para que replique la pandemia.

**Brutal Kangaroo**

Para proteger una Red de alta seguridad muchas veces dicha red no tiene acceso a Internet por lo que los usuarios utilizan dispositivos Flash para mover contenido desde la internet hacia la red aislada.

Brutal Kangaroo infecta los dispositivos USB en lo que sería el “primer salto”, luego al conectarse dicho dispositivo a la red aislada realiza el “segundo salto” infectando a la computadora de la red, y luego el “tercer salto” sería la infectación de toda la red aislada, robando datos sensibles.

Las redes físicamente aisladas pueden ser bancos y entidades financieras, la industria de la energía nuclear, agencias de inteligencia, ejércitos, etc.

La transmisión de dichos datos se realiza por el camino inverso, de la red aislada a la red conectada a internet mediante las memorias portátiles.

Se cree que es una versión actualizada del virus Stuxnet.

**Bots y botnets**

Los bots representan uno de los delitos cibernéticos más sofisticados y populares. Permiten a los hackers tomar el control de muchos equipos a la vez y convertirlos en equipos "zombis", que funcionan como parte de un poderoso "botnet" que propaga virus, genera spam y comente otros tipos de delitos y fraudes.

Un "bot" es un tipo de programa malicioso que permite a un atacante tomar el control de un equipo infectado. Por lo general, los bots, también conocidos como "robots web" son parte de una red de máquinas infectadas, conocidas como “botnet”, que comúnmente está compuesta por máquinas víctimas de todo el mundo.

Debido a que un equipo infectado por bots cumple las órdenes de su amo, muchas personas se refieren a estos equipos víctima como “zombis”.

Algunos botnets pueden englobar cientos o un par de miles de equipos, pero otros cuentan con decenas e incluso centenares de miles de zombis a su servicio. Muchos de estos equipos se infectan sin que sus dueños se enteren. ¿Existe algún indicio? Un bot puede hacer que un equipo se ralentice, muestre mensajes misteriosos e, incluso, falle.

Roban información privada y personal y se la comunican al usuario malicioso:

- credenciales bancarias

- otra información personal y confidencia

Lanzan ataques de denegación de servicio (DoS) contra un objetivo específico. Los criminales cibernéticos extorsionan a los propietarios de los sitios web por dinero, a cambio de devolverles el control de los sitios afectados.

Sin embargo, los sistemas de los usuarios diarios son el objetivo más frecuente de estos ataques, que sólo buscan molestar.

3.4 Ciberataques Globales.

**WannaCry**

El 12 de mayo de 2017 se registró una infección a gran escala que afectó a las empresas Telefónica, Iberdrola y Gas Natural, entre otras compañías en España, así como al servicio de salud británico, como confirmó el Centro Nacional de Inteligencia. Posteriormente el software malicioso se extendió a otros países, volviéndose un ataque de escala mundial. Se ha informado de al menos 74 objetivos alrededor del mundo que fueron atacados al mismo tiempo.

Los análisis previos sostienen que WannaCry usó la vulnerabilidad EternalBlue, desarrollada por la Agencia de Seguridad Nacional estadounidense y filtrada por el grupo The Shadow Brokers, que permite atacar computadores con el sistema operativo Microsoft Windows. Dicha vulnerabilidad fue detectada en marzo en los sistemas operativos Windows. La compañía Microsoft comenzó a distribuir parches de seguridad al día siguiente de conocerse esta vulnerabilidad, el 10 de marzo de 2017, a través de Windows Update para las versiones de Windows posteriores a Windows Vista y como un parche por separado para Windows 8, Server 2003 y XP una vez desplegado este malware. Los computadores del mundo empresarial que no habían aplicado las actualizaciones de seguridad del 14 de marzo de 2017 que incluían la solución al problema MS17-010 en el sistema operativo Windows quedaron gravemente afectados, con sus archivos codificados y apareciendo un mensaje en pantalla que exigía un rescate de 300 dólares en bitcoins a cambio de descodificar los archivos.

Un programador de Reino Unido pudo detener una mayor expansión del ciberataque global iniciado. El autor del blog MalwareTechBlog estaba estudiando el virus cuando se dio cuenta de que el programa malicioso estaba conectándose a un dominio no registrado. El malware buscaba conectarse a este dominio, si no lo lograba infectaba el equipo, si lo lograba detenía la infección. Después de que ese experto en seguridad cibernética registrara el dominio que se encontraba libre, el malware pudo conectarse al dominio y cesó sus ataques.

4-Defensa, Ciberdefensa y capacidad de respuesta

4.1 Técnicas de Ciberdefensa.

Las técnicas de defensa ante ataques realizados por grupos organizados se adaptan a las agresiones que se conocen y realizando simulaciones de posibles embates futuros.

Para tal fin se pueden utilizar maquinas señuelos, implementadas con software especial y configurada la red de manera que simule ser una red empresarial. De tal forma los ataques se pueden monitorear y luego analizar para generar técnicas de defensa novedosas y adelantarse a un ataque en tiempo real sin perder bajas significativas.

Los ataques más comunes son colapsar los servidores de páginas web generando solicitudes masivas a las cuales el servidor no es capaz de responder, es decir que el servidor es incapaz de recibir y contestar peticiones. Este tipo de ataque DoS, por Denial of Service se realiza desde una sola máquina, lo cual es bastante sencillo de resolver averiguando la dirección ip del pc que genera dichas peticiones y bloqueando el acceso a la misma.

Otro tipo de ataque similar al anterior mencionado es el DDoS, Distributed Denial of Service o Denegación de servicios distribuida, lo cual significa que el ataque no se produce desde una solo pc, sino que lanza desde varias al mismo tiempo.

Para ello se utilizan maquinas que se encuentran dormidas – mediante troyanos - hasta que el atacante las reactiva para realizar el ataque.

Una de las técnicas utilizadas para bloquear la petición de servicios es el bloqueo de las direcciones ip solicitantes, para lo cual existen dos tipos de restricciones para esta práctica; por un lado, se corre el riesgo de bloquear solicitudes auténticas al servicio web y por el otro la capacidad de bloqueo del firewall (capacidad del hardware Memoria / CPU) para abarcar todos los paquetes entrantes.

Una de las formas de evitar o suavizar estos ataques es utilizando balanceadores de carga y servidores auxiliares para alivianar el trabajo.

Otra es realizar un ajuste en la configuración TCP (Hardeningn TCP/IP Stack) del Sistema Operativo del servidor que soporta el servicio WEB para aumentar los tiempos de respuesta a un valor lo suficientemente largo, como para minimizar los efectos sobre el servicio que se ofrece a sus usuarios mientras dure el ataque.

Las técnicas más efectivas son aquellas que disponen de un modelo combinado en cuanto a las medidas de protección, es decir, disponen de sistema de protección automático para bloquear direcciones IP en los sistemas de seguridad, activación de recursos latentes y ajustes de configuración para controlar algunos parámetros en particular del protocolo TCP, como por ejemplo; Modificación del registro de Windows alargando el tiempo de respuesta por cada petición ( timeout ), modificación de los parámetros de hardware evitando el consumo excesivo de recursos (CPU, Ancho de banda, Memoria RAM).

Otras posibles soluciones, serían la utilización de los recursos ofrecidos por los lenguajes de programación tales como módulos de protección (PHP) como por ejemplo FLOOD Y BRUTE FORCE ATTACKS.

4.2 La mejor defensa es el ataque – Defensa Legal.

**Ciberguerra**

Las guerras se habían llevado a cabo en los espacios terrestre, marítimo, aéreo y en el espacio electromagnético. Es a partir de la década de los 90 cuando la consolidación del crecimiento de la infraestructura tecnológica y el uso de las redes, hacen que cada vez se vea más al ciberespacio como un nuevo campo de batalla, donde se lleve a cabo la ciberguerra. Esta nueva forma de hacer la guerra no se limita solo a efectos sobre los equipos informáticos, sino que sus consecuencias pueden trasladarse al mundo físico

Ante tal amenaza los Estados se están organizando. Si el dominio de las tres dimensiones tierra, aire y mar; supuso la creación de los Ejércitos de Tierra, Aire y Armada respectivamente. Hoy, los retos y amenazas que presenta el ciberespacio están haciendo que los Estados estén creando “ciber ejércitos”. Sin embargo, no creamos que todos están compuestos de personas uniformadas frente a un ordenador. La mayoría de los países están contratando a personal experto (muchos de ellos hackers conocidos) para que trabajen en estos cometidos.

Desde el punto de vista de la regulación de los conflictos, los gobernantes que recurran a la ciberguerra lo tendrán que hacer desde el respeto al ius ad bellum (el Derecho Internacional que rige la autorización del empleo de la fuerza por los Estados soberanos) y del ius in bello (el de la conducción de las hostilidades), mientras no se tenga ninguna regulación acorde a la regulación de estos nuevo.

**Principal normativa internacional y nacional**

Una vez planteado la cuestión sobre el vacío legal en el ciberespacio y las posibles formas de regularlo, se van a exponer la principal normativa que existe tanto en el plano internacional como nacional. Ésta no es sólo escasa, sino que tampoco hay voluntad, por parte de los Estados, para su cumplimiento.

La OTAN decidió poner en marcha un programa global de coordinación de la ciberdefensa, con el objetivo de reforzar las capacidades de la Alianza y luchar contra los ataques informáticos. No fue hasta después de los acontecimientos de Estonia (2007), cuando se decidió a trabajar con el objetivo de definir un nuevo concepto estratégico de política de Ciberdefensa, En él se contemplan los ciberataques como acciones que pueden poner en riesgo la prosperidad, la seguridad y la estabilidad de los Estados miembros y se marcan directrices y recomendaciones en el área de la ciberdensa. En general, la OTAN ha tomado el criterio de que son los países miembros los que tienen que proteger sus redes en base a medios (software y hardware) y a una regulación desarrollada.

En cuanto a Naciones Unidas parece enfrentarse a los mismos problemas a los que se tuvo que enfrentar la regulación de las aguas territoriales o a la del espacio aéreo.

**Manual de Tallin**

Como consecuencia de la falta de legislación aplicable a las nuevas guerras en el ciberespacio, una de las primeras iniciativas fue la convocatoria de un Grupo Internacional de Expertos (GIE) en defensa, ciberseguridad y Derecho internacional, para que trabajaran en lo que pudiera ser el equivalente de la Convención de Ginebra sobre el DIH, aplicado a los conflictos en el ciberespacio. El resultado fue el Manual de Tallín, que fue dirigido por el Profesor Michael Schmitt de la US Naval War College, y que se presentó en Londres el 15 de marzo de 2013.

La premisa fundamental con la que se empezó a redactar este Manual fue que la guerra no deja de ser tal porque se lleve a cabo en el ciberespacio, es decir, es posible la guerra en el ciberespacio. Aunque a fecha de hoy no se tengan datos empíricos reales sobre los efectos de las ciber armas, sólo algunos hechos como los de Estonia (2007) y Stuxnet (2010), se cree que no es ciencia ficción y que sus posibilidades pueden ir más allá de una denegación de servicio. Antes de que sea demasiado tarde, es necesario poner de relieve que ciertas acciones, como, por ejemplo, penetrar ilegalmente en los ordenadores centrales de control de una presa y conseguir descargar el agua, pueden tener el mismo efecto que si se volaran con explosivos las compuertas y el agua pudiera salir de la misma.

Interpretar, por primera vez, las normas existentes a los ciberataques.

Unir el mundo ciber con el jurídico en sus análisis y sus comprensiones mutuas.

Valorar la capacidad de los Estados de buscar el consenso sobre los límites éticos y jurídicos en el ciberespacio, especialmente en lo que respecta a la agresión armada y el empleo de la fuerza.

La falta de anticipación a las incertidumbres actuales sobre las normas aplicables al ciberespacio podría tener, en el futuro, consecuencias desastrosas. Así lo señala el Profesor Jack Goldsmith (Harvard): “Un Estado podría emprender una operación cibernética que otro clasificara como acto de guerra, incluso cuando la primera nación no tuviera la intención de emprender semejante acción”.

**Aspectos claves del Manual**

A continuación, se va a estudiar la ciberguerra y el DIH. Como se va a poder observar, hay algunos aspectos de esta forma de conflicto que pueden crear innumerables controversias, al querer tratar de regularlo, desde este prisma. Las particularidades, la forma de actuar y los actores que tienen cabida en el ciberespacio, entre otros; provocarán innumerables comentarios y discrepancias sobre esta forma de poder llevar a cabo la guerra.

**a) Ciberataque y conflictos del DIH.**

Partiendo de la definición de ciberataque como aquella operación cibernética ofensiva o defensiva de la que se espera que pueda causar pérdidas de vidas humanas, lesiones a las personas y daños o destrucciones de bienes; se puede ver que este tipo de acción entra dentro de la definición contemplada en el artíc. 49 del Protocolo Adicional I a los Convenios de Ginebra.

El primer aspecto controvertido es determinar si cualquier operación de ciberguerra puede ser considerada como “un conflicto armado” y, por tanto, puede regularse a través del DIH. En este sentido, surgen dos puntos de vista: los que afirman que cualquier ciberataque tendría cabida y los que piensan que debería existir una relación directa entre la operación y los objetivos militares. Parece lógico pensar que no todas las acciones que se lleven a cabo podrían tener cabida. La razón es que, durante el conflicto, se pueden producir infinidad de ciberataques por actores estatales y no estatales, a priori, de difícil descubrimiento y, caso de hacerlo, de complejidad en definición.

Algunos miembros del GIE señalaron que las acciones de ciberguerra entre Rusia y Georgia (2008) si lo fueron debido a que se efectuaron en el seno de un conflicto armado. Sin embargo, los “supuestos” ciberataques de Rusia contra Estonia (2007) no porque no fueron parte de un conflicto. Además, el gran número de ciberataques y lugares diferentes desde donde se llevaron a cabo dificultó la asignación de responsabilidades. A pesar de que se sospecha que Rusia estaba detrás de ellos, en ningún momento se ha podido demostrar que su culpabilidad.

**b) Soberanía y responsabilidad.**

La soberanía de un Estado también puede ser violada por ataques desde el ciberespacio. Los Estados deberán controlar las infraestructuras cibernéticas que se encuentren en su territorio o que actúan bajo su bandera, sin estar en sus límites geográficos.

La duda aquí surge sobre la responsabilidad del Estado ante acciones cibernéticas que se lleven a cabo desde su territorio o que transiten por él, sin que se pueda comprobar que tuviera conocimiento ni capacidad para detectarlas. Parece lógico pensar que sólo en el caso de tener conocimiento de ello y no haber puesto los medios o informarlo, en caso de no tenerlos, podría incumplir la ley.

Otro aspecto que crea problemas es el control de un Estado por las acciones que se puedan llevar en su nombre. Así, se considerará “hecho del Estado”, según el derecho internacional, “el comportamiento de una persona o de un grupo de personas si esa persona o ese grupo de personas actúa de hecho por instrucciones o bajo la dirección o el control de ese Estado al observar ese comportamiento”. Los ciberataques que sufrió Estonia (2007) si fueron un atentado a su soberanía, sin embargo, y a pesar de las evidencias, no se pudo culpar a Rusia porque en ningún momento se pudo comprobar el más mínimo control sobre el caos originado. No existe prueba alguna de que el grupo de hackers operara bajo control de ningún Estado.

Otro caso anterior, aunque no tuvo como protagonista los ciberataques, fue el apoyo que prestó EEUU a la Contra de Nicaragua. En este caso no se responsabilizó a EEUU por hechos internacionalmente ilícitos porque, a pesar de probarse que estaba financiando a este movimiento, no se pudo comprobar que dirigiera sus acciones (control efectivo o total). Como se puede comprobar el aspecto del “control” es bastante ambiguo y está también presente en el ciberespacio.

Ni que decir tiene que acciones en las que un Estado presta ayuda o asistencia a otro Estado y/o lo dirige en la comisión por este último de un hecho internacionalmente ilícito, también puede tener que responder por hechos internacionalmente ilícitos.

En respuesta a las mismas, cualquier Estado podría recurrir a mecanismos de respuesta (contramedidas) con el objeto de que el Estado agresor se reanude en el cumplimiento de sus obligaciones, cesando en su comportamiento ilegítimo. Sin embargo, estas contramedidas no podrán afectar, de ninguna de las maneras a las obligaciones de carácter humanitario que prohíben las represalias ni incumplir el principio de proporcionalidad. También se excluyen de estas contramedidas las relativas al uso de la fuerza. Sin embargo, dentro de la Resolución de la Asamblea General 56/83 de las NNUU, también se dice que los artículos se entenderán sin perjuicio de lo que exprese la Carta de las NNUU, y esta expresa en su artic. 51 el derecho inmanente a la legítima defensa…en caso de ataque armado (posteriormente se analizarán los ataques armados y el ciberespacio).

**c) Uso de la fuerza.**

Si los criterios que aparecen en la Carta ofrecen múltiples interpretaciones para determinar cuándo un acto constituye un “uso de la fuerza” (artíc. 2.4), el ciberespacio no hace más que aumentar el problema y crear más ambigüedad.

Para tratar de solucionar la cuestión se tendrá en cuenta los aspectos que más íntimamente están ligados con el “uso de la fuerza”: la escala (grado/umbral) y los efectos. En el caso de un ciberataque, a priori, serán determinantes los efectos, los cuales deben ser comparables a los de un ataque convencional.

A continuación, se citan una serie de indicios que van a ayudar a determinar si una acción en el ciberespacio, es un “uso de la fuerza” o no:

Gravedad: Se trata del factor más importante y la cuestión fundamental será determinar cuáles son los límites que, una vez sobrepasados, determinan que se ha hecho “uso de la fuerza”. El alcance, la duración y las consecuencias tendrán gran importancia en la valoración de su gravedad de la acción. En resumen, se tratará de responder a cuestiones como: ¿cuántas personas han muerto?, ¿qué daños se han causado?, etc.

Inmediatez: Tiene que ver con la separación temporal entre acciones y efectos. Muchas acciones en el ciberespacio no producen efectos inmediatos, sino que éstos aparecen con el paso del tiempo. Cuanto mayor sea la separación acción-efecto, más complicado será la posibilidad de afirmar que se ha hecho “uso de la fuerza”.

Intrusión: Se refiere al grado de penetración o alcance de las operaciones. Así, por ejemplo, no todos los dominios en el ciberespacio tienen la misma importancia (no es lo mismo uno que acabe en “…@. mdef.es”, del Ministerio de Defensa de España que uno particular, tipo “…@gmail.com”) y, por tanto, el grado de intrusión no es igual en ambos casos.

El ciberespionaje, que podría ser otra forma intrusión, no está considerado como un “uso de la fuerza”. Un ejemplo serían las acciones para deshabilitar los mecanismos de seguridad y acceder a la información de una red. Sin embargo, un avión que penetra en un espacio aéreo, sin autorización y con intención de llevar a cabo acciones de ciberespionaje, si podría ser acusado de “uso de la fuerza”.

Carácter militar e implicación del Estado: Cuanto mayor sea la relación o nexo entre las ciberoperaciones y las operaciones militares, mayor será la probabilidad de ser considerado un ciberataque como de “uso de la fuerza”.

La presunción de legalidad: El DIH es por naturaleza prohibitivo. si algo no está prohibido estaría autorizado. El ciberespionaje, no parece que suponga una violación del DIH, en cuanto a ser considerado como “uso de la fuerza”. A priori, no supone ni una violación del principio de no intervención ni siquiera un elemento coercitivo, aunque para ello tenga que superar elementos de seguridad (cortafuegos,..). Acciones de denegación de servicio, como los llevados a cabo en el caso de Estonia y que paralizaron su administración, no se consideraron tampoco como una violación del “uso de la fuerza”.

**d) Ataque armado**

La determinación de “ataque armado”, íntimamente ligado al de “uso de la fuerza”, también presenta discrepancias en el caso del ciberespacio. Se trataría ahora de determinar que “artefactos”, al ser usados, pueden dar lugar a un ataque armado. Sin embargo, y en la misma línea del punto anterior, parece que lo verdaderamente importante son las consecuencias que se deriven de su uso, y si estas, podían ser equiparables, por su gravedad a un ataque armado, y, por ende, a un uso de la fuerza.

Se podrían considerar como “ataque armado”, aquellos ciberataques que hieren, matan o destruyen propiedad y no lo serán aquellos que guardan relación con inteligencia, robo y en general aquellos que no interrumpen servicios esenciales (un hipotético ataque a una central distribuidora de agua para envenenamiento y que provocara enfermedades, no hay duda de que sería un ataque armado). Sin embargo, a día de hoy, no se ha considerado ningún ciberataque como ataque armado. De las dos principales acciones, Stuxnet y Estonia, sólo la primera parece haber alcanzado el umbral de la consideración de ataque armado, debido a que supuso la paralización total del programa nuclear. Además, todo apunta a que sea el primer uso, por parte de una nación, de un programa malicioso como arma informática contra la infraestructura de otra nación. Además, este incidente resulta significativo porque, hasta la fecha, inhabilitar una instalación de este tipo sólo habría sido posible mediante alguna acción física, por ejemplo, un bombardeo.

**e) Legítima defensa. Inminencia e inmediatez**

Si en el ciberespacio se ha determinado que se pueden dar casos de “uso de la fuerza”, también tendrá cabida la “legítima defensa”, en respuesta a los mismos. Esta afirmación se justifica con más argumentos si el “uso de la fuerza” es con ocasión de un ciberataque considerado como “ataque armado”. En este sentido, el artíc. 51 de la Carta de las NNUU reconoce el derecho a la legítima defensa.

Dentro de este apartado, es necesario comentar que también en el ciberespacio, como ocurriría en el caso de armas nucleares, se puede aprobar la “legítima defensa anticipada” (inminencia). Aunque este tema ha planteado muchos debates, parece que ésta sólo se pudiera aprobar en el caso de que, de no llevarse a cabo y el Estado esperara a sufrir un ciberataque, éste hubiera perdido cualquier oportunidad de responder ante los efectos del mismo (la relación causa-efecto debe estar muy justificada).

Relacionado con la “legítima defensa” también estaría el principio de inmediatez. El requisito de “inmediatez” (a diferencia de la exigencia de la inminencia) distingue un acto de legítima defensa de la mera represalia. Si la “inminencia” plantea discusiones, la “inmediatez” lo es más ante el tiempo que puede transcurrir hasta que se descubran los efectos y la identificación de los culpables. Esto se debe a que los efectos de los ciberataques no siempre serán conocidos de inmediato y por lo tanto no será fácil verificar si se ha recurrido al “uso de la fuerza” que determine una respuesta del tipo “legítima defensa”.

De cualquiera de las maneras la legítima defensa estará siempre limitada por los principios de necesidad, proporcionalidad y distinción; según las normas del DIH.

**f) Principio de necesidad y proporcionalidad.**

La ciberguerra puede ser un medio recurrente para los actores que se enfrentan a oponentes con los que existe un gran desequilibrio en recursos militares (personal, material, tecnología, etc.). Esta asimetría de medios, también puede completarse con una asimetría de valores provocando que la ciberguerra sea parte de una “guerra sin restricciones”.

Estas acciones deben responder al principio de necesidad de tal forma que se consiga un equilibrio entre las necesidades de la guerra y los condicionamientos humanitarios. En definitiva, se aplicarán ciberataques de tal grado que sus efectos sean los mínimos necesarios para conseguir el objetivo deseado, que es hacer que el enemigo cese en sus acciones.

La proporcionalidad hace referencia a la prohibición de armas y métodos que causen en las personas civiles y a sus bienes, o a ambos a la vez, daños excesivos con respecto a la ventaja militar concreta y directa prevista. Tras esta afirmación se plantea dos cuestiones:

Si hay alguna limitación o prohibición en cuanto a las ciberarmas. Todo parece apuntar que los efectos serán el factor que las delimite. Así pues, el alcance, duración e intensidad será el mínimo que haga al agresor desistir de sus acciones. No obstante, si la respuesta en forma de ciberataques, no fueran suficientes para detener la aptitud violenta del agresor (porque técnicamente no le afectan debido a que dispone de contramedidas que les hace inmunes), se podría hacer uso de acciones cinéticas,

El término “excesivo” no ha sido cuantificado. A pesar del comentario contradictorio del CICR, los expertos consideran que solo se autorizan los daños colaterales cuando la anticipación concreta y directa de la ventaja militar es suficiente respecto al ataque en su conjunto.

**g) Participación directa en las hostilidades.**

La participación directa en las hostilidades es otra cuestión que genera numerosas controversias en las nuevas formas de actuación en los conflictos (Artículos 51.3 del Protocolo adicional I y 13.3 del Protocolo adicional II).

Los civiles (a veces de forma individual tipo “lobo solitario”) podrían llevar a cabo ciberataques que tengan relación directa con las hostilidades, con los efectos ocasionados y a favor de una de las partes, por simpatizar con ellas.

El problema de estas acciones es la variable “tiempo”. Los expertos, mayoritariamente, consideran que la participación comprende desde el momento de la preparación de la misión hasta el final de la participación activa. Así, Rodríguez-Villasante afirma que “el carácter directo de la intervención se extiende a la preparación o al retorno desde el lugar atacado. Relacionado con esto, durante los conflictos de Irak y Afganistán se ha puesto de moda el concepto de “puerta giratoria” o “revolving door”, es decir, aquellos individuos que en un momento determinado deciden participar de forma activa en el conflicto. Por ejemplo, un individuo, que, movido por un sentimiento de odio, prepara un IED y lo coloca al paso de una patrulla. En este caso su intervención comprendería desde que prepara la bomba hasta que vuelve a su domicilio.

De la misma manera puede ocurrir con los ciberataques. Así, un hacker puede preparar un virus para ser introducido en el sistema informático que controla los procesos de una planta de depuración de aguas y que, al cabo de unos días, provoque muertos por envenenamiento entre la población. El inicio de la participación directa lo definiría el momento en que empieza a diseñar el virus informático, sin embargo, el final no queda claro. Se podría decir que acaba cuando lanza el virus, aunque los efectos se manifiesten después. Cabe también preguntarse si se le podría atacar, en el momento de conocer los efectos, aunque haya pasado ya un tiempo.

La mayoría del GIE acordó que los civiles retienen su estado civil, incluso si participan directamente en las hostilidades cibernéticos. Otros, como T. Ruys afirman que una vez han cesado sus actividades, habrían recuperado su estatus de civiles y sólo cabría detenerles y en ningún momento podrían ser atacados. Sin embargo, podríamos estar ante un abuso flagrante del estatuto de personas civiles.

4.3 Situación en Argentina.

Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas

Misión: Ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar.

Funciones:

Coordinar sus acciones con los Centros de Ciberdefensa de las Fuerzas Armadas.

Establecer los criterios rectores, a nivel del Instrumento Militar, para la determinación de infraestructuras críticas a ser protegidas.

Entender:

En el establecimiento de estándares y procedimientos de Ciberdefensa, criptografía e informática forense.

En la supervisión de los centros de respuesta de cada Fuerza Armada.

En el proceso de capacitación de personal propio.

En la organización y desarrollo de actividades académicas (foros, seminarios, simposios, etc.).

Intervenir:

En la elaboración, revisión y experimentación de Doctrina de Ciberdefensa.

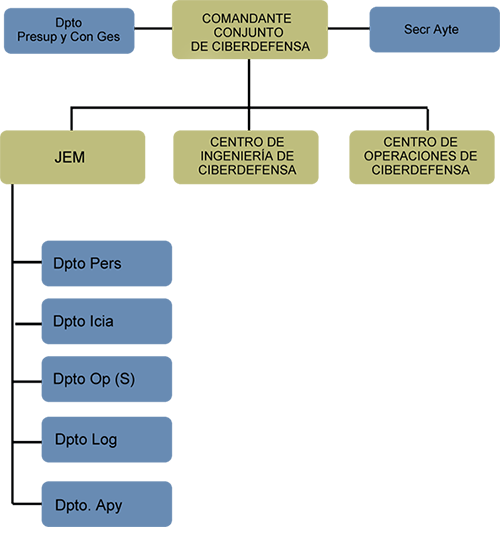
Participar:

A requerimiento del Ministerio de Defensa, en apoyo a otros Organismos.

En la concientización de las FF.AA. en materia de Ciberdefensa.

En la determinación y supervisión de los estándares de seguridad y certificación de protocolos afines en las FF.AA.

Estructura Orgánica



|  |  |  |
| --- | --- | --- |
| **Tipos de Ciberataques** | | |
| **Ransomware de SCI** | **Ciber-espionaje industrial** | **Ataques sobre tecnología inteligente embebida** | |
| Ataque basado en el cifrado de configuraciones de Sistemas de Control Industrial (SCI) que operan procesos físicos, como el tratamiento de agua, generación de energía, control aéreo, tráfico terrestre, fabricación de plástico.  Para pedir un rescate o colapsar un organismo, compañía o estado. | Ataque de espionaje con alto conocimiento, tanto interno, como externo, a través de tácticas de ingeniería social, y acceso continuo mediante múltiples canales correo, dispositivos móviles, web, red industrial, red corporativa. | Ataque a tecnologías inteligentes que disponen de sistemas embebidos que permiten la conexión con Internet y disponen de capacidad de procesamiento, almacenamiento y control. | |

|  |  |
| --- | --- |
| **Actores** | **Medidas** |
| Estado | |  |  |  | | --- | --- | --- | | Prevención:   |  | | --- | | * Establecer o favorecer canales de colaboración eficientes entre proveedores tecnológicos, proveedores de ciberseguridad, organizaciones industriales y CERTs para alerta temprana de este tipo de ciberdelitos. | | * Generar regulaciones con sanciones para las empresas que no tomen medidas de control para evitar incidentes, y sobre todo más severas para quienes no lo comuniquen adecuadamente. | | | Defensa:   |  | | --- | | * Fomentar la existencia de planes de recuperación y continuidad, así como gestión de cambios sobre los procesos físicos automatizados que garanticen la recuperación de las configuraciones. | | | Reacción:   |  | | --- | | * Dar participación a los especialistas miembros de las fuerzas de seguridad o áreas de inteligencia para analizar los incidentes con el fin de apremiar a quienes cometan estos delitos, y comprender si se trata de un incidente de seguridad aislado contra una empresa o una amenaza para el país. | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Proveedores tecnológicos | |  |  |  |  |  | | --- | --- | --- | --- | --- | | Prevención:   |  | | --- | | * Definir buenas prácticas para el resguardo de las configuraciones y archivos críticos de los sistemas. | | * Definir configuraciones de protección contra accesos y supervisión de los ficheros de configuración críticos de sistemas y aplicaciones. | | Definir y mantener canales de comunicación bidireccionales tanto con los CERT nacionales, las fuerzas de ciberseguridad nacional, como con las organizaciones industriales que son clientes directos de sus productos o servicios. | |  | | | Defensa:   |  | | --- | | * Trabajar de forma conjunta con otros proveedores para generar herramientas y configuraciones que permitan garantizar la integridad de los archivos de configuración, y evitar que sean accedidos por personas o procesos ajenos a los legítimamente autorizados. | | | Reacción:   |  | | --- | | * Analizar de forma conjunta con especialistas en el tema el comportamiento de éstos códigos maliciosos para definir y adecuar las medidas de prevención y defensa para las nuevas instalaciones, así como notificar sobre los cambios que deban realizar las organizaciones industriales cliente antes de que se vean afectados. | | |
| Organizaciones Industriales | |  |  |  |  | | --- | --- | --- | --- | | Prevención:   |  | | --- | | * Establecer planes de concienciación y formación. | | * Establecer planes de recuperación y continuidad sobre los procesos físicos automatizados que garanticen la recuperación de las configuraciones. | | * Definir planes y procedimientos de notificación y alerta temprana durante un incidente siguiendo los procedimientos establecidos, tanto dentro de la organización, como a nivel de los CERT nacionales y los proveedores tecnológicos. * Establecer una arquitectura de seguridad que permita detectar estos ataques de forma temprana (por ejemplo, IDS que contenga una alerta de detección de negociaciones de claves con servidores externos). | | | Defensa:   |  | | --- | | * Establecer, configurar, mantener y operar herramientas de supervisión y control sobre la integridad y accesos de los archivos críticos del sistema. * Establecer procedimientos de gestión de incidentes que contemplen su clasificación y una definición clara de roles y responsabilidades. | | | Reacción:   |  | | --- | | * Aplicación de los planes de recuperación y continuidad, así como la realización de un análisis forense y de comunicación del incidente. | | |

# 5-Conclusiones

Las formas de poder atacar y acceder a computadoras ajenos son muchas, hoy en día los administradores de sistemas son los encargados de proteger la seguridad de un servidor en línea, y cada uno de los usuarios son quienes deben protegerse de los ataques de algún hacker.

Las redes están formadas por miles de millones de nodos, de modo que si bombardean un país y con el miles de nodos, siempre existirán otros nodos para seguir manteniendo una comunicación abierta. Sin embargo, al crearlo no se tuvo en cuenta la ciberguerra ni el origen de los propios hackers. Un simple gusano puede colapsar la red en pocas horas y en el mejor de los casos, un simple virus puede ser enviado a millones de máquinas conectadas en todo el mundo

Queda claro que las amenazas Cibernéticas se encuentran en franco incremento. El rango de éstas va desde la actividad criminal tradicional del hurto y fraude, hasta el espionaje avanzado y daño a la información y el equipamiento. La Defensa Cibernética requiere de un esfuerzo político coordinado, a fin de establecer las estructuras legales, programas educacionales y de la capacidad institucional para responder a los acontecimientos que se presenten a lo largo del espectro de amenazas. El reto no es insuperable, pero requiere que las instituciones, empresarios y el gobierno inviertan tiempo y dinero. Muchos de los riesgos pueden ser reducidos significativamente, mediante la adopción e implementación rigurosa de algunas buenas prácticas. La tarea para los líderes está en reconocer los riesgos y disponer las acciones convenientes

Su alcance es mayor al de cualquier hecho delictivo convencional. Puesto que es posible que terroristas tengan objetivos como ser sistemas de control de energía, aeropuertos, red ferroviaria, redes de satélites, servicios de emergencia etc.

Este peligro obliga a los estados a poseer unos sistemas de seguridad, con grandes medios técnicos, personal muy bien entrenado para poder hacer frente a la amenaza, es necesario planes de contingencia y respuestas rápidas.

El problema afecta el bienestar digital de la sociedad, de las organizaciones y de los países y, en particular, afecta a las distintas dimensiones: política, social, económica, legal, justicia y policial y técnica. Los desafíos son complejos y afrontarlos requiere de la voluntad política para diseñar e implementar una estrategia global que incluya una estrategia de ciberseguridad coherente y efectiva. Se necesita una respuesta rápida, firme en el ámbito humano, legal, económica y tecnológica de las necesidades de seguridad de toda la sociedad.

Su alcance es mayor al de cualquier hecho delictivo convencional. Puesto que es posible que terroristas tengan objetivos como ser sistemas de control de energía, aeropuertos, red ferroviaria, redes de satélites, servicios de emergencia etc.

Este peligro obliga a los estados a poseer unos sistemas de seguridad, con grandes medios técnicos, personal muy bien entrenado para poder hacer frente a la amenaza, es necesario planes de contingencia y respuestas rápidas.

El problema afecta el bienestar digital de la sociedad, de las organizaciones y de los países y, en particular, afecta a las distintas dimensiones: política, social, económica, legal, justicia y policial y técnica. Los desafíos son complejos y afrontarlos, como se ha mencionado se quiere de la voluntad política para diseñar e implementar una estrategia global que incluya una estrategia de ciberseguridad coherente y efectiva. Se necesita una respuesta rápida, firme en el ámbito humano, legal, económica y tecnológica de las necesidades de seguridad de toda la sociedad.

Pese a todo lo que estamos mencionando de los aparentes peligros de internet, tiene que quedar claro que navegar por internet no es peligroso, ni se corre ningún riesgo al hacerlo. Muchas de las situaciones peligrosas se pueden evitar aplicando un mínimo de sentido común.

**Bibliografía**

* Instituto Español de Estudios Estratégicos (IEEE).
* Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas.
* LA CIBERGUERRA. GÉNESIS Y EVOLUCIÓN(<http://www.armada.mde.es>)
* McAfee en el punto de mira, las infraestructuras críticas en la era de la ciberguerra.

* <https://www.symantec.com/es/mx/page.jsp?id=stuxnet>

* <http://www.abc.es/tecnologia/redes/20150615/abci-ciberguerra-ciberataque-china-201506131801.html>

* <http://www.huffingtonpost.es/2017/02/07/ciberguerra-hackers_n_14248228.html>

* <https://actualidad.rt.com/actualidad/182812-estado-islamico-hackear-datos-eeuu>
* http://tecno.americaeconomia.com/articulos/ciberguerras-la-proxima-generacion-de-los-conflictos-internacionales