OCTUBRE 2022

ARMAS CIBERNÉTICAS

INTELIGENCIA VISUAL ANALÍTICA

GRUPO 3

Preparado por: Grupo 3
Para: Master Analista de Inteligencia

Índice

1.- Introducción

Las armas cibernéticas representan una amenaza para empresas, Estados y ciudadanos. En el ámbito empresarial, el desarrollo de armas cibernéticas ha abierto un espacio en el que delinquir en la red es sumamente variado y en el que confluyen numerosos intereses. En este sentido, las empresas lidian con delitos relacionados desde la estafa, el robo de información, el secuestro de datos, la destrucción de archivos, hasta el espionaje empresarial. Por otro lado, en el ámbito de los Estados, la guerra cibernética está ganando protagonismo y constituye un nuevo elemento desestabilizador para las relaciones internacionales. Así, las armas cibernéticas han abierto un nuevo paradigma en materia de defensa de los Estados, obligándolos a adaptarse al lanzamiento y respuesta de estas nuevas tecnologías.

La peligrosidad de las armas cibernéticas reside en su rápida distribución, su bajo coste y la exoneración de responsabilidad frente a estos ataques. Por ello, es esencial conocer su clasificación, tipología y objetivos; el mercado de las armas cibernéticas y su proliferación; cuáles son los retos para el derecho internacional; conocer su alcance mediante el estudio de casos y; reflexionar sobre el avance de esta tecnología y hacia qué tendencias apunta.

2.- Análisis

2.1.- Definiendo un arma cibernética

No existe una definición única de armas cibernéticas. En 2011, el Departamento de Defensa de los EE.UU. reconoció que "la naturaleza interconectada del ciberespacio plantea desafíos importantes para la aplicación de algunos de los marcos legales desarrollados para dominios físicos específicos" y que "actualmente no existe un consenso internacional con respecto a la definición de arma cibernética". La dualidad en las funciones de las armas cibernéticas (ataque o defensa, pacífica o agresiva, legal o ilegal) dificulta más aún lo mencionado.

De esta manera, existen diferentes aproximaciones que enfatizan unos u otros aspectos de dicho término. En el ámbito militar destaca la definición del Diccionario de Términos Militares Asociados del Departamento de Defensa de los EE.UU. en el que se menciona que un arma cibernética es aquella diseñada explícitamente para incapacitar al personal o material enemigo, al tiempo que se reducen las lesiones y muertes y los daños colaterales no deseados tanto a la propiedad como al medio ambiente.

El Manual de Tallín resalta los efectos derivados del uso de este tipo de armas definiéndolas como medios cibernéticos de guerra que se utilizan, diseñan o tienen la intención de ser utilizados para causar lesiones; la muerte de personas; daños o la destrucción de objetos. Destaca además que estas consecuencias son las requeridas para calificar a una operación cibernética como un ataque cibernético. Por su parte, Loïc Simonet y David Brown definen el concepto de arma cibernética equiparándolo al armamento menos convencional como las armas tipo NBQ o las armas cinéticas.

En el ámbito informático destacan las definiciones que incluyen el criterio de funcionalidad adoptado por la comunidad internacional en la Convención sobre Armas Biológicas y en la Convención sobre Armas Químicas. De esta manera, se entiende que un arma cibernética es un software y sistema de tecnología de la información que causa efectos destructivos a través de las redes TIC sin tener otro uso posible que no sea el mencionado. Este criterio establece la intención del usuario como requisito para considerar si una ciber herramienta es calificada como arma cibernética.

Esta última definición tiene ciertas limitaciones. Bajo su criterio, en caso de que una herramienta fuese empleada sin un fin destructivo, no sería calificada como arma cibernética. Este caso no se ajustaría a las definiciones que los Estados han otorgado a las actividades cibernéticas ofensivas y pone de manifiesto la amplia variedad de definiciones existentes para el concepto de arma cibernética y la necesidad de una definición consensuada en términos jurídicos o institucionales.

Pese a la carencia de lo mencionado, las armas cibernéticas poseen cinco elementos clave que distinguen este tipo de armas de un arma convencional: la descentralización de la capacidad, la ejecución no letal, la multifuncionalidad, la incertidumbre atribucional y la asimetría operativa.

La descentralización de la capacidad se refiere al bajo coste de su producción y a la consecuente deslocalización de ésta. Puesto que los requisitos para la construcción de un arma cibernética son escasos (tener un ordenador, conexión a internet y conocimientos avanzados de ingeniería informática), tanto estados como actores subestatales e incluso individuos aislados se convierten en actores relevantes en el escenario de producción.

Esta realidad otorga a las armas cibernéticas ventaja respecto a las armas convencionales en el ámbito de la producción puesto que estas últimas requieren grandes sumas de dinero y una cantidad elevada de personal y recursos físicos. Además, al contrario que con desarrolladores de armas convencionales, los grupos dedicados a las ciberarmas pueden trabajar en remoto (deslocalizándose) y compartir información sobre cómo crear malware en foros en línea. Esta escalabilidad difumina la línea entre las capacidades de actores estatales y las de los actores no estatales.

La ejecución no letal de las armas cibernéticas se refiere a la ausencia de tal objetivo en su uso, pero no a la ausencia de capacidad letal derivada de tal uso. Esto supone que los objetivos prioritarios son interrumpir, destruir o manipular sistemas o dispositivos informáticos. A consecuencia de tales objetivos pueden producirse daños materiales que conlleven a la pérdida humana. No obstante, tal hecho sería un subproducto de su uso y no el principal objetivo.

La multifuncionalidad de las armas cibernéticas también supone una ventaja respecto a las armas convencionales puesto que este tipo de armas tiene capacidad para ejecutar simultáneamente varias funciones. Realizadas dichas funciones, atribuir el origen del ataque es de alta complejidad gracias al anonimato que concede internet. De esta manera, la incertidumbre operacional se refiere a la dificultad de identificar al atacante y responder ante este.

Por último, las armas cibernéticas otorgan una ventaja asimétrica a los actores al tener la capacidad de socavar total o parcialmente la operatividad de una fuerza militar tradicional. Esto se traduce en que un actor inferior puede obtener ventaja sobre un sistema de armas convencional manipulando o desactivando el sistema de radar antes de un ataque aéreo que, debido a la velocidad de despliegue de un arma cibernética, dejaría poco tiempo de reacción.

2.2.- ¿Cómo se diferencian?

En la actualidad existe una amplia variedad de armas cibernéticas que surgen de dar respuesta a los objetivos de ataque de los estados. Al ser diseñadas en base a la tarea específica que van a desempeñar, los efectos de cada arma varían significativamente respecto a otra. Aquellas con mayor impacto en el estado enemigo son las que operan en el ámbito de la ciber inteligencia, puesto que al atacar a la información que el estado posee, atentan directamente contra su soberanía.

Una manera útil de clasificar los tipos de ciberarmas es según su modo de propagación, de ocultación, la tarea específica para la que fueron diseñados, o su estructura. Dicha clasificación se expone en la siguiente tabla:

Tipo de Malware:	Clasificación según:	Modo de actuación:
Virus	Paso 1: Modo de propagación	Se instala en el código de un programa ya existente y cuando este se ejecuta, se expande a otros programas. Altera el funcionamiento normal del dispositivo.
Gusanos Worms	Paso 1: Modo de propagación	Se instala en el código de un programa ya existente y desde allí se replican y difunden de manera autónoma. Modifica los servidores y los hace inoperativos.
Puerta trasera o Backdoor	Paso 2: Modo de ocultación	Configura vías de acceso alternativas por las que garantiza el acceso y control de la red
Rootkit	Paso 2: Modo de ocultación	Oculta la presencia de otro software malicioso ya instalado en el sistema
Troyano	Paso 2: Modo de ocultación	Utiliza su apariencia benigna para acceder al sistema y una vez dentro desempeña su función
Drive-by-downloads	Paso 2: Modo de ocultación	Accede al sistema cuando el usuario visita un sitio web infectado
Rogue antivirus	Paso 2: Modo de ocultación	Manda un mensaje al usuario ofreciendo un servicio de protección ficticio que lleva a la descarga del software

Spyware	Paso 3: Tarea específica	Recopilan datos sobre el comportamiento del usuario durante la navegación en internet
Adware	Paso 3: Tarea específica	Muestran al usuario ventanas emergentes con publicidad durante la navegación en internet
Keyloggers	Paso 3: Tarea específica	Registra todas las pulsaciones de teclado que realiza el usuario y las reporta al creador del software
Bots	Paso 3: Tarea específica	Incluye al ordenador infectado en una red de ordenadores zombies propiedad del creador del software. La funcionalidad del ordenador queda al servicio del creador del software
Ransomware	Paso 3: Tarea específica	Cifra los datos del disco duro del ordenador. A menudo se ofrece la devolución de estos a cambio de una cantidad de dinero acordada
Malvertising	Paso 3: Tarea específica	Deriva al usuario a una página web infectada
BHO	Paso 3: Tarea específica	Modifica el funcionamiento habitual del navegador al que infecta. Altera el funcionamiento del dispositivo
MitM	Paso 3: Tarea específica	Concede al creador del software control total sobre el equipo infectado
MitMo	Paso 3: Tarea específica	Variante del anterior utilizada en dispositivos móviles
Malware polimórfico	Paso 4: Estructura	Incluye funciones específicas para cambiar su fichero ejecutable de forma periódica
Malware metamórfico	Paso 4: Estructura	Cambia su código al propagarse

En el contexto de las guerras cibernéticas, los softwares expuestos suelen utilizarse para la violación de la privacidad del sujeto o de la soberanía del estado y para la destrucción de datos y/o el robo de propiedad intelectual. Las armas más empleadas para ello son el Ransomware y los ataques DDoS o ataques de día cero. Este tipo de ataques, producidos a través de un malware, hacen inaccesible el sistema atacado.

De acuerdo con Cárdenas (2022), los tipos de malware más utilizados en una ciberguerra serían los siguientes:

- Malware para Botnets: diseñados para infectar redes de sistemas en todo el mundo y utilizar éstos contra el propio enemigo.
- Malware para espionaje e inventario: diseñados para robar información enemiga, suelen utilizarse en el ámbito de la inteligencia y la defensa.
- Malware para control e inventario: construyen mapas sobre el inventario de infraestructuras críticas del enemigo como pueden ser el sistema eléctrico, el transporte aéreo o el sistema público sanitario. Tras ello, se autodestruyen.
- Malware de ataque a infraestructuras: atacan las anteriormente identificadas como infraestructuras críticas. Los objetivos suelen ser los sistemas SCADA, de control, de transporte, energético y de suministro.

2.3.- Objetivo de un ataque con arma cibernética

Las armas cibernéticas persiguen seis objetivos diferentes en el ámbito de la ciberguerra:

1. Espiar: las armas cibernéticas se usan para monitorizar a otros países con la intención de robar secretos o documentos confidenciales. Esto implica el uso de botnets o ataques de phishing selectivo para comprometer los sistemas informáticos confidenciales antes de acceder y filtrar la información.
2. Sabotear: los ataques con armas cibernéticas que sabotean los sistemas informáticos del gobierno pueden ser usados para apoyar los esfuerzos de guerra convencionales. Estos ataques pueden bloquear comunicaciones oficiales del gobierno, contaminar los sistemas digitales, permitir el robo de inteligencia o amenazar la seguridad nacional de forma global.
3. Ataques de denegación de servicio (DdoS): evitan que los usuarios legítimos accedan a un sitio web al inundarlo con solicitudes falsas y obligar al sitio web a manejar dichas solicitudes. Este tipo de ataque se puede utilizar para interrumpir operaciones y sistemas críticos y bloquear el acceso a sitios web confidenciales por parte de civiles, personal militar y de seguridad u organismos de investigación. Cuando estos ataques son lanzados por actores no estatales, se suelen considerar más a menudo una forma de hacktivismo político.
4. Desestabilización: consistente generalmente en ataques a infraestructuras críticas, incluidas entidades como sistemas de transporte, sistemas bancarios, redes eléctricas, suministros de agua, presas u hospitales. La adopción del internet de las cosas (IOT) hace que la exposición sea cada vez mayor. Desde una visión de seguridad nacional, la desestabilización de la infraestructura digital crítica inflige daños en los servicios o procesos modernos vitales. Por ejemplo, un ataque a la red de energía podría tener consecuencias masivas para los sectores industriales, comerciales y privados. También podría permitir a los atacantes deshabilitar sistemas críticos, interrumpir la infraestructura y potencialmente provocar daños globales. Además, estos ataques a la red eléctrica también pueden interrumpir las comunicaciones y dejar inutilizados y paralizados servicios tales como mensajes de texto y comunicaciones. Otro ejemplo de desestabilización es la provocada en el

sector económico, ya que la mayoría de los sistemas económicos modernos funcionan con ordenadores. Los atacantes pueden apuntar a las redes informáticas de la infraestructura económica, como mercados de valores, sistemas de pago o bancos, para robar dinero e impedir que las personas accedan a los fondos que necesitan.

5. Ataques previos a operaciones militares: se llevan a cabo ataques masivos, consiguiendo debilitar las defensas e infraestructuras críticas y desestabilizando el país parcial o completamente. Esta operación suele acontecer a un ataque cinético clásico en el contexto de la guerra híbrida.
6. Propaganda: se trata de un método barato y efectivo con el que se incorpora información masiva ya sea textual o visual de manera instantánea en el sistema operativo que se desee. En caso de provenir de un actor no estatal, se trataría de un arma cibernética utilizada para mostrar propaganda como método de hacktivismo.

Además de los objetivos específicos mencionados, destaca el objetivo macro perseguido por la mayoría de las armas cibernéticas: su capacidad disuasoria. Gracias a ella se mitiga la interferencia externa en asuntos nacionales y regionales. En esta línea, las armas cibernéticas tienen la capacidad de proyección de poder a un coste mínimo convirtiéndose en una fuerza igualadora entre estados con diferentes recursos.

2.4.- Protección de sistemas: la ciberseguridad

2.4.1.- Ciberseguridad y ciberdefensa, ¿son lo mismo?

El concepto de ciberseguridad es complementario al de ciberdefensa y materializa la defensa nacional digital. Sin embargo, el desarrollo de conceptos como el ciberterrorismo o el cibercrimen, cada vez más presentes en la sociedad, hacen fundamental la existencia de mecanismos exclusivos para la ciberdefensa. La ciberseguridad es la protección de sistemas conectados a través de una red, tales como hardware, software, y datos, de ciberamenazas. Esta práctica es usada por individuos y compañías para protegerse contra acceso no autorizado a centros de datos y otros sistemas.

La International Telecommunication Union (ITU), organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas, establece cinco elementos fundamentales para desarrollar las estrategias de ciberseguridad. Entre ellos se encuentra el desarrollo de un marco legal para la acción y de medidas técnicas o la aplicación de una cultura de Ciberseguridad y de cooperación internacional.

Una sólida estrategia de ciberseguridad proporciona un muro de defensa frente a ataques maliciosos diseñados para acceder, alterar, eliminar, destruir, y extorsionar a una organización o individuo a través de datos sensibles. La ciberseguridad es esencial en la prevención de ataques que deniegan el servicio de un sistema o un dispositivo. Y esto se aplica especialmente a los sistemas de instituciones gubernamentales.

En el caso de España, el Mando Conjunto de Ciberdefensa (MCCD) es el organismo encargado de garantizar un acceso libre al ciberespacio y de dar respuesta ante amenazas o agresiones que puedan afectar a la defensa nacional. También trabaja para garantizar la disponibilidad, integridad y confidencialidad de la información y coopera en materia de Ciberdefensa a nivel nacional.

En la actualidad, con cada vez un mayor número de usuarios, dispositivos, programas y un crecimiento exponencial de la cantidad y usabilidad de los datos, la ciberseguridad se establece como una parte necesaria dentro de cualquier organización. El creciente volumen y la sofisticación de los atacantes y sus técnicas incrementan más aún las dimensiones del problema.

2.4.2.- Campos de la ciberseguridad

La ciberseguridad es un amplio campo que cubre varias disciplinas, las cuales se pueden aglutinar en siete pilares principales.

2.4.2.1.- Seguridad de Redes

La mayoría de los ataques cibernéticos ocurren sobre la red, por lo que se han desarrollado herramientas para identificar y bloquear estos ataques entrantes. Las soluciones incluyen controles de acceso y datos como el Data Loss Prevention (DLP), Identity Access Management (IAM), Network Access Control (NAC), y Next-Generation Firewall (NGFW), aplicaciones para controlar y asegurar un uso seguro de la red, acorde a las políticas establecidas.

También existen tecnologías más avanzadas que permiten una red con múltiples capas que prevengan posibles amenazas, como el IPS (Intrusion Prevention System), NGAV (Next-gen Antiviurs), entornos Sandbox, y CDR (Content Disarm and Reconstruction). Otro de los puntos importantes son las herramientas para analizar métricas de la red, detectar amenazas y automatizar respuestas a través de un SOAR (Security Orchestration and Response).

2.4.2.2.- Seguridad en la Nube

La digitalización de la sociedad empuja a las empresas a compartir sus servicios en la nube. Este servicio ofrece mayor flexibilidad y capacidad para afrontar las necesidades actuales. No obstante, los peligros que supone este servicio convierten a la seguridad informática como un objetivo prioritario de dichas empresas.

Una correcta estrategia de seguridad incluye una serie de herramientas, políticas, controles y servicios que permitan proteger todo el contenido que la empresa expone en la nube en forma de aplicaciones, datos, infraestructuras, etc. Dichas herramientas pueden ser ofrecidas por proveedores de servicios o por terceros. A menudo las soluciones ofrecidas por los proveedores son insuficientes y es necesario acudir a las soluciones de terceros.

2.4.2.3.- Seguridad Endpoint

El modelo Zero-Trust prescribe la creación de micro segmentos alrededor de la localización de datos, independientemente de la ubicación de estos. Una manera de hacer esto con un cuerpo de empleados móvil es usar seguridad endpoint. Dicho método permite a las compañías asegurar dispositivos para el usuario final como pueden ser escritorios y portátiles mediante la protección de datos y de redes, la prevención avanzada de amenazas como el phishing o el Ransomware y el uso de tecnologías que proveen análisis forenses como las soluciones EDR (Endpoint Detection and Response).

2.4.2.4.- Seguridad móvil

A menudo sobreestimada, la seguridad en los dispositivos móviles como tabletas o smartphones es menos rígida de lo debido pese a tener acceso a datos corporativos. Estos dispositivos pueden estar sujetos a amenazas desde aplicaciones maliciosas, fallos del día de lanzamiento, phishing y ataques a través de mensajería instantánea. Cuando se incluyen estos dispositivos con un MDM (Mobile Device Management), las empresas pueden asegurarse de que sólo dispositivos con seguridad suficiente puedan acceder a los datos corporativos.

2.4.2.5.- Seguridad IoT

El término IoT (Internet of Things) se refiere a dispositivos interconectados que las empresas proveen a sus trabajadores como una de las vías para aumentar la producción. Sin embargo, esta conexión a la red aumenta la exposición ante posibles ciberamenazas. El objetivo criminales y hackers es encontrar dispositivos conectados carentes de protección que ofrezcan una ventana a la red corporativa.

La seguridad en los dispositivos IoT permite descubrir y clasificar los dispositivos conectados, auto segmentarlos para controlar la actividad de la red y usar IPS como parche para evitar la propagación de la amenaza. En algunos casos también se pueden incluir agentes en el firmware del dispositivo para evitar exploits y ataques entrantes.

2.4.2.6.- Application Security

Las aplicaciones web, al igual que el resto de herramientas conectadas a la red, son objetivo de hackers y criminales. A través de una correcta seguridad para la aplicación, se pueden prevenir ataques como los bots maliciosos, interacciones sospechosas con aplicaciones y APIs, incluso aunque el equipo de DevOps continúe lanzando nuevo contenido.

2.4.2.7.- Zero Trust

El modelo tradicional de seguridad está centrado en la protección sobre el perímetro mediante la construcción de muros alrededor de los activos más valiosos de la compañía, asemejando así la figura de un castillo. Sin embargo, esta concepción tiene varios problemas inherentes como las posibles amenazas internas y la rápida disolución del perímetro de la red una vez éste se tiene que agrandar.

Conforme los activos y la información corporativa se mueven entre la nube y fuera de la red debido al incremento del trabajo remoto, se hace necesario un nuevo acercamiento a la seguridad corporativa. Una solución es el modelo Zero Trust, el cual supone un acercamiento más granular a la seguridad protegiendo recursos individuales a través de la micro-segmentación, la monitorización, y la imposición de políticas restrictivas y controles de acceso para los empleados remotos.

2.4.3.- Servicios y productos en el mercado

Los fabricantes y vendedores en el ámbito de la ciberseguridad ofrecen una amplia gama de productos y servicios. Los sistemas de seguridad y herramientas más comunes incluyen:

- Identity and Access Management: (IAM)
    - Consiste en un marco de políticas y tecnologías para asegurar que los usuarios tengan un acceso acorde a su autorización. Este tipo de tecnología simplifica el día a día del usuario final, reduciendo posibles problemas que puedan surgir con las contraseñas y manteniendo un marco de seguridad.
- Firewalls
    - Se conoce como firewall al sistema de seguridad de redes que monitorea y controla el tráfico entrante y saliente entre dos redes. Aplicando reglas a dicho tráfico, el firewall logra establecer una barrera entre el tráfico fiable y el de origen desconocido.
- Endpoint Protection
    - Este tipo de producto proporciona control y seguridad sobre dispositivos que están conectados de manera remota a la red corporativa, protegiendo así los dispositivos de los empleados.
- Antimalware
    - Es un tipo de programa creado para proteger sistemas y dispositivos individuales, escaneando el dispositivo para prevenir, detectar, y remover malware.
- Intrusion Prevention/Detection Systems (IPS/IDS)
    - Consiste en un dispositivo o software que monitorea una red o sistema en busca de actividad maliciosa o violaciones de políticas de seguridad. Cualquier actividad intrusiva o violación de las políticas de seguridad detectada es reportada a un administrador o enviada a un SIEM que centralice los eventos y notificaciones de seguridad del sistema.
- Data Loss Prevention (DLP)
    - Esta tecnología permite detectar filtraciones, envíos indebidos o transmisiones de datos, bloqueando datos sensibles en su camino hacia el exterior. De esta manera, un empleado que quisiera enviar información confidencial por error, se encontraría con dicha limitación acompañada de una notificación al administrador del sistema.

- Endpoint detection and response
    - Se trata de una tecnología que de manera continua monitorea y controla los dispositivos endpoint, como ordenadores de empleados o dispositivos portátiles, para mitigar las amenazas.
- Security information and event management (SIEM)
    - Esta tecnología, fácilmente integrable con el resto de sistemas de seguridad corporativos, permite monitorear y obtener inteligencia sobre todos los eventos relacionados con la ciberseguridad que ocurran en el sistema. Gracias a su sistema de alerta y a los datos que recaba, se pueden mejorar los puntos débiles del sistema al proporcionar información forense sobre anteriores ciberamenazas.
- Encryption tools
    - Consiste en una serie de herramientas de diferente alcance que permiten prevenir el acceso no autorizado a la información digital, proporcionando una encriptación al archivo que impide su acceso sin la contraseña.
- Vulnerability scanners
    - Es un programa informático que analiza dispositivos, redes y aplicaciones para descubrir puntos débiles. Esto permite definir de manera más precisa las políticas corporativas necesarias para mantener la seguridad de su información antes de que se lleve a cabo un ataque sobre el sistema.
- Virtual Private Networks (VPNs)
    - Una red virtual privada permite un acceso alternativo a redes públicas o compartidas, ocultando las direcciones IP de los dispositivos conectados. Esto permite encriptar el tráfico entrante y saliente y, de esta manera, camuflar tu identidad online, dificultando el seguimiento y el robo de información.
- Cloud Workload Protection Platform (CWPP)
    - Esta tecnología permite mantener la seguridad en el traspaso de la información hacia la nube digital. Se centra en las cargas de trabajo de los entornos híbridos actuales, que combinan servicios en múltiples nubes, acorde a las necesidades de la empresa. Este software detecta y elimina las amenazas dentro del software de la nube, incluyendo protección activa, detección y eliminación de malware, y segmentación de las redes.
- Cloud Access Security Broker (CASB)
    - Consiste en un software integrado entre la infraestructura corporativa y la del proveedor del Cloud, que tiene como objetivo aumentar la seguridad informática, extendiendo el alcance de sus políticas.

Algunos de los fabricantes más conocidos son Check Point, Cisco, CrowdStrike, Fortinet, IBM, Imperva, McAfee, Microsoft, Palo Alto Networks, y Symantec, entre otros muchos.

2.4.4.- Evolución de las necesidades en ciberseguridad

Las amenazas actuales han variado significativamente respecto a las amenazas previas a la digitalización de la sociedad. Conforme el horizonte de amenazas cambia, las organizaciones necesitan protección frente a las herramientas actuales y futuras de los cibercriminales.

Hasta la fecha, las herramientas y tendencias de los cibercriminales se pueden aglutinar en cinco generaciones.

- Gen I (Virus): en los 80, la tendencia del ataque a dispositivos aislados a través de virus propició la aparición de las primeras soluciones antivirus.
- Gen II (Network): Conforme aparecieron las redes e Internet, los ciberataques a través de la misma se fueron acentuando. Esto inspiró la creación de protección perimetral a dichas redes, lo que generalmente se conoce como los firewalls.
- Gen III (Applications): El uso de exploits y vulnerabilidades en aplicaciones causó la adopción masiva de sistemas IPS (Intrusion Prevention Systems).
- Gen IV (Payload): conforme el malware se diversificaba y encontraba nuevas maneras de infiltrarse en los sistemas, los sistemas de defensa incluyeron sistemas anti-bot con soluciones sandbox capaces de detectar nuevas amenazas.
- Gen V (Mega): la última generación de ciberataques usa ataques multivectoriales a gran escala. Esto hace necesario las prevenciones y los sistemas de ciberseguridad.

Cada generación de ciberataques ha hecho que las anteriores soluciones sean menos eficaces e incluso queden obsoletas. Una correcta protección contra las ciberamenazas actuales incluye necesariamente soluciones de quinta generación.

2.4.5.- El Supply Chain Attack

Históricamente, los esfuerzos de muchas organizaciones han estado centrados en la protección de sus propias aplicaciones y sistemas. Incrementando la seguridad perimetral y permitiendo acceso únicamente a usuarios y aplicaciones autorizados, previenen la entrada de actores malignos en sus sistemas.

Sin embargo, conforme las empresas han reforzado sus lazos con otras empresas en cadenas de suministro más complejas, nuevas amenazas han surgido en el ciberespacio. Los cibercriminales están dispuestos a explotar no sólo las debilidades de una empresa, sino también las de sus proveedores y socios comerciales. A través de dichas relaciones comerciales, los criminales consiguen acceso a las redes de todos sus clientes y proveedores.

La protección contra ataques a proveedores y otras empresas de la cadena de suministro requiere un acercamiento Zero Trust. Mientras que los aliados y socios comerciales son buenos para el negocio, los usuarios y el software de terceros deberían tener limitado el acceso hasta el mínimo necesario para hacer su trabajo, mientras están suscritos a una monitorización continua.

2.4.6.- La necesidad de una arquitectura de ciberseguridad bien consolidada

En el pasado, las organizaciones de seguridad podían sobrevivir con un conjunto de soluciones de seguridad diseñadas para amenazas y casos de uso específicos. El malware era menos común y sofisticado y las infraestructuras corporativas menos complejas. En la actualidad, los equipos de ciberseguridad se encuentran a menudo abrumados mientras tratan de manejar y comprender las complejas arquitecturas de ciberseguridad.

Este cambio se debe a cuatro aspectos clave: la sofisticación de los ataques, la complejidad de los ecosistemas, la heterogeneidad de los Endpoints y el aumento del trabajo en remoto. Tratar de resolver todos estos desafíos con un conjunto de soluciones separadas es insostenible e imposible de escalar. Solamente a través de una arquitectura de seguridad consolidada puede una compañía protegerse ante las amenazas y los ataques.

2.5.- Marco legal

El marco legal de la ciberseguridad tiene luces y sombras según el ámbito de aplicación de la norma. En el ámbito del derecho nacional, la protección contra las armas cibernéticas goza de un marco legal específico y en constante actualización. En este sentido, alrededor del ámbito de la ciberseguridad entre empresas, ciudadanos y junto a la administración, se ha ido desarrollando un articulado legal que ha permitido acotar estas nuevas tecnologías. Aun así, la construcción de este marco legal no venía establecido en los códigos y derechos "tradicionales", sino que se trata de una materia que con el surgimiento de nuevas amenazas y modalidades de delitos e infracciones que superaban el plano físico y trascendían al universo digital, ha obligado al legislador a adaptar la normativa vigente con el dominio ciber.

De este modo, se pretende regular, amparar y proteger a los ciudadanos, empresas y a los propios Estados, contra la comisión de ataques cibernéticos en Internet. Por otro lado, en el ámbito del derecho internacional, los ataques cibernéticos y la ciberguerra no están recogidos por la norma internacional. Así, si bien los Estados a título individual y nacional han conseguido regular y actualizar su normativa en materia de delitos cibernéticos, el derecho internacional no consigue adaptarse a estas nuevas amenazas, dejando lugar simplemente a la interpretación de unas normas anquilosadas y redactadas en un contexto en el que aún no se tenía en cuenta el espacio cibernético.

La ciberseguridad es el ámbito sobre el que se pretende constituir un marco legal para proteger a personas u organismos frente a ataques o actuaciones ilegales o ilícitas de terceros en la red. Dichas actuaciones van desde una estafa online, el uso de armas cibernéticas, robo de cuentas personales, contraseñas de usuario, información personal y la suplantación de identidad hasta actos de ciberguerra. En este último comienzo de siglo, la expansión de internet y el implemento de nuevas tecnologías para cometer actos ilícitos en la red, han supuesto un antes y un después en las relaciones internacionales entre Estados. Los ataques cibernéticos han conseguido elevar los conflictos del plano físico al plano digital.

2.5.1.- ¿Cómo se entiende desde el derecho internacional?

Las herramientas que ofrece el Derecho Internacional para acotar el ámbito de las armas cibernéticas son escasas y atraen a la confusión. La norma primaria del Derecho Internacional es la Carta de Naciones Unidas. Sin embargo, si bien la Carta regula los aspectos de la guerra convencional, no ofrece las respuestas suficientes para los retos que las nuevas tecnologías plantean en el ámbito bélico. Por otro lado, si acudimos al Manual de Tallin, estudio académico dedicado a la aplicación del derecho internacional a los conflictos cibernéticos, llegamos a la conclusión de que se trata de una muy buena y útil aproximación a la materia, pero no deja ser un texto no vinculante para los Estados y, por lo tanto, carece de validez, aplicación y obligado cumplimiento.

El primer problema que presenta la Carta es la terminología jurídica. Las armas cibernéticas y todo el campo semántico relacionado con lo ciber no tienen cabida en ningún precepto de la Carta. En segundo lugar, aparece el problema de la atribución de los ciberataques. El principio de atribución en el Derecho Internacional es la operación jurídica necesaria para entender si una cierta conducta de uno o más individuos es reconducible a un Estado en concreto. En el ámbito ciber, por la dificultad que supone identificar al grupo, equipo y/o las personas que ejecutan el ataque cibernético, no es posible atribuir con toda seguridad la autoría de un ciberataque.

En tercer lugar, derivado del principio de atribución, el principio de responsabilidad internacional de los Estados. La responsabilidad internacional del Estado es un principio institucional en derecho internacional por el cual se impone al Estado que ha cometido un hecho ilícito en perjuicio de otro, la obligación de reparar el daño causado. En este sentido, la dificultad de probar este principio descansa en demostrar que el grupo de personas o la organización que haya realizado un ataque cibernético haya actuado bajo el paraguas de un Estado.

Este análisis indica que los instrumentos que ofrece en la actualidad el derecho internacional están desfasados y yacen insuficientes para combatir los actos de guerra cibernética entre Estados. Por ello, es necesario adoptar un nuevo estándar normativo adaptado a las nuevas tecnologías y a la era digital con la intención de establecer un marco preciso que permita atribuir a un Estado la responsabilidad de un ciberataque y, por otro lado, que cumpla con una función preventiva.

La función preventiva, principio jurídico tradicional, no está presente en el ámbito de los ciberataques en el derecho internacional. En sí, la función preventiva del derecho tiene por objetivo disuadir al delincuente de la acción punible que vaya a cometer y otorga seguridad jurídica. Dicho de otro modo, si no existen riesgos para los Estados y no son objeto de la aplicación de ninguna norma efectiva, los ataques cibernéticos no cesarán, dando pie a la creación y propagación de armas cibernéticas más peligrosas y de mayor alcance.

2.5.2.- ¿Cómo ha afectado a las relaciones internacionales?

El uso de armas cibernéticas ha supuesto una alteración del orden internacional. Por un lado, la ciberguerra se ha convertido en una extensión del conflicto sucedido en el plano físico. Así, los últimos conflictos internacionales (Rusia-Ucrania) muestran que el uso de armas cibernéticas en combinación con la estrategia militar llevada a cabo en el terreno físico constituye un nuevo modelo bélico operacional. En términos de escalada militar, el empleo de ciberataques ocupa un lugar protagonista en esta estrategia.

Por otro lado, está la cuestión de la soberanía de los Estados. Los actos de ciberguerra entre Estados persiguen un fin político: lesionar la soberanía de otro Estado. Las armas cibernéticas diseñadas para el robo de datos, el espionaje, el sabotaje o destinadas a entrar en el sistema de Inteligencia de un país (Pegasus), consiguen obtener información en la que reside la soberanía de un Estado. Además de la información relacionada con asuntos centrales del Estado (inteligencia), el otro tipo de información que es muy sensible para la estabilidad de un país es aquella relacionada con sus entidades e infraestructuras críticas (bancos centrales, sistemas sanitarios, energía, red telecomunicaciones y transportes, etc.).

De este modo, en un sistema cada vez más interconectado y dependiente de Internet, la protección de los intereses del Estado no ha conocido una dificultad técnica y tecnológica igual. El orden internacional, entendido como el sistema de normas organizativas, reglas, valores y costumbres, ha sido atropellado por la emergencia de las armas cibernéticas, materia que elude toda configuración jurídica.

2.6.- Situación del mercado de armas cibernéticas

La industria de las armas cibernéticas son los mercados y eventos asociados a la venta de armas cibernéticas y herramientas usadas para perpetrar ciberataques. El término podría extenderse al mercado negro y mercado gris, en línea y fuera de línea.

Las armas cibernéticas y el uso de ellas, produce una gran abertura en la seguridad de la información de los distintos países a nivel mundial. Esta realidad se acentúa cuando se trata de ciberarmas con gran nivel de perfeccionamiento y sofisticación. Alrededor de la compraventa de este tipo de armas a nivel mundial existe un gran mercado negro donde se pueden obtener las vulnerabilidades de un país en aquellas áreas susceptibles de ser atacadas. Este tipo de armas suponen una desestabilización para la seguridad de un estado con la ventaja sobre las armas tradicionales de tener menos coste, ser fácilmente distribuidas y tener consecuencias controladas. El último informe del Atlantic Council situó en 224 las empresas que venden armas cibernéticas, teniendo 27 de ellas sede en Israel.

Controlar las operaciones de mercado de extensión y proliferación de estas armas, es un determinante con mucho peso para la fluctuación de las relaciones entre Estados. Sobre esto último, algunos países más desarrollados en este área han sabido explotar este mercado. Entre los países que mayor explotación hacen de este tipo de mercado se encuentra Israel. El comercio en este sector fue muy importante para impulsar el crecimiento económico de dicho país y para el establecimiento de nuevas alianzas en buena parte del mundo, asegurándole la supervivencia en el escenario internacional.

Algunos factores que determinan las características del mercado existente en esta materia son:

- El mercado de la ciberseguridad y de las ciberarmas está siendo impulsado por el rápido crecimiento de los incidentes de ciberseguridad y las normativas que exigen la notificación de éstos. Según distintos estudios, los delitos cibernéticos, podrían costar al mundo un 0,8 % de PIB mundial. Se considera la guerra cibernética como una gran amenaza que puede superar incluso a la que representa el terrorismo. Los ataques cibernéticos generan muchas pérdidas económicas a los países, provocando una gran preocupación y dotando de intensidad el mercado que la rodea.
- El crecimiento de iniciativas de ciudades inteligentes demandará un alto uso de armas cibernéticas para la prevención.
- En la actualidad existe una gran dependencia de la tecnología de la información, conteniendo datos de gran sensibilidad para la seguridad de las organizaciones y las naciones. Este hecho ha contribuido al aumento de los atacantes cibernéticos cuyo objetivo es dañar al país en cuestión. Como consecuencia se multiplica el uso de estas herramientas para una buena defensa, lo que influye directamente en la actividad de mercado.
- El Informe de defensa digital de Microsoft (2021) recoge que alrededor del 80 % de los ataques se dirigieron a gobiernos, ONG y grupos de expertos. Los atacantes pueden explotar las conexiones entre las diferentes organizaciones que operan en un país, para conseguir información sobre las vulnerabilidades de las naciones.
- La Pandemia del COVID-19 también ha repercutido a este mercado. Debido al establecimiento de medidas de distancia social, la actividad cibernética ha crecido en intensidad y gravedad, debido a que las herramientas tradicionales para recopilar inteligencia no podían ser aplicadas. Este aumento de ataques cibernéticos ha derivado a su vez en el aumento de demanda de profesionales que operen en el sector de la ciberseguridad.

Como se ha observado, la actividad en el mercado existente alrededor del uso de este tipo de armas, tanto ofensivas como defensivas, es muy significativa. En 2020, el valor global de este mercado se estableció en unos 39 mil millones de dólares. Las previsiones futuras establecen un valor de 103 mil millones de dólares para el año 2016. Esto supondría una tasa de retorno de la inversión de aproximadamente un 17% para dicho periodo.

Otro factor a tener en cuenta es que en este mercado varios actores luchan por la cuota de mercado. Dichos actores tienen capacidades muy diferentes. Los más avanzados ofrecen tecnología avanzada como Aprendizaje Automático (IA) y disponen de una efectiva y potente estructura para su distribución. Estos líderes tecnológicos realizan grandes inversiones en innovaciones, fusiones y asociaciones para conservar una ventaja competitiva en el mercado. Como ejemplo de lo mencionado, en enero de 2020 Airbus Cybersecurity y Amossys firmaron un acuerdo de asociación y en julio de 2021 Leonardo y A2A se unieron para impulsar la ciberprotección de estructuras energéticas.

Entre las empresas más potentes que operan en la Guerra Cibernética se encuentran Bae Systems PLC, General Dynamic, Lockhedd Martin Corporation, Fire Eye Inc, The Boeing Company. En cuanto a los países, aquellos países con mayor tasa de mercado se encuentran englobados en América del Norte, los cuales alcanzaron la participación más alta en el año 2021. Dicha ventaja se explica de acuerdo a tres aspectos clave.

En primer lugar, se ha producido un incremento en el presupuesto para la defensa cibernética, lo cual impulsa el reforzamiento de la seguridad cibernética. En consecuencia, se han implantado poderosos sistemas de ciberseguridad dentro de las organizaciones que operan en los países y que son grandes impulsores del desarrollo empresarial. En segundo lugar, se han endurecido las penas por violaciones de la seguridad cibernética. Entre las medidas con las que cuenta el gobierno de EE. UU. destacan las ordenes ejecutivas mediante las cuales, los proveedores de software tienen que comunicar al gobierno federal cualquier violación de la seguridad cibernética a todos los niveles.

En tercer lugar, estos países forman parte de diferentes iniciativas contra los ataques cibernéticos y demuestran continuamente sus capacidades de guerra cibernética para reducir la sofisticación en los ataques que reciban. También participa en capacitación y desarrollo proactivos para su personal militar.

Paralelamente, se espera que el mercado cibernético de Asia Pacífico sea el que mayor crecimiento registre en los próximos años. Ello se debe a las recientes y crecientes amenazas a la seguridad de la región que están favoreciendo la evolución del sector. Concretamente, India ha sufrido un rápido crecimiento en delitos cibernéticos. Otro factor es la atribución a China del 30% de los ataques cibernéticos a nivel global que se han producido desde marzo de 2021. Al mismo tiempo, se ha producido un aumento del presupuesto derivado a este mercado en países como Corea del Sur con el objetivo de responder de manera más eficaz a las nuevas amenazas digitales.

2.7.- Ataques con éxito

2.7.1.- En el sector público:

2.7.1.1.- Stuxnet

Stuxnet es un gusano informático que penetró en el sistema de la planta nuclear de Natanz (Irán) en el año 2010. Su objetivo era causar el caos digital y la destrucción física de las instalaciones de la planta de enriquecimiento de uranio iraní. Introducido en el sistema informático de la planta a través de un USB infectado, el gusano informático viajó a través de los ordenadores para llegar al hardware que controlaban. A continuación, Stuxnet alteró los controladores lógicos programables (PLC) que interactuaban con las centrifugadoras responsables de la producción de material nuclear para su posterior fabricación de armas. El gusano modificó la velocidad de las centrifugadoras, haciendo que giraran demasiado rápido y durante más tiempo, provocando así que la maquinaria industrial fuera estropeándose hasta causar numerosas bajas en la planta. Esto retrasó el programa nuclear iraní puesto que además de causar daños físicos en los sistemas en los que se instalaba, el gusano era capaz de reprogramar los ordenadores y ordenar la autodestrucción de las centrifugadoras.

Por otro lado, enviaba información falsa al centro de control causando desconcierto entre los ingenieros iraníes que, ante el desplome continuo de sus centrifugadoras, no hallaban una explicación técnica relacionada con el error producido. En definitiva, Stuxnet fue un hito en la era de los ciberataques por la sutileza con la que operaba. La peligrosidad de Stuxnet radicaba en su capacidad de propagación y mutación. Y es que, aunque el virus se infiltró a través de un USB malicioso o un dispositivo de medios extraíble similar (el sistema que gestionaba el programa de enriquecimiento nuclear de Irán estaba aislado y desconectado de Internet), el gusano consiguió alcanzar ordenadores con conexión a Internet extendiéndose rápidamente a terceros.

Finalmente, tras meses de propagación en la planta nuclear y en otros dispositivos, el gusano fue advertido por un grupo de especialistas en ciberseguridad bielorrusos. Aunque las investigaciones no consiguieron apuntar directamente al responsable de la creación y difusión del malware, los indicios señalan que los autores del ciberataque fueron los Estados Unidos junto con Israel. Estos dos países, preocupados por la progresión que estaba tomando Irán en el desarrollo de su programa de armas nucleares, decidieron atacar la planta de enriquecimiento de uranio de una forma distinta a la convencional: un ataque discreto, anónimo y sin despliegue militar consiguiendo frenar la carrera armamentística de Irán. Este nivel de sofisticación en un ciberataque entre países no había conocido precedente antes de Stuxnet.

2.7.1.2.- NotPetya

NotPetya es un malware que atacó a los servicios esenciales e institucionales ucranianos en 2017. La ciberguerra encontró una forma de ejecución de alto nivel con NotPetya cuando hackers rusos quisieron intervenir en las finanzas de Ucrania, creando el malware para cifrar y destruir el contenido de los sistemas informáticos. Las principales entidades estatales ucranianas afectadas fueron el Banco Nacional de Ucrania (NBU), el metro de Kiev y los servicios informativos del Gobierno ucraniano. Junto con este malware, un programa de robo de contraseñas y un exploit, el ataque alcanzó al 10% de los dispositivos en Ucrania en tan solo 24 horas.

El malware provocó el cierre de bancos, puntos de venta y se paralizaron gran parte de las Administraciones públicas del país, quedando afectados también aeropuertos y líneas de ferrocarril, hospitales y oficinas de correos. Sin embargo, los daños de este virus siguieron trascendiendo y afectando gravemente a empresas navieras, farmacéuticas, de transporte, de construcción y alimentarias a nivel mundial provocando un caos logístico en puertos, cajeros automáticos y en la seguridad vial. El daño económico causado por el ciberataque fue valorado en más de 10.000 millones de dólares. Además de Ucrania, primer destinatario del ataque, el malware afectó -aunque en menor medida- a las infraestructuras y entidades estatales de países como Francia, Alemania, Reino Unido, Polonia, Italia y Estados Unidos.

NotPetya cifraba de forma permanente cualquier equipo infectado, siendo imposible deshacer el cifrado, aunque se pagara el rescate. Por ello, expertos en ciberseguridad concluyeron que el ataque no fue un intento de secuestro de información, sino que se trataba de un ciberataque patrocinado por un Estado, cuyo objetivo único era interrumpir y dañar los sistemas atacados en Ucrania: es considerado el ciberataque más destructivo conocido hasta la fecha. Aunque nunca se reconoció la autoría del ciberataque y se rechazaron las acusaciones, los líderes de los países afectados culparon a Rusia de la hostilidad del ataque.

2.7.2.- En el sector privado

2.7.2.1.- WannaCry

A mediados de mayo de 2017, el ciberataque denominado "WannaCry" infectó a más de 360.000 dispositivos electrónicos en más de 180 países, bloqueando e impidiendo su uso. Gran parte de estos dispositivos formaban parte de la red de diversas empresas, por lo que ha sido considerado como uno de los ataques cibernéticos en el sector privado más dañinos de la historia. La tipología de arma cibernética de este ataque se cataloga dentro de los Ransomware, dado que su fin era encriptar documentos en los ordenadores infectados para posteriormente solicitar el pago de una suma de dinero.

Si bien su alcance se cifró en los citados 360.000 equipos infectados según comunicados oficiales de organismos y empresas, otras fuentes amplían la extensión del alcance hasta los 15 millones entre infecciones y reinfecciones. Esta extensión a otros equipos se produjo gracias a la configuración de gusano que permitió escanear la red a la que el equipo infectado y extenderse a los equipos conectados al primero.

Tras la infección del equipo, el gusano encriptaba los archivos del dispositivo y mostraba una nota al usuario en la que se exigía el pago de 300 dólares a cambio de recuperar la información. Los países más afectados resultaron China, Rusia, Estados Unidos y Reino Unido.

El impacto de esta arma cibernética en el mundo empresarial tuvo varias vertientes.

- Impacto económico directo: recoge los costes de reparación y recuperación de los equipos infectados, así como de las horas de trabajo perdidas asociadas a dichas máquinas.
- Impacto indirecto: motivado por la inversión e implementación de medidas adicionales de seguridad para prevenir futuros ataques de la misma naturaleza, así como costes reputacionales, legales y financieros derivados de la infección.
- Impacto diferido: engloba los costes generados por el cambio en el comportamiento de los consumidores a raíz del ciberataque, así como por la alteración de la productividad por la inactividad del negocio.
- Impacto bursátil: la infección masiva de equipos dentro de una empresa supone un factor de riesgo que puede afectar al valor de la compañía en los mercados. El comportamiento de la Bolsa durante el viernes 12 de mayo, día del ataque, así como el rebrote del día 15, tuvieron un impacto significativo en la cotización bursátil de diversas empresas, si bien tras unas horas el mismo fue mitigado.

Cabe destacar que el impacto económico indirecto por actividad fue mitigado en gran medida por el "efecto viernes", dado que el grueso del ciberataque tuvo lugar dicho día de la semana, no suponiendo en gran medida horas de inactividad por indisponibilidad de los equipos.

A nivel global, el impacto económico por la infección con este Ransomware se cifra en más de 200 millones de dólares, resultando afectadas diversas empresas multinacionales como Renault, que se vio obligada a detener su producción en Francia, Eslovenia y Rumanía; FedEx en Estados Unidos, o Telefónica y Gas Natural en España. Adicionalmente, entidades del sector público como el Sistema de Salud Nacional británico, la policía estatal india o dos hospitales públicos de Yakarta también se vieron afectadas.

2.7.2.2.- Ataque sobre Saudi Aramco

A mediados de 2012, la compañía petrolífera Saudí Aramco, una de las más importantes a nivel mundial y productora de aproximadamente el 10% del crudo producido, sufrió uno de los ciberataques más devastadores de la historia. La propagación de un malware a través de la apertura por un operario de un correo de spam infectado desencadenó la pérdida parcial o total de información de 35.000 equipos de la compañía.

Un grupo autodenominado "Cutting Sword of Justice", cuya identidad nunca se desveló, reivindicó el ataque alegando el apoyo a la monarquía saudí por parte de la empresa petrolera. Las medidas adoptadas por la Compañía para evitar la propagación del malware se orientaron principalmente a la desconexión de la red de los equipos, resultando un aislamiento completo de cada una de las oficinas.

Si bien la actividad extractiva del crudo no se vio afectada directamente debido a la automatización de los sistemas, el resto de la actividad de la empresa si se vio directamente afectada por la desconexión de la red. Los efectos se produjeron en la gestión de suministros, el transporte o la gestión contractual con clientes.

Para solventar el problema, la compañía saudí contrató a un extenso equipo de consultores externos y envió a representantes a las principales fábricas de componentes informáticos del sudeste asiático para la compra de 50.000 discos duros que sustituyeran a los infectados. Esta compra masiva, realizada a mayor precio que el de mercado con el objetivo de conseguir preferencia en el suministro, tuvo afectó a la disponibilidad global de este componente electrónico, así como en su precio.

Finalmente, tras cinco meses de labores de reparación, la compañía pudo recuperar la actividad en sus sistemas informáticos. El coste directo para la compañía se estima en 38 mil millones de dólares, lo que le convierte en el ataque cibernético de mayor coste de la historia.

2.7.2.3.- Ataque a Sony Pictures

A finales de noviembre de 2014, se hizo pública la información sobre un ciberataque al estudio de cine Sony Pictures, uno de los más relevantes de la industria cinematográfica mundial. El ciberataque tuvo como consecuencia la imposibilidad por parte de los empleados de acceder a sus terminales, mensajes en diversas cuentas oficiales de twitter de algunas de las películas de la productora en las que aparecía el mensaje "Hackeado por #GOP" y amenazas a los altos ejecutivos de la compañía.

Durante aproximadamente una semana, se bloqueó el acceso a la red informática por parte de todos los trabajadores, generando importantes disrupciones en el funcionamiento normal de la productora. La repercusión principal del ciberataque resultó el robo de grandes cantidades de información, que incluía desde películas sin estrenar a comunicaciones entre empleados o datos personales de los mismos.

El grupo que reivindicó el ataque, autodenominados como GOP ("Guardians of Peace), demandó que no se estrenara la película "La entrevista", producida por el estudio, la cual versa sobre una operación por parte de la CIA para eliminar al líder norcoreano Kim Jong-Un.

Por este motivo, diversas fuentes entre las que se incluyen fuentes oficiales del gobierno de Estados Unidos apuntan a la conexión del grupo de atacantes con el régimen norcoreano. Asimismo, algunas partes del código malicioso con el cual se llevó a cabo el ataque se encontraban escritas en coreano, reforzando esta tesis como la más plausible. Sin embargo, destaca el hecho de que todas las evidencias que apoyan dicha tesis resultan circunstanciales.

2.8.- El ciberespacio en el conflicto entre Ucrania y Rusia

El ciberespacio, apoyado en un progreso tecnológico exponencial en los últimos años, se ha constituido como el quinto dominio, estando interconectado a los otros cuatro, estos físicos: tierra, mar, aire y espacio.

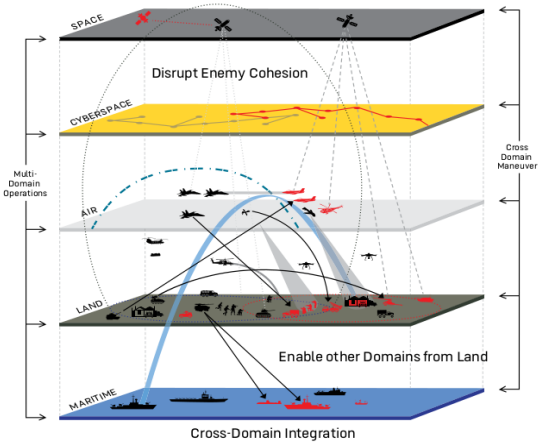

Ilustración 1 - Multidominio de un conflicto

El uso de armas cibernéticas en los últimos años ha proliferado en gran medida motivado por dos ventajas fundamentales: la dificultad para atribuir la autoría de los ataques y la asimetría de los mismos, dado que, con poca inversión en medios, se pueden lograr efectos dañinos multiplicadores. No obstante, hasta la invasión de Ucrania por parte de Rusia, la guerra cibernética no se había aplicado con anterioridad a un conflicto de estas magnitudes en el ámbito físico, resultando un ejemplo esclarecedor sobre el papel real en la actualidad de las armas cibernéticas a nivel global.

En las semanas previas al inicio de la ofensiva rusa, se incrementó de manera significativa el número de ataques cibernéticos dirigidos contra Ucrania, destacando el denominado

WhisperGate. Este caso se trata de un malware del tipo "wiper" muy similar al NotPetya en naturaleza, pero concebido para limitar su expansión al ámbito de Ucrania. Se detectó entre el 13 y el 15 de enero.

Ilustración 2 - Captura mensaje WhisperGate

La autoría de este malware se relaciona con los servicios de inteligencia rusos y su objetivo resultaba doble: técnico y psicológico. El ataque técnico tuvo como objetivo producir el mayor daño posible en la infraestructura tecnológica ucraniana. Por su parte, el ataque psicológico se produjo al introducir en los equipos infectados el mensaje "tengan miedo y esperen lo peor".

Asimismo, el 15 de febrero tuvo lugar una segunda gran oleada de ataques DDoS dirigidos contra la web del Ministerio de Defensa, el ejército y los dos bancos más importantes de Ucrania. El 23 de febrero, horas antes del comienzo de la ofensiva sobre suelo ucraniano, el Centro de Inteligencia de Amenazas de Microsoft detectó una tercera oleada de ciberataques ofensivos dirigidos contra la infraestructura digital de Ucrania.

El principal malware utilizado, bautizado como "FoxBlade" y desconocido hasta la fecha, tenía como objetivo diversos dispositivos de organizaciones pertenecientes a los sectores de la aviación, las tecnologías de la información, la defensa y el sector financiero. Estos ataques fueron mitigados por la multinacional tecnológica, dejando patente el papel relevante que ha de jugar la cooperación entre entes privados y públicos en las labores de ciberdefensa.

A la luz de estos hechos se identifica en el modus operandi dos fases claramente marcadas:

- La fase previa a la invasión física, comenzada el 13 de enero y cuyo principal objetivo resultó la preparación del entorno operacional, esto es, infundir confusión y temor entre la población civil ucraniana para debilitar su confianza en instituciones y dirigentes y menoscabar su voluntad de resistencia.
- Una segunda fase, iniciada de manera conjunta con la invasión física y llevada a cabo con herramientas cibernéticas similares a las de la fase preliminar, cuya intensidad se ha ajustado a lo largo del conflicto y sincronizado puntualmente con acciones del resto de ámbitos operacionales en el plano militar.

Cabe destacar que, previamente al estallido del conflicto, el historial de ciberataques rusos ya denotaba una alta agresividad y una eficaz coordinación de las capacidades del Estado, si bien la voluntad de no traspasar líneas rojas por parte del gobierno ruso limitaba en cierta medida su utilización. Sin embargo, tras el estallido del conflicto abierto en Ucrania y la dilución de los límites autoimpuestos por Rusia, se vaticinó en un primer momento en base al historial previo de ataques, una ciberguerra de profundas consecuencias, en las que un "ciber apagón" generalizado y de difícil solución se barajaba como uno de los peores escenarios.

No obstante, analizando el transcurso de los ciberataques conocidos por la opinión pública en el conflicto hasta la fecha, éstos han resultado de una complejidad técnica limitada, han causado efectos no duraderos y han estado supeditados en la mayoría de los casos a las operaciones desarrolladas en los otros cuatro dominios físicos. Las razones de esta menor predominancia de lo inicialmente esperado de las armas cibernéticas en el conflicto pueden ser múltiples.

En primer lugar, Rusia puede estar limitando el empleo de ciberarmas a gran escala en el conflicto para evitar que su propagación, muchas veces difícil de acotar, afecte a otros Estados que puedan tomar el ataque como un acto de guerra. Al mismo tiempo, Ucrania, tras el inicio del conflicto en 2014, ha reforzado en gran medida y de manera eficaz su infraestructura cibernética. Por último, el estado del arte del dominio cibernético aún no permite que un conflicto de alta intensidad se pueda librar predominantemente en este ámbito.

Se pueden extraer por lo tanto del conflicto de Ucrania conclusiones extrapolables a la situación global de las armas cibernética en la actualidad. Las armas cibernéticas han revolucionado diversos ámbitos relacionados con la seguridad como son la obtención de información, el espionaje, la guerra psicológica, campañas de desinformación o afección a infraestructuras tanto físicas como virtuales entre otros. Esto hace que su uso en un escenario prebélico y de zona gris sea extenso y acapare la mayoría de las acciones.

No obstante, su uso intensivo como dominio único en el que llevar a cabo una confrontación de alta intensidad no es factible en la actualidad, resultando por lo tanto un complemento más a las operaciones cinéticas desarrolladas en el resto de los dominios. Por último, es necesario destacar que el control del ámbito cibernético resulta en muchos casos un elemento determinante para la consecución de objetivos en el entorno físico por su efecto multiplicador de fuerzas y su transversalidad, por lo que es altamente probable que su relevancia sea creciente en conflictos posteriores.

3.- Tendencias y conclusiones

Las ciberarmas han experimentado un gran desarrollo en los últimos años a la luz de su utilidad en la ciberguerra, cuya principal conquista ha resultado pasar desapercibida para operar con mayor libertad y menor escrutinio.

Este gran desarrollo ha sido posibilitado por diversos factores. Por un lado, el avance exponencial de la tecnología ha permitido diseñar armas cibernéticas más eficaces, indetectables y adaptables al objetivo, convirtiéndolas en elemento esencial del arsenal de estados y organizaciones de todo tipo.

Por otro lado, un marco regulatorio y de derecho internacional difuso, así como la enorme dificultad que supone en muchos casos atribuir la autoría de los ciberataques, han fomentado su uso en gran medida.

Dicha naturaleza intrínseca de las ciberarmas deja patente el reto superior que suponen para los Estados, que tienen que desplegar no solo una ciberdefensa y cultura de la ciberseguridad eficaces, sino ser capaces también de entender los verdaderos actores, motivaciones e intereses que se esconden detrás de cada ciberataque.

Su uso ha cambiado asimismo las relaciones internacionales para siempre, dado que la información sensible entendida como datos de inteligencia, propiedad intelectual y capacidades estratégicas de defensa de los Estados, se encuentran más expuestas que nunca y bajo un riesgo constante de sustracción, sabotaje o desestabilización por la naturaleza permanente que ha adoptado la ciberguerra.

Cabe destacar que, si bien su desarrollo se ha potenciado en gran medida favorecido por un contexto sin grandes conflictos armados entre estados y con una zona gris cada vez más amplia que encajaba a la perfección con las capacidades y naturaleza de las ciberarmas, la guerra de Ucrania ha supuesto el primer demostrador a nivel global de las capacidades reales de la ciberguerra.

A este respecto, el ciberespacio se ha convertido en un dominio más en el que librar los enfrentamientos, con una característica que lo hace realmente diferenciador, la transversalidad al resto de dominios. Este hecho unido al uso indiscriminado y cada vez más eficaz que se observaba en el escenario prebélico, auguraba un papel relevante en el conflicto, si bien el desarrollo de los sucesos ha dejado patente que las ciberarmas han resultado únicamente un complemento al resto de operaciones físicas llevadas a cabo en el resto de dominios, teniendo gran predominancia el entorno cinético sobre el cibernético.

No obstante, es esta propia naturaleza transversal la que confiere a las ciberarmas la capacidad de ser el elemento diferenciador que permita el éxito operacional en el resto de dominios, lo que unido a otras características como la reducción del coste humano que pueden suponer, augura un mayor desarrollo y peso de las mismas en futuros conflictos.

Asimismo, la utilidad real de las ciberarmas, demostrada a través de varios ataques exitosos a entes públicos y privados, la experiencia de su uso en un conflicto a gran escala y la naturaleza

de elemento constante que ha adquirido la ciberguerra como expresión de las tensiones entre las naciones por ejercer su dominio e imponer sus intereses, marcan unas tendencias claras.

La cultura de la ciberseguridad será un aspecto que atraerá el esfuerzo y la inversión de Estados y empresas por la gran importancia que supone la prevención como medida eficaz para la defensa.

Por otro lado, será necesario seguir realizando un ejercicio profundo de identificación de todos los actores y partes interesadas que han de colaborar en la elaboración conjunta de la estrategia nacional de cada país, con especial importancia en la definición de atribuciones y responsabilidades.

En cuanto a la construcción de capacidades, se espera una continua mejora y desarrollo de las mismas por la propia dinámica mutacional del entorno virtual en el que operan las ciberarmas, con el objetivo de mantener la utilidad y poder de disuasión de las mismas.

Por último, el carácter irregular, asimétrico y descentralizado de las ciberarmas, así como su capacidad de propagación al ámbito supranacional, implicará relaciones y acciones conjuntas entre gobiernos de distintos países y entre actores estatales y privados, como demuestra el papel fundamental que ha tenido la multinacional Microsoft en la mitigación de diversos ciberataques durante el conflicto de Ucrania.

4.- Referencias

Blog FTP. (8 de abril de 2021). *Los tipos de malware más importantes en la actualidad*. Obtenido de Grupo FTP: https://www.grupoftp.com/noticias/tipos-de-malware/

Generalitat Valenciana. Conselleria d´Hisenda i Model Econòmic. (2018). Introducción al malware. Valencia, Comunidad de Valencia, España. Obtenido de mestreacasa.gva.es: https://mestreacasa.gva.es/c/document_library/get_file?folderId=500021663486&name=DLFE-1810399.pdf

HornetSecurity. (2022). *Malware ¿Qué es malware? ¿Qué tipos de malware hay?* Obtenido de HornetSecurity: https://www.hornetsecurity.com/es/knowledge-base/malware/?_adin=02021864894

Jose Cardenas, M. (13 de mayo de 2022). *Otras ciberarmas más allá de Pegasus*. Obtenido de LISA News: https://www.lisanews.org/ciberseguridad/las-otras-ciberarmas-mas-alla-de-pegasus/

Robles Carrillo, M. (3 de octubre de 2016). *El concepto de arma cibernética en el marco internacional: una aproximación funcional*. Obtenido de Instituto Español de Estudios Estratégicos: https://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO101-2016_Arma_Cibernetica_MargaritaRobles.pdf

Robles Carrillo, M. (3 de octubre de 2016). *El concepto de arma cibernética en el marco internacional: una aproximación funcional*. Obtenido de Instituto Español de Estudios Estratégicos: https://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO101-2016_Arma_Cibernetica_MargaritaRobles.pdf

Robles Carrillo, M. (2016). *Instituto Español de Estudios Estratégicos.* Obtenido de ieee.es: https://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO101-2016_Arma_Cibernetica_MargaritaRobles.pdf

Vicerrectorado de Tecnologías de la Información y la Comunicación y Universidad Digital. (enero de 2018). Guias de Seguridad UJA. Software malicioso (malware). Jaén, Andalucía, España.

Cubeiro Cabello, E. (2022). *Instituto Español de Estudios Estratégicos.* Obtenido de https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO32_2022_ENRCUB_Ucrania.pdf

Microsoft (2022). *Defending Ukraine: Early Lessons from the Cyber War.* Obtenido de https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK

Buxton, O. (16 de agosto de 2022). *Stuxnet: ¿Qué es y cómo funciona?*. Obtenido de Avast Academy: https://www.avast.com/es-es/c-stuxnet

Cocchini, A. (02 de marzo de 2021). *Ciberdiligencia debida: ¿una actualización necesaria para el Derecho Internacional del ciberespacio?.* Obtenido de Real Instituto Elcano: https://www.realinstitutoelcano.org/analisis/ciberdiligencia-debida-una-actualizacion-necesaria-para-el-derecho-internacional-del-ciberespacio/

Pérez Sierra, I. (28 de mayo de 2021). *La legítima defensa del Estado frente a ataques cibernéticos según el Derecho internacional.* Obtenido de Global Strategy: https://global-strategy.org/la-legitima-defensa-del-estado-frente-a-ataques-ciberneticos-segun-el-derecho-internacional/

Przetacznik, J. & Tarpova, S. (junio 2022). Russia's war on Ukraine: Timeline of cyber-attacks. Obtenido de Parlamento Europeo: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Consejo Europeo. *Ciberseguridad: cómo combate la UE las amenazas cibernéticas.* Consultado en: https://www.consilium.europa.eu/es/policies/cybersecurity/

Octubre 2022
Inteligencia Visual Analítica

Preparado por: Grupo 3
Para: Master Analista de Inteligencia