Tomás Illuminati

Ciberconflictos

Sin fronteras

UN ENFOQUE INTRODUCTORIO

Ciberconflictos: Sin Fronteras

Por Tomás Illuminati

Índice

Introducción

"La guerra es un fenómeno permanente que adapta su forma a medida que emergen nuevas formas de manifestar el poder".

A lo largo de la historia humana, hemos sido testigos de cómo las conquistas han evolucionado, impulsadas por la necesidad de controlar territorios y recursos en constante cambio. La tecnología ha desempeñado un papel crucial en estas transformaciones, alterando el panorama de los conflictos y otorgando ventajas a aquellos que se mantienen a la vanguardia. Desde el uso de armas de bronce en la antigüedad hasta las sofisticadas tecnologías de la era moderna, cada innovación ha redefinido las estrategias y tácticas de la guerra.

En la era actual, nos enfrentamos a una guerra que, en gran medida, transcurre de manera invisible para la mayoría de las personas. Se trata de una batalla por el control absoluto del ciberespacio, cuyas consecuencias podrían ser catastróficas, a pesar de que muchos ignoren su existencia. Esta guerra, que afecta a todo el mundo, se ha gestado en el intento de dominar un nuevo espacio: la red global de comunicaciones y los datos que alberga. Es una nueva carrera armamentista, dónde el poder se disputa a través de la tecnología y la información.

La guerra digital se libra en múltiples frentes, desde ataques dirigidos a infraestructuras críticas hasta campañas de desinformación masiva en las redes sociales. Los actores involucrados pueden ser estados nacionales, grupos terroristas, organizaciones delictivas o incluso individuos con habilidades técnicas avanzadas. Desde la seguridad nacional y la estabilidad económica hasta la privacidad

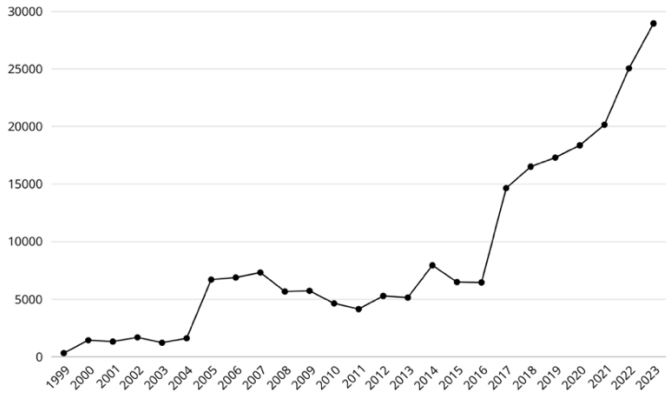
individual y la integridad de las instituciones democráticas, ningún ámbito queda exento de su influencia.

La importancia de proteger el ciberespacio no puede subestimarse. A medida que las sociedades se digitalizan, la interdependencia de sistemas y redes aumenta, haciendo que los ciberataques tengan el potencial de causar interrupciones generalizadas. Esto incluye desde el robo de información confidencial hasta la manipulación de sistemas críticos que pueden afectar la vida cotidiana de millones de personas.

A su vez podemos ver que nuestros sistemas informáticos, parten de una máxima de la ciberseguridad como es “NINGÚN SISTEMA ES SEGURO”. Entendemos las posibilidades que tienen los distintos actores para adentrarse a sistemas informáticos, mediante las vulnerabilidades existentes y aquellas que aún no han sido descubiertas, o que lo fueron y se mantienen en secreto por organizaciones estatales o no estatales que las utilizan como posibles ciberarmas. Y es que si vislumbramos un gráfico de cuantas vulnerabilidades se descubren por año, podemos observar, que no es algo extraño que exista la posibilidad de que distintos actores se aprovechen de ellas para cometer sus acciones.

Cantidad de CVE por años

Esta gráfico muestra la cantidad de CVE (Common Vulnerabilities and Exposures) clasificados por año



Fuente: CVE Site - https://www.cve.org

(El gráfico proporcionado termina en 2023, dado que aún no se tiene la totalidad del año 2024)

Además, la naturaleza del ciberespacio ofrece una cobertura ideal para los atacantes. La capacidad de lanzar ataques desde cualquier parte del mundo, a menudo utilizando técnicas que ocultan su identidad y ubicación, presenta un desafío significativo para la defensa y la atribución. Los perpetradores pueden enmascarar sus acciones detrás de proxies y redes de anonimato, haciendo que la tarea de rastrear y detener estas actividades sea increíblemente compleja.

La creciente interconexión de dispositivos a través del Internet de las Cosas (IoT) ha ampliado el campo de batalla, brindando nuevas oportunidades para los ciberdelincuentes y aumentando la vulnerabilidad de infraestructuras críticas como sistemas de energía, transporte y salud. La proliferación de dispositivos conectados, desde electrodomésticos inteligentes hasta vehículos autónomos, ha creado un entorno en el que casi cualquier aspecto de la vida moderna puede ser un objetivo potencial.

En este contexto, la ciberseguridad se convierte en una prioridad urgente. Proteger nuestra infraestructura digital requiere no solo de medidas técnicas, como el desarrollo de sistemas de defensa avanzados y la implementación de protocolos de seguridad robustos, sino también un cambio cultural que promueva la conciencia y la educación en materia de ciberseguridad en todos los niveles de la sociedad. La formación y sensibilización de la población en general, así como la capacitación especializada para profesionales en el campo, son esenciales para construir una defensa eficaz contra las ciberamenazas.

Este texto pretende sacar a la luz estos ciberconflictos que vivimos en la actualidad, una guerra que trasciende fronteras y que tiene el potencial de moldear nuestro futuro de manera significativa. A medida que avanzamos hacia un mundo cada vez más digitalizado, es crucial comprender las dinámicas de estos conflictos y desarrollar estrategias que nos permitan enfrentar las amenazas emergentes de manera efectiva.

Los métodos de combate en esta guerra digital son tan variados como sofisticados, desde malware diseñado para infiltrarse en sistemas y robar información confidencial, hasta técnicas de ingeniería social que manipulan a individuos para obtener acceso a redes protegidas. Los ataques pueden tener objetivos políticos, económicos o simplemente buscar sembrar el caos y la desconfianza en la sociedad. La sofisticación de estos ataques refleja la creciente profesionalización de los actores involucrados, quienes utilizan herramientas y técnicas cada vez más avanzadas para lograr sus objetivos.

El papel de los estados en el ciberespacio también merece una consideración especial. Gobiernos de todo el mundo han desarrollado capacidades cibernéticas ofensivas y defensivas como parte de su arsenal estratégico. Esto incluye desde la creación de unidades militares especializadas en ciberoperaciones, hasta la implementación de políticas y marcos legales destinados a regular y proteger el ciberespacio. La competencia entre naciones en este ámbito puede llevar a un aumento en la frecuencia y severidad de los ataques, a medida que cada país busca afirmar su dominio y proteger sus intereses.

Sin embargo, no solo los estados son actores clave en el ciberespacio. Organizaciones criminales, grupos terroristas y hacktivistas también juegan roles significativos. Estos actores pueden operar con distintos niveles de sofisticación y

motivación, desde el lucro económico hasta la promoción de agendas ideológicas. La diversidad de actores y objetivos en el ciberespacio crea un entorno complejo y dinámico, donde las amenazas pueden surgir de múltiples direcciones y con distintos grados de impacto.

La interconexión global y la dependencia de la tecnología han creado un escenario en el que la ciberseguridad no puede ser vista como una preocupación aislada de los expertos en tecnología. Es un problema que afecta a todos los sectores de la sociedad y requiere una respuesta coordinada y multifacética.

En este texto describiremos aquellas problemáticas más importantes y abordaremos de manera clara ejemplos de los casos ocurridos anteriormente.

I - Un mundo interconectado

Para comenzar debemos hablar sobre la red de redes, aquella que es el escenario de esta guerra actual, con esto nos referimos a Internet, el cual en sus inicios, no fue concebida como una red pública para el uso cotidiano de las personas. Su origen se remonta a un proyecto del Departamento de Defensa de los Estados Unidos destinado a facilitar las comunicaciones militares y académicas. Surgió como respuesta a la necesidad de establecer un sistema de comunicación descentralizado que pudiera resistir posibles interrupciones, incluso ante la devastación provocada por un ataque nuclear.

El contexto de la Guerra Fría y la carrera tecnológica con la Unión Soviética fueron el telón de fondo de este proyecto. Tras el lanzamiento del Sputnik en 1957, que puso de manifiesto la capacidad tecnológica de la Unión Soviética, el presidente Eisenhower ordenó la creación de la Agencia de Proyectos de Investigación Avanzada (ARPA) en 1958 para impulsar la investigación y el desarrollo en áreas estratégicas, incluyendo las comunicaciones.

La primera señal visible de lo que sería Internet se produjo en 1969, cuando se logró establecer una conexión de datos entre la Universidad de California en Los Ángeles (UCLA) y el Instituto de Investigación de Stanford (SRI), utilizando una tecnología innovadora de conmutación de paquetes. Esta conexión marcó el nacimiento de ARPANET, la primera red de computadoras descentralizada.

A lo largo de la década de 1970, ARPANET se expandió más allá de las fronteras de los Estados Unidos, con la incorporación de nodos en Europa a través del cable transatlántico. Esta expansión marcó el inicio de Internet como una red global e

interconectada, sentando las bases para la revolución digital que transformaría el mundo en las décadas siguientes.

El impacto de Internet en la sociedad y la tecnología ha sido monumental desde sus modestos comienzos en la década de 1960. Desde ARPANET hasta la Internet moderna, la red ha experimentado una expansión impresionante y ha transformado casi todos los aspectos de nuestras vidas.

En la actualidad, Internet es mucho más que una red de computadoras interconectadas. Se ha convertido en un vasto ecosistema digital que abarca desde la comunicación instantánea hasta el comercio electrónico, la educación en línea, el entretenimiento digital y la gestión de datos a gran escala. Pero sobre todo, se ha convertido en el actual campo de batalla de una guerra en constante crecimiento.

La realidad a día de hoy es que la conectividad que ofrece Internet nos ha permitido romper las barreras internacionales en cuestión de segundos, logrando así comunicarnos con cualquier parte del mundo sin importar nuestra ubicación. Pero esto a su vez ha traído consecuencias negativas, y es que a medida que el mundo se ha digitalizado, nuestra información también. Todos nuestros datos e información se encuentran almacenados en centros masivos, desde registros públicos hasta aquella información que brindamos de manera voluntaria. Pero, ¿qué tiene de negativo esto?

“Quien tiene la información, tiene el poder”. Con esto nos referimos a que aquellos que controlan la información, “nuestra información”, tienen un poder sobre nosotros. El control sobre la información ha sido siempre una herramienta poderosa en manos de gobiernos, empresas y otros actores. La capacidad de recopilar, analizar y utilizar

datos personales ha llevado a preocupaciones sobre la privacidad y la seguridad de los individuos en la era digital.

Esto puede recordarnos a un mundo similar al planteado en la obra "1984" de George Orwell, en donde el gobierno totalitario controla cada aspecto de la vida de los ciudadanos, incluyendo su información personal y sus pensamientos. En esta distopía, la vigilancia constante y la manipulación de la verdad son herramientas fundamentales para mantener el poder.

Pero lejos de ser simple ficción, en el mundo actual la tecnología ha avanzado a un ritmo increíblemente rápido, lo que ha permitido una recopilación masiva de datos en una escala nunca antes vista. Las redes sociales, los dispositivos inteligentes, las cámaras de seguridad y otras tecnologías recopilan constantemente información sobre nuestras actividades, preferencias y relaciones. Esta información puede ser utilizada para diversos fines, desde publicidad dirigida hasta la vigilancia masiva.

A su vez en la actualidad, esta información no es solo recopilada por un actor de manera autoritaria como ocurría en "1984". En palabras del filósofo surcoreano Byung-Chul Han, "La entrega de datos no sucede por coacción, sino por una necesidad interna"[1], y es que mediante los servicios que utilizamos diariamente entregamos nuestra información voluntariamente a cambio de obtener gratis ese servicio. Esta información que entregamos se posiciona como uno de los activo más valioso de cualquier empresa y estado, los datos que posee son el nuevo petróleo u oro negro, que generan el poder en estas.

[1] Byung-Chul Han. (2014). Psicopolítica. Herder

Aunque aquí surge una problemática y es que aquellos datos recopilados presentan un recurso valioso para los estados y empresas, pero a su vez un objetivo para aquellos actores maliciosos que desean hacerse con ellos.

Pero, ¿es esta la única problemática que genera la digitalización? Definitivamente no. Como se mencionó anteriormente, todo se ha digitalizado, incluida la información confidencial sobre la seguridad interna de los estados, la cual ahora circula por las redes privadas que mantienen estos organismos y se almacena de manera digital. Esta información altamente sensible resulta de gran interés para actores externos, tanto estatales como no estatales, que buscan obtenerla.

La preocupación por la seguridad nacional ante la digitalización de información sensible es solo una parte del problema. Otro gran fenómeno es el de las campañas de desinformación masiva, que permiten sembrar el caos de manera generalizada al manipular la información que llega al público.

Además, los países dependen de infraestructuras críticas que permiten el correcto funcionamiento de la sociedad, como las redes eléctricas, sistemas de agua y transporte. Estas infraestructuras están mayoritariamente informatizadas y, aunque cuentan con altas normativas de seguridad, debemos recordar que ningún sistema está siempre a salvo.

La digitalización de las infraestructuras críticas, aunque ha traído consigo avances significativos en eficiencia y gestión, también ha expuesto a los países a vulnerabilidades sin precedentes. Los sistemas de energía, transporte, comunicaciones, salud y finanzas, entre otros, están interconectados y dependen en gran medida de la tecnología digital para operar. Esto los hace susceptibles a

ciberataques que pueden tener consecuencias devastadoras. Un claro ejemplo de esto es la infraestructura digital de los hospitales, los cuales en su mayoría cuentan con sistemas operativos obsoletos o no actualizados. Esto presenta grandes complicaciones, dado que son aquellos los que albergan información confidencial de los pacientes y al no estar actualizados se vuelven susceptibles a ataques que permitirían el robo de dicha información.

La falta de actualización de los sistemas hospitalarios no solo expone datos sensibles, sino que también podría comprometer la prestación misma de servicios médicos. Imaginemos un escenario donde un hospital sufre un ciberataque que paraliza sus sistemas de registro de pacientes o incluso sus equipos médicos conectados a la red. Esto no solo pone en riesgo la privacidad de los pacientes, sino que también puede afectar su atención médica directa.

Los ciberataques pueden ser perpetrados por actores estatales, grupos terroristas, organizaciones criminales o incluso individuos con habilidades técnicas, actores de los cuales hablaremos más adelante. Estos pueden tener como objetivo robar información confidencial, interrumpir servicios vitales, causar daños físicos o desestabilizar la infraestructura de un país. La amenaza cibernética es una realidad que los gobiernos y las organizaciones deben abordar de manera proactiva y continua.

La creciente sofisticación de los ciberataques ha llevado a un incremento en la inversión en ciberseguridad por parte de gobiernos, empresas y organizaciones internacionales. Se han desarrollado estrategias de defensa, marcos de trabajo de seguridad, dispositivos especializados como firewalls, sistemas de detección de intrusiones y difusión a la población mediante programas de concientización sobre

seguridad para el personal. Sin embargo, la naturaleza cambiante y adaptable de las ciberamenazas significa que la seguridad nunca puede ser garantizada al cien por ciento.

Además de la preocupación por los ciberataques dirigidos a infraestructuras críticas, también existe la amenaza del ciberespionaje y la ciberguerra entre naciones. Los estados han desarrollado capacidades ofensivas en el ámbito digital, utilizando técnicas de hackeo y sabotaje para obtener información clasificada, interrumpir las operaciones del enemigo y socavar su capacidad de defensa

Las ciberguerras pueden tener consecuencias igualmente devastadoras que las guerras convencionales, pero con la ventaja para los actores que las emplean de que pueden llevarse a cabo de manera encubierta y sin necesidad de desplegar tropas en el terreno.

Uno de los aspectos más preocupantes de la ciberguerra es la dificultad para atribuir los ataques a un actor específico. A diferencia de las guerras convencionales, donde los uniformes y las banderas identifican a los participantes, en el ciberespacio es fácil para los perpetradores ocultar su verdadera identidad detrás de múltiples capas de anonimato y falsificación. Además, la naturaleza transnacional de Internet dificulta la aplicación efectiva de las leyes y normas internacionales.

II - Actores en la sombra

Como mencionamos en el capítulo anterior, las guerras siempre han tenido algo en específico, y es que es fácil reconocer a los participantes de ellas. Ya sea por sus uniformes, banderas, lenguaje, historia, etc. Pero la guerra en el mundo digital presenta una problemática ante esto, y es que aquellos actores que participan suelen ser desconocidos y por lo menos difíciles de identificar a simple vista. En la mayoría de los casos se logra, hasta luego de una investigación o cuando estos se atribuyen públicamente el ataque.

Esto se debe por ejemplo, a la posibilidad de que el atacante pertenezca a un cierto país como puede ser Rusia, que el ataque provenga desde un servidor en Suiza y que el objetivo esté en Estados Unidos. Lo que complica aún más la identificación es la capacidad de ocultar la verdadera ubicación y origen del ataque mediante técnicas como el enmascaramiento de direcciones IP, el uso de servidores proxy y la manipulación de datos de geolocalización. Esto significa que, a diferencia de las guerras convencionales donde las identidades y afiliaciones de los participantes suelen ser más transparentes, en el ciberespacio es difícil determinar quién está detrás de un ataque.

En la actualidad estos actores maliciosos han sido clasificados en cinco posibles grupos, actores estatales o patrocinados por el estado, hacktivistas, ciberterroristas, delincuencia organizada y civiles con conocimientos en el área que buscan realizar ataques.

Comenzando por aquellos que son parte clave del arsenal de cada país tenemos a los actores estatales, quienes son respaldados y financiados por gobiernos para llevar a cabo acciones cibernéticas con objetivos políticos, económicos o militares. Estos actores cuentan con recursos significativos, incluyendo personal altamente capacitado y acceso a tecnología avanzada, lo que les permite llevar a cabo ataques sofisticados y de gran escala.

Los actores estatales, como parte fundamental del panorama actual, operan en un espectro que va desde la vigilancia y el espionaje hasta la interrupción y el sabotaje. Sus capacidades y recursos les permiten llevar a cabo operaciones altamente coordinadas y a veces encubiertas, con el potencial de causar daños significativos tanto a nivel nacional como internacional.

Algunos ejemplos de actores estatales en el ámbito cibernético incluyen a las Tropas Cibernéticas del Ejército Popular de Liberación (EPL) de China. O ya que se cree que el EPL cuenta con unidades especializadas en ciberoperaciones que se dedican a actividades como el espionaje cibernético, la recopilación de información sensible y la infiltración de redes extranjeras.

Otro ejemplo es el Grupo de Inteligencia de Señales de Rusia (GRU), una agencia de inteligencia militar rusa conocida por llevar a cabo ciberoperaciones como el hackeo de sistemas informáticos extranjeros y la interferencia en elecciones y procesos políticos en otros países.

La Agencia de Seguridad Nacional (NSA) de Estados Unidos es también un actor relevante, dedicada a la recopilación de inteligencia de señales y ciberoperaciones defensivas y ofensivas.

A su vez también tenemos a la Unidad 8200 de Israel, una unidad de inteligencia militar israelí especializada en ciberoperaciones y de inteligencia electrónica, se ha implicado en actividades como el desarrollo de malware y la vigilancia cibernética a nivel internacional. Finalmente, otro ejemplo podría ser el Servicio Federal de Seguridad (FSB) de Rusia, principal servicio de inteligencia de ese país, que se involucra en actividades cibernéticas que van desde la vigilancia hasta la desinformación y el sabotaje cibernético.

Sin embargo estos son solo una parte de los actores que se pueden identificar, puesto que también tenemos a otro grupo que son aquellos que forman parte de grupos extremistas o que buscan sembrar el terror en la población, a estos se los denomina ciberterroristas.

Los ciberterroristas, a diferencia de los actores estatales que tienen respaldo gubernamental, operan de manera independiente o en pequeños grupos con el objetivo de causar daño, generar miedo o promover sus agendas extremistas a través de ciberataques. Su modus operandi puede incluir la interrupción de servicios críticos como la energía o las comunicaciones, el robo de información confidencial para extorsión o difusión, o la manipulación de datos para desestabilizar la confianza en instituciones o gobiernos.

Estos grupos suelen tener motivaciones ideológicas o religiosas y pueden aprovecharse de la facilidad de acceso a herramientas y técnicas de hacking disponibles en internet para llevar a cabo sus ataques. Algunos ejemplos de ciberterroristas incluyen grupos que pueden estar afiliados a organizaciones extremistas o terroristas con agendas políticas o religiosas específicas. Por ejemplo,

el Estado Islámico (ISIS) ha utilizado el ciberespacio como una herramienta para reclutar seguidores, difundir propaganda y coordinar ataques.

Aunque si bien estos grupos son grupos que actúan sin cooperación de un estado, es importante definir al siguiente grupo que se suele confundir con ciberterroristas y son los hacktivistas. El concepto de hacktivismo surge de la fusión entre el hacking y el activismo, representando una convergencia entre la acción política y el uso de habilidades hacker para expresar descontento en el entorno digital. En esencia, implica el empleo, ya sea legal o ilegal, de herramientas digitales con objetivos políticos y de protesta. No se percibe como una actividad criminal en sí misma, sino más bien como una forma legítima de protesta que se enfoca en instituciones gubernamentales o corporativas, con el propósito de promover el boicot, la desobediencia civil digital o la convocatoria a protestas virtuales.

El hacktivismo puede manifestarse de diversas maneras, desde la publicación de información confidencial hasta el bloqueo de servicios en línea, pasando por la alteración de sitios web para enviar mensajes políticos. Algunas de las tácticas más comunes incluyen ataques de denegación de servicio (DDoS), filtraciones de datos (como WikiLeaks), hackeo de sitios web gubernamentales o corporativos y campañas de concienciación a través de las redes sociales.

Los hacktivistas a menudo se organizan en grupos, como Anonymous, Cult of the Dead Cow (cDc) o LulzSec, aunque también puede haber individuos que actúan solos. Estos grupos suelen operar de manera descentralizada y anónima, utilizando pseudónimos y técnicas de ciberseguridad para proteger su identidad.

Como siguiente grupo describiremos a la delincuencia organizada. Su objetivo es la obtención de información para conseguir beneficios económicos. Estos grupos, lejos de operar de manera caótica, se organizan en estructuras jerárquicas definidas.

Dentro de las estructuras mencionadas anteriormente, cada individuo ocupa un lugar concreto, con roles y responsabilidades claramente definidos. Existen distintos grados de poder dentro de estas organizaciones, donde líderes y subordinados coexisten en una dinámica que se rige por la obediencia y la disciplina. La obtención y control de información es fundamental para su supervivencia y éxito, ya que les permite anticiparse a las acciones de las autoridades y de otros grupos rivales. Son grupos organizados que reclutan personas con grandes capacidades técnicas en el área, para realizar acciones delictivas.

Finalmente como último grupo, o mejor dicho individuos tenemos a civiles con conocimientos en el área que buscan realizar ataques. Estos a menudo se sienten atraídos por la emoción de desafiar sistemas de seguridad y pueden realizar acciones como el Defacement de sitios web, el robo de datos personales para uso personal o la interrupción de servicios en línea sin comprender completamente las implicaciones legales y éticas de sus acciones.

Aunque sus ataques suelen ser menos sofisticados que los de otros grupos, su número y diversidad pueden hacer que representen una amenaza considerable para individuos, empresas e incluso infraestructuras críticas en línea.

III - Ciberconflictos internacionales

Desde tiempos inmemoriales, los conflictos internacionales han sido una constante en la historia de la humanidad. Con la llegada de la era digital y la interconectividad que proporciona Internet, ha surgido un nuevo ámbito de confrontación: el ciberespacio. Este espacio virtual ha abierto nuevas oportunidades para la interacción global, pero también ha creado un terreno fértil para los conflictos y las tensiones internacionales.

La expansión de Internet y las tecnologías digitales ha transformado la manera en que los países interactúan, colaboran y, lamentablemente, entran en conflicto. Los ciberconflictos se han convertido en una parte integral de las estrategias de defensa y ataque de muchas naciones. Estos conflictos pueden manifestarse de diversas formas, incluyendo ciberataques a infraestructuras críticas, espionaje cibernético, desinformación y sabotaje digital.

Una de las características más preocupantes de los ciberconflictos es su capacidad para causar daño sin necesidad de una confrontación física directa. Los ciberataques no solo afectan a las naciones implicadas directamente, sino que también pueden tener repercusiones globales. Por ejemplo, un ataque cibernético a una gran empresa tecnológica puede afectar a millones de usuarios en todo el mundo, causando pérdidas económicas y erosionando la confianza en la seguridad digital.

La interconectividad global ha creado un entorno en el que la ciberseguridad es crucial no solo para la defensa nacional, sino también para la estabilidad económica y social.

Para comenzar a hablar de ciberconflictos a nivel internacional, es esencial entender el fenómeno más cotidiano que es el ciberdelito, es decir a la comisión de ilícitos en el ciberespacio. Para comprender esto debemos remontarnos al convenio sobre la ciberdelincuencia, celebrado en Budapest, en el año 2001.

El Convenio sobre la Ciberdelincuencia, también conocido como Convenio de Budapest, es un tratado internacional adoptado en 2001 que tiene como objetivo principal armonizar las leyes nacionales en materia de ciberdelincuencia, mejorar las técnicas de investigación y aumentar la cooperación entre las naciones. Este convenio aborda una amplia gama de delitos cometidos a través de Internet y otras redes informáticas, tales como:

El convenio establece medidas para que los países firmen acuerdos de cooperación internacional que faciliten la lucha contra estos crímenes a través de la extradición, la asistencia judicial recíproca y el intercambio de información.

Este marco legal proporciona una base sólida para la colaboración entre naciones en la lucha contra la ciberdelincuencia. Facilita la investigación y el enjuiciamiento de los ciberdelincuentes y asegura que las barreras legales y jurisdiccionales no impidan la justicia.

La adopción del Convenio de Budapest refleja un reconocimiento global de la necesidad de abordar la ciberdelincuencia de manera coordinada y eficaz. Este convenio es especialmente relevante en el contexto de los ciberconflictos internacionales, donde los ataques pueden tener repercusiones en múltiples países y jurisdicciones.

Debemos destacar que convenio de Budapest establece el término "ciberdelito" como cualquier delito penal que se cometa mediante el uso de tecnologías de la información y la comunicación, incluyendo la computación en red, Internet, sistemas informáticos, o cualquier dispositivo de tecnología de la información o comunicaciones que utilice software como medio para cometer el delito. Esto puede incluir una amplia gama de actividades delictivas, como el acceso no autorizado a sistemas informáticos, la interferencia con datos, el fraude, la difusión de virus, el robo de identidad en línea, la explotación sexual de menores en línea y muchas otras formas de conducta delictiva que involucran el uso indebido de la tecnología.

Los cibercrímenes o ciberdelitos a su vez pueden ser categorizados en dos grupos esenciales como son los de tipo violentos o potencialmente violentos y aquellos que

no lo son. Dentro de aquellos ciberdelitos no violentos encontramos a las apuestas por internet, el ciberfraude, la venta de drogas y/o material ilícito por internet y el lavado de dinero entre otros.

Por otro lado, tenemos aquellos ciberdelitos que se consideran violentos o potencialmente violentos, como pueden ser el ciberterrorismo, la pornografía infantil, etc.

Estos ciberdelitos traen aparejados consigo una violencia innata por detrás, aquella que debe ser aplicada como es el caso de la pornografía infantil para la producción de este material. Este es uno de los crímenes más repugnantes y perturbadores que existen en la sociedad. Implica la explotación sexual de niños y niñas para la producción, distribución y consumo de material pornográfico. Esta forma de abuso infantil deja secuelas devastadoras en las víctimas, tanto a nivel físico como psicológico, y socava gravemente su bienestar emocional y desarrollo.

La producción y distribución de este material no solo perpetúa el sufrimiento de las víctimas directas, sino que también contribuye a alimentar un mercado clandestino y perverso que perpetúa el abuso sexual infantil. Es fundamental abordar este problema desde múltiples frentes, incluyendo la aplicación rigurosa de la ley, la sensibilización pública, la educación sobre la prevención del abuso infantil y el apoyo integral a las víctimas.

Además, es necesario reconocer que la pornografía infantil no existe en un vacío, sino que está vinculada a redes más amplias de explotación sexual, tráfico de personas y otras formas de violencia y criminalidad.

Estos ciberdelitos de tipo violentos son realizados muchas veces por agrupaciones cibercriminales internacionales, en las cuales para comprender cómo funcionan primeramente debemos tener en cuenta que es una agrupación criminal y es que la Organización de las Naciones Unidas, en su art. 2 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional refiere:

> *"Por 'grupo delictivo organizado' se entenderá un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material"*[2]

Estas actividades pueden tener repercusiones significativas a nivel nacional e internacional, ya que pueden desencadenar crisis diplomáticas, afectar la estabilidad económica y socavar la seguridad nacional.

Esto podemos ponerlo en el contexto de la ciberguerra, donde los actores estatales y no estatales pueden emplear tácticas de ciberdelito como parte de sus estrategias. Por ejemplo, el ciberespionaje, el sabotaje de infraestructuras críticas y los ciberataques coordinados pueden ser utilizados como medios para lograr objetivos políticos, económicos o militares."

El ciberespionaje, por ejemplo, se ha convertido en una herramienta común utilizada por agencias de inteligencia y actores estatales para obtener información confidencial de otras naciones. Este tipo de actividad puede incluir la infiltración de redes gubernamentales, el robo de datos clasificados y la vigilancia electrónica de individuos y organizaciones clave.

[2] Art. 2- Convención de las Naciones Unidas contra la delincuencia organizada transnacional. 2000.

La neutralidad en el ciberespacio es otro punto a tener en cuenta la cual plantea un dilema fundamental: ¿cómo pueden los países neutrales evitar que sus recursos sean utilizados para perpetrar ciberataques contra otros estados? Si bien existe una expectativa de que los estados neutrales se abstengan de participar en ciberconflictos, la realidad es que la infraestructura soberana de los países es vulnerable a la infiltración. En este sentido, ¿es justo responsabilizar a los países neutrales por los ataques lanzados desde su territorio sin su conocimiento? Además, ¿cómo se puede atribuir la responsabilidad en un entorno donde la autoría de los ataques puede ser fácilmente enmascarada?

Es crucial reconocer que la neutralidad no implica necesariamente ignorancia o pasividad por parte de los países neutrales ante ciberactividades potencialmente maliciosas que se originan en su territorio. Los estados neutrales tienen la responsabilidad de garantizar la seguridad de su ciberinfraestructura y de tomar medidas proactivas para prevenir la utilización de sus recursos con fines ilegítimos.

Sin embargo, es importante también tener en cuenta los desafíos inherentes a la atribución de la responsabilidad en el ciberespacio. La naturaleza intrínsecamente anónima y fácilmente enmascarable de los ciberataques dificulta la identificación precisa de los perpetradores. Esto puede complicar la capacidad de los países neutrales para detectar y responder adecuadamente a las actividades maliciosas que se originan en su territorio.

Ante esto, podemos retomar el tema de los ciberdelitos que se han cometido, como es el caso de páginas famosas como Silk Road.

Silk Road fue una plataforma de comercio en línea en la dark web que se especializaba en la venta de drogas ilegales, armas y otros bienes ilícitos. Utilizando tecnologías de anonimato como TOR y Bitcoin para ocultar las identidades de sus usuarios, Silk Road operaba en un mercado clandestino que desafiaba las leyes de múltiples jurisdicciones.

Estos conflictos, como hemos mencionado anteriormente, pueden estar facilitados por el anonimato que provee Internet gracias a herramientas como TOR (The Onion Routing), Freenet, I2P, entre otras.

Para explicar una de las más conocidas, TOR, debemos saber que es una herramienta que protege la identidad en línea al desviar la conexión del usuario a través de una red global de servidores voluntarios. Este proceso, conocido como enrutamiento de cebolla, cifra cada paso del camino, dificultando enormemente el seguimiento de la actividad del usuario hasta su ubicación real.

El funcionamiento de TOR se basa en una red superpuesta de usuarios comunes de Internet que configuran sus computadoras como nodos. El anonimato que esta red puede proporcionar depende críticamente de la cantidad de nodos disponibles, ya que la privacidad de un usuario se asegura al mezclar su tráfico con el de muchos otros usuarios en la red.

Cuando un usuario desea conectarse a la red TOR, primero contacta a los servidores de directorio, que le proporcionan un listado de nodos activos. A partir de esta lista, el cliente de TOR selecciona tres nodos para establecer un circuito: un nodo de entrada o "guardia", un nodo intermedio y un nodo de salida.

La seguridad del tráfico en TOR se logra mediante el cifrado en capas. El cliente TOR cifra cada paquete de datos tres veces: primero con la clave pública del nodo de salida, luego con la del nodo intermedio y, finalmente, con la del nodo de entrada. De esta manera, cuando un paquete es enviado al nodo de entrada, este nodo solo sabe que debe enviarlo al nodo intermedio sin conocer su contenido o destino final. El nodo intermedio tampoco conoce el contenido de la comunicación, solo sabe a qué nodo debe reenviar el paquete. Finalmente, el nodo de salida puede conocer el destino final del paquete y, si la comunicación no está cifrada (por ejemplo, si se usa HTTP en lugar de HTTPS) también puede ver el contenido, pero no sabe de dónde proviene originalmente.

Además de TOR, otras tecnologías de anonimato como Freenet y I2P también juegan un papel crucial en la preservación del anonimato en línea. Freenet, por ejemplo, es una red descentralizada que permite la publicación, consulta y conservación de información sin censura. I2P (Invisible Internet Project) es otra red anónima que permite aplicaciones descentralizadas, similar a TOR pero optimizada para la comunicación entre servicios dentro de la propia red I2P.

La existencia de estas herramientas ha generado un campo de batalla constante entre quienes defienden la privacidad y el anonimato en línea y aquellos que buscan responsabilizar y atrapar a los cibercriminales. Mientras que las autoridades y los cuerpos de seguridad se esfuerzan por desarrollar métodos para rastrear actividades ilegales en estas redes, los defensores de la privacidad subrayan la importancia de estas tecnologías para la libertad de expresión y la protección de la privacidad personal frente a gobiernos y empresas.

IV – Ciberterrorismo

"*Los terroristas medran en la desesperación. Pueden conseguir reclutas o partidarios cuando no existen formas pacíficas y legítimas de remediar una injusticia, o parecen haberse agotado. Por este proceso, se sustrae el poder a las personas y se lo coloca en las manos de grupos pequeños y con fines poco claros."* [3]

El fenómeno del terrorismo ha sido objeto de análisis multidisciplinarios que buscan comprender sus causas y dinámicas subyacentes. En este contexto, la relación entre la desesperación y el reclutamiento terrorista ha sido un tema de interés creciente. La frase en cuestión, "Los terroristas medran en la desesperación", encapsula esta conexión intrincada entre la angustia social y la propagación del terrorismo. Este concepto es llevado a las batallas digitales que estamos viviendo en la actualidad.

La realidad es que muchos grupos extremistas utilizan medios digitalizados para promover sus ideas y perpetrar sus ataques de manera de obtener la mayor repercusión mediática sobre sus causas. Podemos remontarnos a ejemplos donde se han utilizado redes sociales como medio de reclutamiento a células terroristas, permitiendo el "Lavado de cerebro" de personas en haz de convertirlos en nuevos miembros de sus tropas.

Al hablar de terrorismo surge una necesidad de explicar una de las formas de "lavado de cerebro" que se tiene y es que aquellos que actúan con alguna forma de terrorismo lo hacen provocados por una falsa visión o una visión distorsionada de una realidad que les promete que aquello es lo correcto

[3] Annan, K. (22 de septiembre de 2003). Discurso pronunciado en la Conferencia "La lucha contra el terrorismo en pro de la humanidad: una conferencia sobre las raíces del mal". Nueva York.

Sin embargo, es crucial reconocer que la desesperación que impulsa a algunas personas hacia el terrorismo no surge únicamente de interpretaciones erróneas de la religión, sino también de contextos sociales, políticos y económicos desfavorables. La falta de oportunidades, la discriminación, la marginalización y la opresión son factores que alimentan la desesperación y la vulnerabilidad de ciertos grupos, convirtiéndolos en blancos fáciles para la propaganda extremista.

La lucha contra el terrorismo no es solo una batalla militar o de inteligencia, sino también una lucha por los corazones y las mentes de las personas. Es una tarea multidimensional que requiere un enfoque integral y colaborativo que involucre a gobiernos, organizaciones internacionales, sociedad civil, líderes religiosos y comunidades locales.

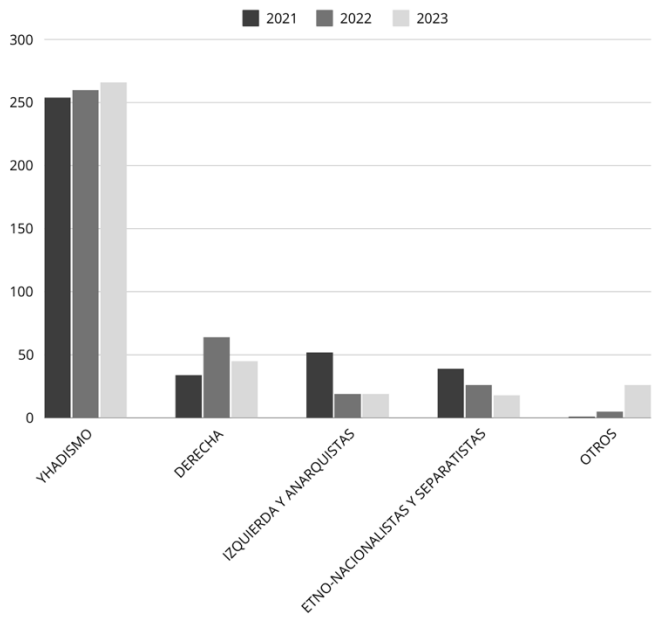
En este sentido, la educación juega un papel fundamental. No solo se trata de educar sobre los peligros del extremismo y la radicalización, sino también de promover la educación en valores como la tolerancia, la comprensión intercultural y la resolución pacífica de conflictos. La alfabetización mediática y digital también es crucial para capacitar a las personas a discernir la información y resistir la propaganda manipuladora en línea.

A nivel internacional, la cooperación entre países es fundamental para combatir el terrorismo de manera efectiva. Esto incluye el intercambio de información y mejores prácticas, la coordinación de esfuerzos en la prevención y la represión del terrorismo, así como el abordaje de las raíces profundas del extremismo violento a través de la diplomacia, el desarrollo y la asistencia humanitaria.

El ciberterrorismo, es una manifestación contemporánea del terrorismo tradicional con las mismas ideologías pero migrado al ciberespacio, de cualquier manera representa un desafío aún más complejo en este panorama. Dado a que los avances tecnológicos han proporcionado a los terroristas nuevas herramientas para reclutar, radicalizar y coordinar ataques de una manera sin precedentes. La naturaleza descentralizada y globalizada de Internet permite que las ideas extremistas se difundan rápidamente, alcanzando audiencias en todo el mundo con solo unos pocos clics.

Los grupos terroristas han adaptado sus métodos de reclutamiento y propaganda a la era digital, utilizando herramientas como las redes sociales, foros en la dark web y aplicaciones de mensajería encriptada. Estas plataformas les permiten difundir su ideología, reclutar nuevos miembros y coordinar acciones con una mayor eficiencia y anonimato. La desesperación social y la manipulación de visiones distorsionadas de la realidad son tácticas comunes empleadas para atraer a individuos vulnerables.

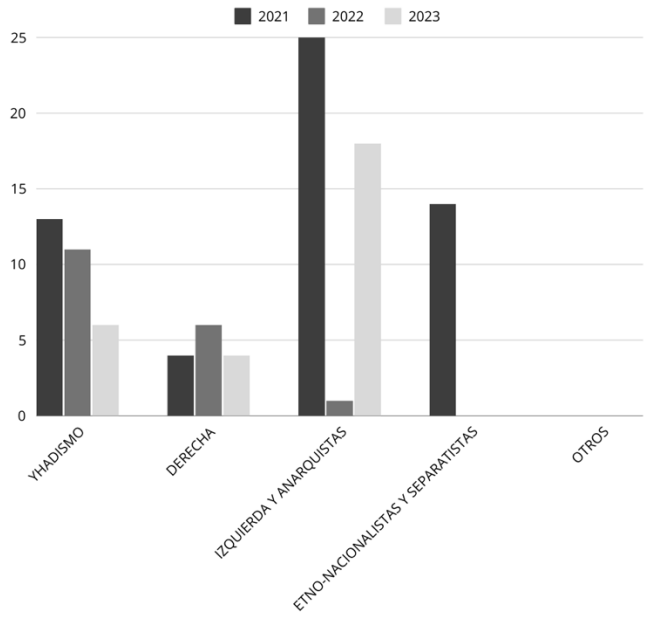
Detenciones por sospecha en la EU por tipo de terrorismo 2020-2022



Fuente: Europol (2023) - Informe TE-SAT 2023

El gráfico muestra el número de detenciones por sospecha de terrorismo en la Unión Europea (UE) desde 2020 hasta 2022, desglosado por tipo de terrorismo. Se observa que la mayoría de las detenciones por sospecha de terrorismo están relacionadas con el yihadismo, con más de 250 detenciones en cada uno de los tres años. Las detenciones relacionadas con el terrorismo de derecha son considerablemente menores en comparación con el yihadismo, con un notable aumento en 2022 en comparación con 2021 y 2023. Las detenciones por terrorismo de izquierda y anarquistas son pocas y se mantienen similares a lo largo de los tres años. En cuanto a los etno-nacionalistas y separatistas, hay un número moderado de detenciones, con una tendencia general a la disminución a lo largo del tiempo. La categoría de "otros" muestra el menor número de detenciones, pero con un ligero incremento en 2023.

Atentados terroristas (completados, fallidos, frustrados) en la EU 2020-2022



Fuente: Europol (2023) - Informe TE-SAT 2023

Observamos en el segundo gráfico que los atentados yihadistas y los ataques de extrema derecha son los más prevalentes en la Unión Europea. En 2021, los ataques yihadistas muestran un notable incremento, lo que subraya la persistente amenaza de este tipo de terrorismo. Los atentados de izquierda y anarquistas, aunque menos frecuentes, también presentan variaciones significativas entre los años.

Este patrón se refleja también en el ciberespacio, donde grupos extremistas utilizan la web para coordinar y ejecutar sus planes. Las plataformas en línea facilitan la planificación y ejecución de ataques, permitiendo a los terroristas operar con un alto grado de anonimato y protección contra la detección.

El uso de tecnologías de la información y comunicación (TIC) por parte de los terroristas no solo les permite alcanzar un mayor número de personas sino también ejecutar ciberataques que complementan sus ataques físicos. Por ejemplo, antes de un atentado, podrían lanzar ciberataques para desactivar sistemas de seguridad o causar pánico y desorganización.

Las estadísticas presentadas en el gráfico refuerzan la necesidad de una ciberseguridad robusta que no solo se enfoque en proteger infraestructuras críticas, sino también en anticipar y prevenir el uso malintencionado de la tecnología por parte de estos grupos.

La lucha contra el ciberterrorismo requiere una comprensión profunda tanto de las técnicas de reclutamiento digital como de los patrones de ataque tradicionales. Los datos presentados nos permiten ver las tendencias y preparar estrategias más efectivas para combatir estas amenazas en todas sus formas.

Además de la propaganda y el reclutamiento, el ciberterrorismo abarca ataques directos contra infraestructuras críticas, sistemas financieros y gubernamentales. Desde ataques de denegación de servicio hasta intrusiones en sistemas de control industrial, estas acciones representan una amenaza significativa para la seguridad nacional y la estabilidad global.

Enfrentar estas amenazas exige la colaboración estrecha entre las agencias de seguridad y los sectores tecnológicos. Es crucial que las empresas de tecnología trabajen en conjunto con los gobiernos para identificar y neutralizar ciberamenazas antes de que puedan causar daño significativo. Además, la actualización constante y el fortalecimiento de las medidas de ciberseguridad son vitales para proteger contra ataques emergentes y sofisticados.

El desarrollo de capacidades de ciberdefensa robustas también implica invertir en la formación y capacitación de profesionales en ciberseguridad. Estos expertos deben estar equipados con las habilidades y conocimientos necesarios para detectar, analizar y responder a incidentes cibernéticos en tiempo real. La creación de programas de educación y certificación en ciberseguridad, así como la promoción de una cultura de seguridad en todos los niveles de la sociedad, son pasos fundamentales para fortalecer la resiliencia frente a ciberamenazas.

Además, reiterando nuevamente se debe fomentar la cooperación internacional en la lucha contra el ciberterrorismo. Dado que las actividades cibernéticas no conocen fronteras, es esencial que los países trabajen juntos para compartir inteligencia, recursos y estrategias. Esta colaboración puede incluir la creación de marcos legales internacionales que faciliten la persecución y el enjuiciamiento de los

ciberterroristas, así como el establecimiento de centros de respuesta conjunta ante incidentes cibernéticos.

La lucha contra el terrorismo, tanto en el ámbito físico como en el cibernético, es una tarea compleja que requiere un enfoque multidimensional y coordinado. No basta con la represión de los actos terroristas; es igualmente importante abordar las causas subyacentes que alimentan la desesperación y la radicalización.

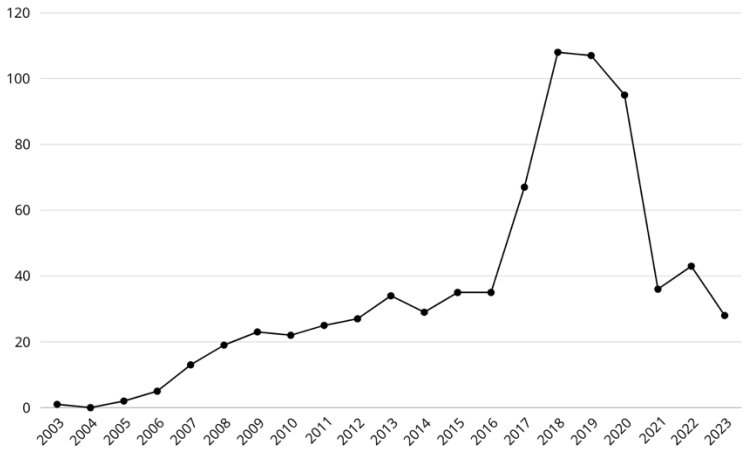
V – Ciberguerra

Actualmente nos encontramos en medio de una guerra de proporciones inimaginables, donde no solo participan estados, sino grupos extremistas, activistas, grupos criminales organizados y civiles. Una guerra invisible, que mucha gente desconoce que se está llevando a cabo, hablamos de la ciberguerra. Una batalla que parte como una abstracción de la guerra tradicional física, llevada al ciberespacio.

Esta guerra recuerda mucho a la guerra fría, dado que se centra en el espionaje, robo de información y acceso a lugares restringidos pero sin llegar a un punto bélico. Aunque no podemos negar que a su vez cuenta con un alto impacto que puede llegar a ser catastrófico e incluso mortal para la población en cuanto a la repercusión de los ataques. Para ilustrar la evolución y el impacto creciente de los ciberataques, el siguiente gráfico muestra los ciberincidentes significativos entre 2003 y 2023. Se enfoca en acciones estatales, espionaje y ciberataques donde las pérdidas superan el millón de dólares.

Incidentes cibernéticos significativos 2003-2023

*Esta gráfico enumera incidentes cibernéticos **significativos** desde 2003. Enfocado en acciones estatales, espionaje y ciberataques donde las **pérdidas superan el millón de dólares.***



Fuente: Center for Strategic and International Studies (CSIS) - https://www.csis.org

(El grafico se extiende hasta 2023, dado que no se tiene la totalidad del año 2024)

Como se observa en el gráfico, el número de incidentes ha experimentado un crecimiento considerable, especialmente a partir de 2016, lo que subraya la escalada en la intensidad y frecuencia de los ciberataques. Este aumento puede atribuirse a la creciente sofisticación de las herramientas y técnicas utilizadas por los atacantes, así como a la expansión del ciberespacio como un nuevo campo de batalla.

En este campo de batalla digital, las armas son códigos maliciosos, programas de espionaje y técnicas de hacking avanzadas. Los ataques pueden provenir de cualquier parte del mundo y su objetivo puede variar desde desestabilizar economías hasta influir en procesos políticos cruciales.

Los gobiernos invierten enormes recursos en fortalecer sus ciberdefensas y en desarrollar capacidades ofensivas para contrarrestar estas amenazas. Sin embargo, los grupos extremistas y los hackers independientes también tienen un papel significativo en este conflicto, ya que operan con relativa libertad y pueden llevar a cabo ataques con motivaciones diversas, desde el lucro hasta el activismo político.

En esta ciberguerra, la población civil también se ve afectada de manera directa. Los ciberataques pueden paralizar infraestructuras críticas como sistemas de energía, transporte o salud, poniendo en peligro la vida de miles de personas. Además, la manipulación de la información en línea puede sembrar el caos y la desconfianza en la sociedad, socavando las bases de la democracia y la estabilidad social.

Los incidentes de ciberguerra han ido en aumento, involucrando no solo a estados-nación, sino también a grupos terroristas, organizaciones políticas y sociales, así como a ciberactores transnacionales. Estos ataques pueden variar desde simples interrupciones de servicios en línea hasta la paralización de infraestructuras críticas,

como sistemas financieros o de suministro de energía. Ejemplos como los ataques a Estonia y Georgia en 2007 y 2008, respectivamente, destacan el potencial disruptivo de la guerra cibernética en el ámbito internacional.

Pero partamos desde el inicio. En 1996, un estudio publicado por el Instituto Nacional de Investigación de Defensa planteaba la inevitable transformación de la estrategia de seguridad de Estados Unidos debido al acelerado desarrollo del ciberespacio. Bajo el título "Guerra de Información Estratégica: Un Nuevo Rostro de la Guerra", este informe, financiado por el Departamento de Defensa, exploraba los desafíos potenciales que la guerra de información estratégica podría plantear para la seguridad nacional y sugería posibles medidas defensivas.

La ciberguerra plantea una serie de desafíos que afectan tanto a la seguridad nacional como a la estabilidad global. Uno de los principales aspectos a considerar es su accesibilidad y economía, lo que facilita que individuos o grupos con recursos mínimos lleven a cabo ciberataques que causen gran daño.

A su vez otra característica de esta guerra es la posibilidad de la manipulación de la percepción, la cual es un desafío significativo en la ciberguerra. La capacidad de influir en la opinión pública y en las decisiones gubernamentales mediante la difusión de información falsa o la alteración de contenido multimedia afecta la confianza en las instituciones y puede desestabilizar sociedades enteras.

Otro aspecto crítico a considerar es la limitación en la inteligencia estratégica. Los métodos tradicionales de inteligencia se ven desafiados por la velocidad y el anonimato del ciberespacio, dejando a los gobiernos vulnerables frente a amenazas desconocidas y dificultando la formulación de respuestas efectivas.

En medio de esta compleja realidad, las estrategias de ciberdefensa se han convertido en una prioridad para muchos países. Se están desarrollando algoritmos avanzados de detección de amenazas, se están fortaleciendo las infraestructuras críticas y se están estableciendo alianzas internacionales para compartir información y recursos en la lucha contra el ciberterrorismo y la guerra digital.

Sin embargo, a pesar de todos estos esfuerzos, la naturaleza cambiante y evolutiva de la tecnología hace que la guerra digital sea un campo de batalla en constante transformación. Se necesita una respuesta ágil y adaptable para hacer frente a las nuevas amenazas que surgen constantemente, y esto requiere una colaboración estrecha entre el sector público y privado, así como una inversión continua en investigación y desarrollo tecnológico.

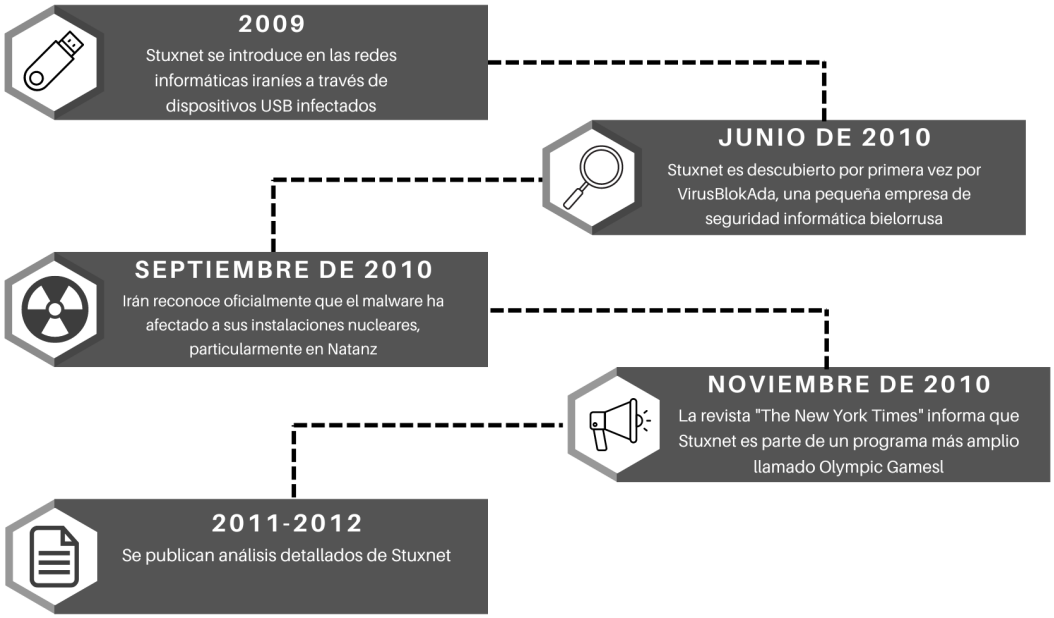
Es decir los esfuerzos internacionales no son suficientes ante la busqueda de poder de parte de estados y actores no estatales, los cuales con ilimitadas motivaciones políticas y/o religiosas buscan avanzar armamentísticamente, es decir, los estados y actores no estatales con conocimientos desarrollaran armas constantemente para lograr sobresalir, y a su vez avanzar de manera ágil en esta guerra, podemos encontrar que aquel con la última tecnología será el que predominara.

La guerra digital, ha sido no solo una guerra aislada sino un factor complementario de muchas guerras actuales, puesto que a pesar de ser un fenómeno individual que ocurre diariamente, también es un complemento o subcategoría de la guerra tradicional. Hemos visto su implementación innumerables veces, como pueden ser el caso, de la ciberguerra en Estonia en 2007, la operación Aurora en 2009-2010, el conflicto entre Georgia y Rusia en 2008, Etc.

Pero surge un problema cuando hablamos de ciberguerra, y es que es complicado trasladar esto al espacio físico, es decir, es difícil considerar que esta guerra digital pueda provocar muertes. La realidad es muy distinta, tenemos que partir de la base de que la mayoría de infraestructura critica a nivel global está compuesta de sistemas informáticos, muchas veces interconectados y otras aislados pero que cuentan con una posibilidad de error humano, desde reactores nucleares, centrales eléctricas, etc.

Esto nos remonta a dar un ejemplo de lo ocurrido en 2010 con el gusano informático Stuxnet, el cual tenía como posibles objetivos las turbinas en la planta de energía nuclear de Bushehr en Irán y las centrifugadoras en Natanz.

Lo que hizo a Stuxnet único fue su capacidad para infiltrarse en sistemas informáticos y luego manipular equipos físicos controlados por computadoras, como centrifugadoras utilizadas en el enriquecimiento de uranio. Fue diseñado para afectar los controladores lógicos programables (PLC) fabricados por Siemens, una empresa alemana de automatización industrial.



Stuxnet demostró ser una pieza de malware muy avanzada y compleja, con múltiples componentes y técnicas de evasión de detección. Su descubrimiento generó preocupaciones sobre la seguridad cibernética en infraestructuras críticas y planteó preguntas sobre quién podría estar detrás de un ataque tan elaborado. Aunque se desconoce a los autores de Stuxnet se cree fue una colaboración entre servicios de inteligencia estadounidenses e israelíes parte de una operación conocida como Olympic Games.

A partir de este punto, el campo de la guerra cibernética se ha vuelto más sofisticado y generalizado. El caso de Stuxnet no solo alertó a las naciones sobre la vulnerabilidad de sus infraestructuras críticas, sino que también incentivó una carrera armamentista en el ciberespacio. Países de todo el mundo han desarrollado unidades especializadas en ciberseguridad y ciberdefensa, integrando estas capacidades en sus estrategias de defensa nacional.

La ciberguerra, al ser una guerra sin fronteras físicas y con un nivel de anonimato considerable, plantea desafíos únicos para la legislación y la cooperación internacional. Las leyes internacionales aún están en proceso de adaptarse para abordar adecuadamente los ciberataques. Convenciones y tratados existentes a menudo no cubren las especificidades de la guerra digital, lo que dificulta la atribución y la responsabilidad.

Además, la atribución en el ciberespacio es particularmente complicada. Identificar a los responsables de un ataque puede tomar meses o incluso años, y la incertidumbre en la atribución puede llevar a tensiones diplomáticas o a la imposibilidad de tomar represalias adecuadas. Esta dificultad en la atribución también puede ser explotada por actores maliciosos para llevar a cabo ataques bajo falsas banderas, creando confusión y desestabilización adicional.

En este contexto, la cooperación internacional se vuelve esencial. Organismos como la OTAN y la Unión Europea han intensificado sus esfuerzos para compartir información y coordinar respuestas a ciberamenazas. La creación de equipos de respuesta a incidentes de ciberseguridad (CSIRT, por sus siglas en inglés) y la realización de ejercicios conjuntos de ciberdefensa son pasos importantes para fortalecer la resiliencia colectiva.

No obstante, la rapidez con la que evoluciona la tecnología cibernética requiere un enfoque continuo y adaptable. Los actores maliciosos constantemente desarrollan nuevas tácticas y herramientas, lo que obliga a las defensas a estar siempre un paso adelante. Esto no solo implica una inversión en tecnología y recursos humanos, sino también en educación y concienciación de la población sobre las mejores prácticas de ciberseguridad.

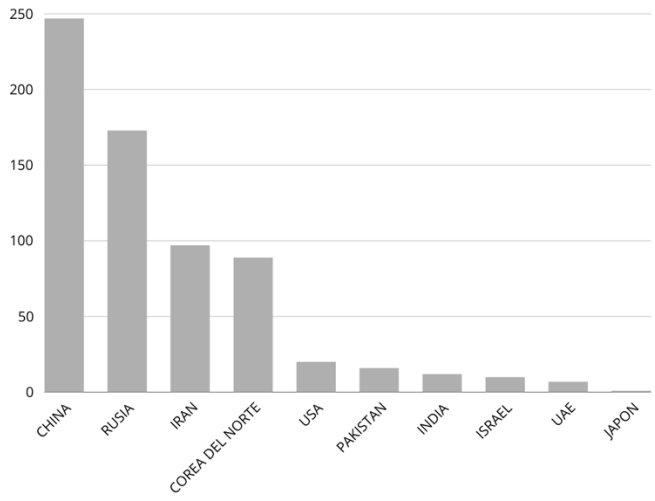
VI – Las Grandes Potencias en el Ciberespacio

En los últimos años, las grandes potencias han intensificado sus actividades en el ciberespacio. Las ciberoperaciones han pasado a ser una herramienta estratégica esencial, utilizada para influir en eventos globales, realizar espionaje industrial y político, y para demostrar poderío tecnológico.

Para entender mejor la magnitud de las ciberoperaciones estatales, a continuación se presenta un gráfico que muestra las ciberoperaciones patrocinadas por países. Este gráfico destaca a los actores más activos en el ciberespacio y proporciona una visión clara de la distribución de estas operaciones a nivel global.

Ciberoperaciones patrocinadas por países

Ciberoperaciones patrocinadas por países desde 2005-2023. Los datos destacan a China como el país con el mayor número de ciberoperaciones, seguido por Rusia, Irán y Corea del Norte



Fuente: Council on Foreign Relations - https://www.cfr.org/cyber-operations/

(Como se observa, China y Rusia lideran en número de ciberoperaciones, reflejando su enfoque agresivo en la ciberguerra. Irán y Corea del Norte también figuran notablemente, mientras que otros países como Estados Unidos, Pakistán, India, Israel, Emiratos Árabes Unidos y Japón muestran una actividad considerable, aunque menor en comparación con los demás.)

La ciberguerra, una forma moderna de conflicto, ha transformado radicalmente el panorama de la seguridad global. En este contexto, el gráfico anterior proporciona una visión clara sobre la cantidad de ciberataques impulsados por distintos estados. Según el gráfico, China lidera con un notable número de aproximadamente 250 operaciones, seguido por Rusia. Irán y Corea del Norte también muestran una actividad considerable de operaciones respectivamente. Estados Unidos, Pakistán, India, Israel, Emiratos Árabes Unidos y Japón presentan cifras menores, reflejando la distribución global de estas ciberamenazas.

La preeminencia de China en el ámbito de las ciberoperaciones no es sorprendente. Según el "Council on Foreign Relations", China ha desarrollado capacidades cibernéticas avanzadas y es conocida por su espionaje cibernético industrial y militar. Las unidades especializadas del Ejército Popular de Liberación (EPL), como la Unidad 61398, han sido vinculadas a numerosos ataques destinados a robar propiedad intelectual y datos sensibles de empresas y gobiernos extranjeros.

Rusia, otra potencia destacada en el gráfico, utiliza sus capacidades cibernéticas tanto para el espionaje como para la desestabilización política. El Grupo de Inteligencia de Señales (GRU) y el Servicio Federal de Seguridad (FSB) han sido asociados con ciberoperaciones que incluyen la interferencia en elecciones y la difusión de desinformación. La famosa intervención en las elecciones presidenciales de Estados Unidos en 2016 es un ejemplo destacado de la capacidad rusa para influir en procesos democráticos a través del ciberespacio.

Irán, con sus 100 operaciones, se ha consolidado como un actor importante en el ciberespacio, particularmente en el ámbito de la represalia contra sanciones económicas y agresiones militares. El grupo APT33, vinculado al gobierno iraní, ha

llevado a cabo ataques contra sectores de energía y aeroespacial en Estados Unidos y Medio Oriente, utilizando técnicas sofisticadas de phishing y malware.

Corea del Norte, a pesar de sus limitaciones económicas, ha demostrado una capacidad cibernética significativa. Las operaciones del Grupo Lazarus, un equipo de hackers patrocinado por el estado, incluyen el ataque al Banco Central de Bangladesh en 2016 y el ransomware WannaCry en 2017, que afectó a sistemas en todo el mundo. Estas acciones subrayan la capacidad de Pyongyang para utilizar el ciberespacio como una herramienta para generar ingresos y causar trastornos a nivel global.

Estados Unidos, aunque presenta un número menor de ciberoperaciones en comparación con China y Rusia, mantiene una postura ofensiva y defensiva robusta en el ciberespacio. La Agencia de Seguridad Nacional (NSA) y el Comando Cibernético de Estados Unidos han desarrollado capacidades avanzadas para proteger infraestructuras críticas y llevar a cabo operaciones ofensivas contra amenazas externas. La operación Stuxnet, un esfuerzo conjunto con Israel para sabotear las centrifugadoras nucleares de Irán, es un ejemplo notable de la sofisticación y alcance de las capacidades cibernéticas estadounidenses.

Pakistán, India, Israel, Emiratos Árabes Unidos y Japón también aparecen en el gráfico con un menor número de operaciones, lo que refleja su participación en el ciberespacio, aunque a una escala más modesta. Pakistán e India, por ejemplo, han estado involucrados en una serie de ciberataques mutuos, reflejando sus tensiones geopolíticas de larga data. Israel, a través de su Unidad 8200, ha estado a la vanguardia de la guerra cibernética, desarrollando capacidades tanto defensivas como ofensivas para protegerse de amenazas regionales y globales.

Este panorama de ciberoperaciones patrocinadas por estados destaca la naturaleza global y compleja de la ciberguerra. Los ciberataques pueden tener repercusiones significativas, desde el robo de información confidencial hasta la interrupción de infraestructuras críticas y la desestabilización de procesos políticos. La atribución de estos ataques es un desafío constante debido a la naturaleza anónima y enmascarada del ciberespacio, lo que complica los esfuerzos de defensa y respuesta.

En el caso de China, sus ciberoperaciones a menudo se centran en objetivos económicos y estratégicos, reflejando su enfoque en el espionaje industrial y la obtención de ventajas tecnológicas. Las actividades de la Unidad 61398, que ha sido vinculada a múltiples campañas de espionaje contra empresas y gobiernos occidentales, son un claro ejemplo de esta estrategia. Estos esfuerzos están diseñados para cerrar la brecha tecnológica con Occidente y asegurar la ventaja competitiva de China en sectores clave.

Rusia, por otro lado, utiliza el ciberespacio no solo para el espionaje, sino también como una herramienta para influir en la política internacional y desestabilizar a sus adversarios. Las operaciones del GRU y el FSB han incluido ataques a sistemas electorales, campañas de desinformación y sabotaje de infraestructuras críticas, demostrando una comprensión sofisticada de cómo el ciberespacio puede ser utilizado para proyectar poder e influencia.

La estrategia cibernética de Irán se centra en la retaliación y la disuasión. Frente a sanciones económicas y amenazas militares, Irán ha desarrollado capacidades para llevar a cabo ciberataques como una forma de represalia y para demostrar su capacidad de infligir daño a sus adversarios. Los ataques contra el sector energético

y las empresas aeroespaciales muestran la capacidad de Irán para afectar a industrias críticas y resaltar su capacidad de respuesta.

Corea del Norte ha utilizado sus capacidades cibernéticas como una herramienta para generar ingresos a través de actividades ilícitas y para mostrar su capacidad de causar trastornos a nivel global. El ataque al Banco Central de Bangladesh y la campaña de ransomware WannaCry subrayan la habilidad de Corea del Norte para llevar a cabo operaciones complejas y de gran impacto, a pesar de sus limitaciones económicas y tecnológicas.

Estados Unidos mantiene una postura proactiva en el ciberespacio, desarrollando capacidades tanto defensivas como ofensivas para proteger sus intereses y proyectar poder. La operación Stuxnet es un ejemplo de cómo Estados Unidos utiliza el ciberespacio para llevar a cabo operaciones ofensivas de alta precisión, con el objetivo de neutralizar amenazas potenciales antes de que se materialicen.

VII – Un arsenal en bits

Las ciberarmas son una manifestación moderna del poderío militar que se encuentra en constante evolución y cuya efectividad radica en su capacidad para explotar las vulnerabilidades de los sistemas informáticos y de comunicación. Y es que aquel que posee un arma que su enemigo desconoce, tendrá momentáneamente la ventaja sobre este.

Las naciones invierten enormes sumas en desarrollar sistemas de protección cibernética capaces de detectar y neutralizar amenazas antes de que causen daño. Sin embargo, la carrera armamentística digital es una batalla constante de ingenio y habilidad, donde cada avance en seguridad es contrarrestado por una nueva técnica de ataque.

En este contexto, la diplomacia digital se vuelve crucial. Los acuerdos internacionales sobre normas de comportamiento en el ciberespacio pueden ayudar a establecer límites y reducir la escalada de conflictos. La transparencia en las ciberoperaciones y la cooperación en la investigación de incidentes son pasos fundamentales hacia la construcción de la confianza entre las naciones. Además, el fortalecimiento de las capacidades de respuesta y recuperación ante ciberataques es esencial para minimizar el impacto y garantizar la resiliencia de las infraestructuras críticas.

A lo largo del tiempo desde que la informática paso de ser utilizada para crear armas a ser un arma como tal, podemos encontrar distintos ejemplos que han sido utilizados.

Entre los ejemplos empezaremos con "The Olympic Games" el cual era un programa de ciberarmas altamente sofisticado y secreto, meticulosamente diseñado por agencias de inteligencia y expertos en ciberseguridad. Su objetivo principal era infiltrarse en las infraestructuras críticas de un país objetivo para llevar a cabo operaciones de sabotaje encubiertas. Estas infraestructuras podían abarcar desde redes eléctricas y sistemas de comunicación hasta instalaciones nucleares o financieras.

El programa se caracterizaba por su complejidad técnica y su capacidad para eludir los sistemas de seguridad más avanzados. Utilizaba diversas técnicas, como malware específicamente diseñado, técnicas de infiltración avanzada y ataques dirigidos, para lograr su cometido sin ser detectado.

Como parte del programa, se le atribuye aunque sin confirmación la inclusión de la ciberarma Stuxnet de la cual hablamos anteriormente y la cual parecía apuntar hacia la planta nuclear iraní y el sitio de enriquecimiento de uranio en Natanz.

Los sistemas de control industrial, como los PLC (Controladores Lógicos Programables), son componentes vitales en entornos de fabricación y procesamiento industrial. Sin embargo, la creciente interconexión de estos sistemas con redes informáticas ha expuesto vulnerabilidades que podrían ser explotadas por atacantes malintencionados.

Una de las vulnerabilidades identificadas es la posibilidad de un Ataque de Denegación de Servicio (DoS). En este tipo de ataque, los atacantes pueden enviar paquetes de datos manipulados para interrumpir la comunicación entre el PLC y el software de control remoto, lo que podría paralizar operaciones industriales críticas.

Otra preocupación es el Secuestro de Sesión, donde los atacantes pueden interrumpir una conexión establecida entre el PLC y el software de control remoto, lo que podría llevar a un DoS o incluso permitir la manipulación de datos en tiempo real.

Además, se ha descubierto un exploit que permite la Eliminación del Programa Principal en los PLC, lo que puede resultar en la interrupción completa de la funcionalidad del sistema de control industrial.

La planta nuclear de Natanz opera en una red informática cerrada y aislada del aire, lo que significa que no tiene conexión a Internet ni a otras redes. Por lo tanto, es muy probable que Stuxnet haya infectado la red a través de un dispositivo USB extraíble Esto implica que los creadores del gusano necesitaron de una persona para introducirlo y así infectar la red.
A nivel internacional, el ciberataque logró retrasar brevemente el programa de enriquecimiento de uranio de Irán, lo que disminuyó ligeramente las tensiones internacionales relacionadas. De hecho, parecía que los retrasos aparentes en el programa habían tranquilizado lo suficiente a Israel como para que no arriesgara lanzar un ataque aéreo para detener físicamente el enriquecimiento.

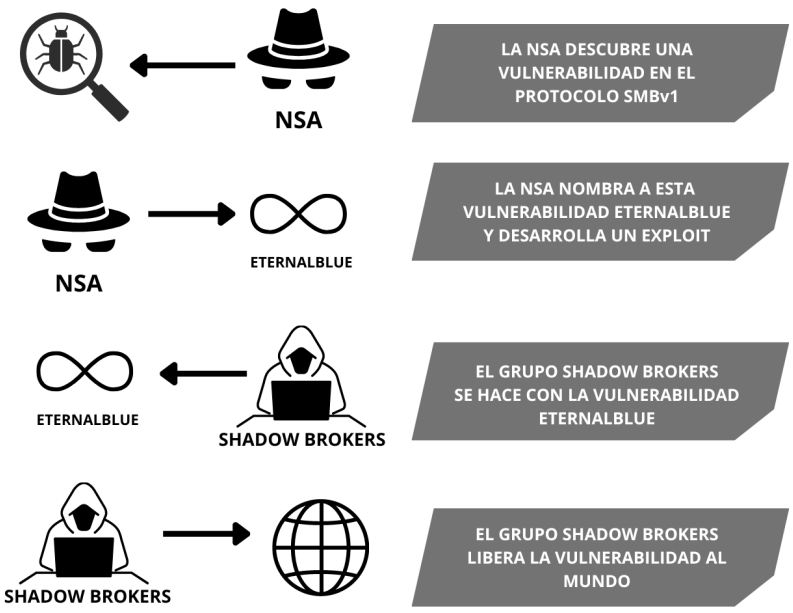
El desarrollador de Stuxnet, aunque su identidad sigue siendo incierta y se atribuye a la colaboración de dos estados, demostró que es posible construir una herramienta cibernética ofensiva altamente sofisticada y que los perpetradores tienen los recursos para llevar a cabo tal ataque. Además, este caso demostró que separar la red de infraestructura crítica de internet ya no puede considerarse una medida de seguridad suficiente. Los estados se dieron cuenta de que necesitaban tomar medidas para evitar convertirse en víctimas de tales ataques.

A su vez tenemos a Duqu el cual se considera un "hermano" de Stuxnet debido a sus similitudes en cuanto a su complejidad y su capacidad para infectar sistemas informáticos de manera sigilosa. El malware Duqu estaba diseñado principalmente para recopilar información confidencial de sistemas informáticos, como datos empresariales, industriales o gubernamentales. A menudo se utilizaba en ataques dirigidos a objetivos específicos, en lugar de propagarse ampliamente como un virus común.

El origen exacto de Duqu no está confirmado, pero se cree que fue creado por un grupo de hackers altamente sofisticado con habilidades técnicas avanzadas. Se ha especulado que podría tener vínculos con agencias estatales o grupos cibernéticos respaldados por estados debido a su complejidad y el tipo de objetivos que buscaba. Sin embargo, hasta donde sé, no hay una atribución definitiva del desarrollo de Duqu a una entidad específica.

Otra ciberarma conocida fue "Flame" el cual no fue solo un malware común, sino un ente digital que envolvía una complejidad extraordinaria. Su descubrimiento en 2012 dejó perplejos a expertos en ciberseguridad de todo el mundo. Concebido para infiltrarse en sistemas operativos Windows, no se limitaba a espiar; su versatilidad y alcance iban más allá de lo convencional en el mundo de la ciberdelincuencia.
Su diseño meticuloso y sus funciones polifacéticas lo distinguieron de otros malware contemporáneos. Se considera que "Flame" fue una creación sofisticada, posiblemente urdida por un estado-nación con fines de ciberespionaje. Este ente digital estaba dotado de capacidades tan amplias que incluso podía realizar tareas de vigilancia avanzada, recopilando datos confidenciales y transmitiéndolos a sus controladores de forma sigilosa.

A la hora de hablar de ciberarmas, no podemos dejar pasar a aquella que explotaba la vulnerabilidad "EternalBlue" la cual se originó en 2017 cuando ciertas ciberherramientas desarrolladas por la Agencia de Seguridad Nacional (NSA) de Estados Unidos fueron liberadas al público. Una de estas herramientas era un exploit que aprovechaba la vulnerabilidad EternalBlue, y su difusión causó estragos a nivel mundial. ¿Cómo llegó esta herramienta a manos de civiles y, por consiguiente, a actores malintencionados? La respuesta yace en un grupo de hackers conocido como The Shadow Brokers (TSB), que emergió en 2016. En ese año, anunciaron que habían obtenido acceso a las ciberherramientas clasificadas de la NSA, las cuales pertenecían al grupo de élite de hackers de la NSA llamado "Equation Group". Estas herramientas incluían exploits y malware diseñados para comprometer sistemas informáticos de diversas maneras.



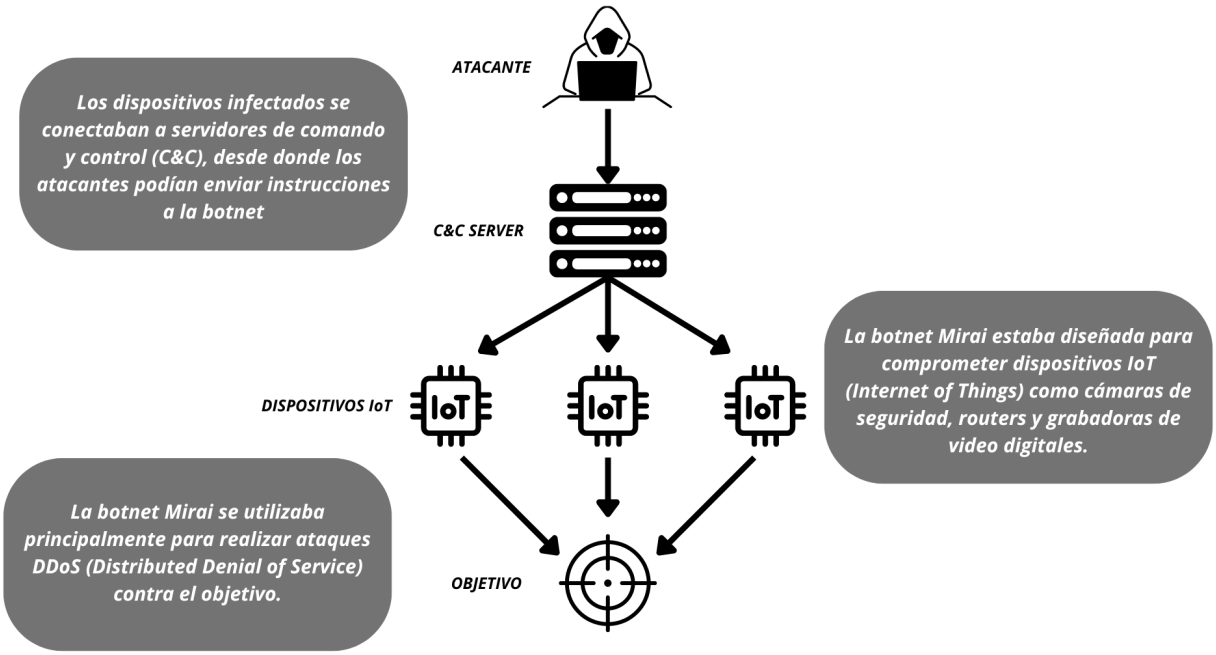
La vulnerabilidad EternalBlue fue descubierta en el protocolo de comunicación SMB (Server Message Block) utilizado por los sistemas operativos Windows. Permitía a los atacantes enviar paquetes de datos especialmente diseñados a través de la red para ejecutar código de forma remota en sistemas que no estuvieran parcheados adecuadamente.

Lo preocupante de EternalBlue era su capacidad para propagarse de manera automática a través de redes conectadas, lo que lo convertía en una herramienta ideal para ataques de ransomware y otros tipos de malware. El incidente más notable que explotó esta vulnerabilidad fue el ataque global de WannaCry en mayo de 2017, que afectó a cientos de miles de computadoras en más de 150 países en cuestión de horas.

Esta ciberarma conocida como “EternalBlue Exploit”, es decir un exploit, (pieza de software, secuencia de comandos o técnica que se utiliza para aprovechar una vulnerabilidad en un sistema informático), que aprovechaba esta vulnerabilidad, está actualmente disponible de manera libre, mediante herramientas como Metasploit, o exploits libres en internet.

Finalmente otra arma a mencionar la cual ha dado de que hablar el último tiempo es Mirai. La botnet Mirai se ha destacado por su capacidad para aprovechar dispositivos IoT (Internet de las cosas) comprometidos para llevar a cabo ataques DDoS (denegación de servicio distribuido). Este tipo de ataques pueden causar interrupciones significativas en servicios en línea al inundar los servidores con una cantidad abrumadora de tráfico malicioso.

Mirai se hizo famosa por su participación en ataques masivos, como el que afectó a Dyn en 2016, causando interrupciones en servicios importantes de Internet y sitios web populares.



La preocupación con Mirai y otros ataques de botnet es su capacidad para reclutar y coordinar una gran cantidad de dispositivos comprometidos, lo que les otorga una capacidad de ataque considerablemente amplificada. Además, la naturaleza distribuida de estos ataques los hace difíciles de mitigar sin una estrategia de defensa adecuada.

Los ataques de botnet como Mirai ponen de relieve la importancia de la seguridad en los dispositivos IoT, ya que muchos de estos dispositivos carecen de medidas adecuadas de protección y son vulnerables a la intrusión y explotación. Los fabricantes y los usuarios deben tomar medidas para asegurar que los dispositivos IoT estén actualizados con parches de seguridad, que tengan contraseñas fuertes y

que se implementen otras medidas de seguridad, como cortafuegos y sistemas de detección de intrusiones.

Por ende notamos que las ciberarmas modernas representan una creciente amenaza en el panorama de la seguridad cibernética. Estas armas digitales, diseñadas con habilidad y sofisticación, son utilizadas tanto por actores estatales como por grupos delictivos con el objetivo de infiltrarse en sistemas informáticos, robar datos sensibles, interrumpir infraestructuras críticas y desestabilizar economías enteras. Entre las ciberarmas más notorias de la actualidad se encuentran el malware altamente especializado, capaz de evadir las defensas más avanzadas y causar estragos en redes empresariales y gubernamentales.

Los ataques de ransomware, como el infame WannaCry y NotPetya, de los cuales hablaremos más adelante, que han demostrado el poder destructivo de estas ciberarmas al cifrar datos y exigir un rescate para su liberación, paralizando empresas e instituciones en todo el mundo.

Además, las operaciones de ciberespionaje, como las llevadas a cabo por grupos como DarkHotel y Equation Group, demuestran la capacidad de las ciberarmas para infiltrarse en sistemas altamente seguros y robar información confidencial con el fin de obtener ventajas políticas, económicas o militares. Los ataques dirigidos a infraestructuras críticas, como los perpetrados por Stuxnet y BlackEnergy, revelan la vulnerabilidad de sectores vitales como la energía, las comunicaciones y el transporte frente a la sofisticada ingeniería de las ciberarmas modernas.

En un mundo cada vez más interconectado, donde la dependencia de la tecnología digital es omnipresente, la amenaza representada por las ciberarmas actuales es una

preocupación constante. La lista sigue evolucionando a medida que surgen nuevas amenazas y técnicas de ataque. La defensa contra estas amenazas requiere una combinación de medidas técnicas, como el uso de software de seguridad actualizado y firewalls, así como prácticas de seguridad sólidas, como la concienciación del usuario y la gestión adecuada de contraseñas. Prácticas que si bien no evitaran por completo ser sometidas por próximas armas que se desarrollen, pero si pondrán una primera barrera de defensa ante un posible ataque

Aunque debemos hacernos una pregunta, y es que dado a la cantidad de horas y muchas veces presupuesto que requiere desarrollar estas armas, ¿Cuál es su beneficio frente a armas convencionales?. Según Eugene Kaspersky, los siguientes motivos [4]

- **Efectividad:** Se ha demostrado que las ciberarmas son altamente efectivas para lograr sus objetivos militares, como lo demuestran ejemplos como Stuxnet, Duqu y Flame.
- **Rentabilidad:** Son considerablemente más baratas de desarrollar y desplegar en comparación con las armas tradicionales, lo que las convierte en una opción atractiva para estados con recursos limitados.
- **Dificultad de detección y atribución:** Las ciberarmas son difíciles de detectar y atribuir a un atacante específico, lo que hace que las medidas defensivas proactivas sean menos efectivas.
- **Destructividad comparativa:** Las ciberarmas, a pesar de ser menos visibles y reguladas que las armas tradicionales de destrucción masiva, tienen un potencial destructivo comparable, con el atractivo adicional de la invisibilidad y la precisión.

[4] Eugene Kaspersky. (2012). The Flame That Changed the World.. EUGENE KASPERSKY – OFFICIAL BLOG.

El panorama de las ciberarmas se presenta como un desafío constante en el ámbito de la seguridad cibernética. Estas herramientas digitales, con su capacidad de infiltración, sabotaje y espionaje, han redefinido el concepto de guerra en el siglo XXI. Y como se mencionó anteriormente la diplomacia digital emerge como un elemento crucial para mitigar los riesgos y promover la cooperación internacional en materia de ciberseguridad. Los acuerdos sobre normas de comportamiento en el ciberespacio, la transparencia en las ciberoperaciones y el fortalecimiento de las capacidades de respuesta son pasos fundamentales hacia un futuro más seguro y resiliente.

Estamos viviendo una carrera, la carrera armamentista digital la cual es un fenómeno que refleja la competencia entre países, organizaciones e individuos por obtener superioridad en el ámbito de la tecnología y la ciberseguridad. A medida que la sociedad se vuelve cada vez más dependiente de la tecnología digital, desde las comunicaciones hasta las infraestructuras críticas, el control y la protección de los sistemas informáticos se convierten en prioridades estratégicas.

Esta carrera abarca una amplia gama de actividades, que van desde el desarrollo de malware y técnicas de hacking hasta la creación de sistemas de defensa cibernética y herramientas de inteligencia artificial para contrarrestar las amenazas digitales. Los actores involucrados pueden ser gobiernos, agencias de inteligencia, empresas de seguridad cibernética e incluso grupos criminales.

Las motivaciones detrás de esta carrera son diversas, que van desde el espionaje y la recolección de información sensible hasta el sabotaje y la guerra cibernética. Los ciberataques pueden tener consecuencias devastadoras, desde el robo de datos

confidenciales hasta el sabotaje de infraestructuras críticas como redes eléctricas o sistemas financieros.

Para mantenerse a la vanguardia en esta carrera, los países y las organizaciones invierten grandes sumas de dinero en investigación y desarrollo de tecnologías avanzadas, así como en la formación de expertos en ciberseguridad. Sin embargo, a medida que avanza la tecnología, también lo hacen las amenazas, lo que hace que esta carrera sea un desafío continuo y en constante evolución.

VIII – El mercado Zero Day

¿Dónde acuden los distintos hackers cuando quieren comprometer objetivos?. Cuando los hackers buscan comprometer objetivos específicos, recurren a varios recursos especializados donde pueden adquirir conocimientos y herramientas necesarias para llevar a cabo sus ataques. Uno de estos recursos es el mercado de Zero Day, donde se venden vulnerabilidades no descubiertas previamente por sumas significativas de dinero. Estas vulnerabilidades, conocidas como Zero Day, son especialmente peligrosas porque no se han desarrollado parches para mitigarlas, permitiendo a los atacantes explotarlas sin ser detectados. Imaginemos una vulnerabilidad descubierta ya hace unas semanas, seguro que ya posee un parche o varios. ¿Qué pasa con una vulnerabilidad descubierta hace un par de días?. Pues seguramente muchos aspirantes a hackers estén intentando accionar mediante ella, y ya se esté trabajando en el parche. Pero cuando un sistema posee una vulnerabilidad que no ha sido reportada, estamos frente a lo que se conoce como vulnerabilidad Zero Day.

Estas vulnerabilidades son invaluables para los distintos actores en el ciberespacio, ya que pueden ser una oportunidad de cambiar sus vidas significativamente en cuanto a la venta de ellas, o pueden ser usadas para lograr sus cometidos. Pero ¿Dónde se adquieren esta vulnerabilidades?. Aquí es donde surgen los mercados Zero Day. Estos operan en las profundidades de la darknet, una parte oculta de Internet accesible solo mediante software específico como Tor. La darknet permite el anonimato y el cifrado, lo que la convierte en un entorno ideal para actividades ilegales, incluyendo la venta de exploits y vulnerabilidades de software. Estos mercados ofrecen un espacio donde hackers, investigadores de seguridad y

criminales pueden comprar y vender información sobre vulnerabilidades que no son de conocimiento público.

Por ejemplo, una vulnerabilidad crítica en un sistema operativo popular puede ser vendida por millones de dólares debido a su capacidad para causar daños significativos o proporcionar acceso no autorizado a sistemas altamente protegidos. La venta de estas vulnerabilidades a menudo implica un proceso detallado que incluye la validación de la eficacia del exploit, la negociación del precio y, en algunos casos, la firma de contratos que garantizan la exclusividad del comprador.

La darknet es una red oculta que proporciona un nivel de anonimato y privacidad no disponible en la internet convencional. Esto es posible gracias a tecnologías como Tor (The Onion Router), que encripta y redirige el tráfico a través de una serie de nodos distribuidos globalmente. Este entorno ha dado lugar a una variedad de actividades ilegales, desde el tráfico de drogas y armas hasta servicios de hacking y la venta de exploits Zero Day.

En la darknet, existen numerosos foros y mercados clandestinos donde se intercambian conocimientos y herramientas de hacking. Estos espacios no solo venden exploits, sino que también ofrecen tutoriales, servicios de hacking a pedido, y plataformas para la colaboración entre hackers. Por ejemplo, foros como Exploit.in o TheRealDeal Market han sido conocidos por ofrecer vulnerabilidades Zero Day a una clientela global.

Los exploits Zero Day son especialmente valiosos porque explotan fallos en el software que son desconocidos tanto para el fabricante como para la comunidad de seguridad en general. Esto significa que no existen parches ni defensas disponibles, lo que permite a los atacantes utilizar estos exploits para acceder a sistemas vulnerables sin ser detectados.

La existencia y operación de mercados Zero Day subraya la importancia crítica de las medidas proactivas y reactivas de seguridad en las organizaciones. Para protegerse contra estas amenazas, es esencial que las empresas y entidades gubernamentales implementen estrategias de seguridad robustas y estén preparadas para responder rápidamente a nuevas vulnerabilidades.

El uso de ataques Zero Day por actores estatales es una práctica bien documentada y ha sido un componente clave en la ciberguerra moderna. Los gobiernos invierten

significativamente en el descubrimiento y desarrollo de exploits Zero Day para usarlos en operaciones de espionaje, sabotaje y recopilación de inteligencia. Por ejemplo, el ataque Stuxnet, que es quizás el caso más famoso de un exploit Zero Day utilizado en un contexto estatal, demostró cómo estas vulnerabilidades pueden ser empleadas para objetivos de sabotaje. Stuxnet, un malware desarrollado presuntamente por los gobiernos de Estados Unidos e Israel, fue diseñado específicamente para atacar las centrifugadoras utilizadas en el programa nuclear de Irán, causando daños físicos significativos y retrasando su progreso.

Además de las operaciones de sabotaje, los exploits Zero Day también son herramientas poderosas para el espionaje. Los actores estatales utilizan estos ataques para infiltrarse en redes de gobiernos extranjeros, organizaciones no gubernamentales, y corporaciones para obtener información clasificada y estratégicamente valiosa. China, Rusia, y Estados Unidos son conocidos por tener programas sofisticados y bien financiados dedicados al descubrimiento y utilización de estas vulnerabilidades. Por ejemplo, se ha informado que el grupo de hackers APT28, asociado con la inteligencia militar rusa, utiliza exploits Zero Day para realizar operaciones de ciberespionaje contra objetivos en Europa y América del Norte.

Por otro lado, los actores no estatales también han encontrado en los ataques Zero Day una herramienta poderosa para sus propios fines. Grupos de ciberdelincuentes y hackers éticos o de sombrero gris pueden descubrir y explotar estas vulnerabilidades para obtener acceso no autorizado a sistemas, robar datos o incluso extorsionar a organizaciones. A diferencia de los actores estatales, que a menudo tienen recursos prácticamente ilimitados, los actores no estatales suelen operar con

presupuestos más reducidos y dependen más de la creatividad y la comunidad para descubrir y explotar vulnerabilidades Zero Day.

El mercado negro de exploits Zero Day es un entorno donde tanto actores estatales como no estatales pueden adquirir estas vulnerabilidades. Los precios de los exploits varían considerablemente dependiendo de la criticidad y el impacto potencial de la vulnerabilidad, con algunos llegando a costar millones de dólares. Este mercado también fomenta una carrera armamentista cibernética, ya que los actores buscan continuamente descubrir y adquirir nuevos exploits antes que sus adversarios.

Además, las corporaciones privadas, especialmente aquellas en el sector de la tecnología, invierten considerablemente en descubrir y protegerse contra exploits Zero Day. Empresas como Google y Microsoft tienen equipos dedicados de ciberseguridad que se enfocan en identificar estas vulnerabilidades en sus productos antes de que puedan ser explotadas por actores malintencionados. Los programas de recompensas por bugs (bug bounty) son una práctica común en estas empresas, incentivando a los hackers éticos a reportar vulnerabilidades a cambio de recompensas financieras, en lugar de venderlas en el mercado negro.

La proliferación de ataques Zero Day también ha llevado al desarrollo de sofisticadas ciberdefensas y estrategias de mitigación. Las organizaciones ahora emplean técnicas avanzadas de monitoreo y análisis de comportamiento para detectar posibles exploits Zero Day antes de que puedan causar daño significativo. Sin embargo, a pesar de estos esfuerzos, la naturaleza misma de las vulnerabilidades Zero Day –que son desconocidas hasta que son explotadas– sigue presentando un desafío significativo para la ciberseguridad.

Entre las medidas reactivas para hacer frente a esta amenaza podemos encontrar:

- **Monitoreo Continuo y Detección de Intrusos:**
  Implementar sistemas de detección y prevención de intrusos (IDS/IPS) y soluciones de monitoreo continuo puede ayudar a detectar actividades sospechosas en tiempo real. Estos sistemas deben estar configurados para alertar inmediatamente a los equipos de seguridad sobre posibles incidentes.

- **Planes de Respuesta a Incidentes:**
  Desarrollar y mantener un plan de respuesta a incidentes es crucial para minimizar el daño en caso de un ataque. Este plan debe incluir procedimientos claros para la contención, erradicación, recuperación y comunicación durante y después de un incidente de seguridad.

- **Análisis Forense:**
  Después de un incidente de seguridad, es vital realizar un análisis forense para comprender cómo ocurrió el ataque, qué vulnerabilidades se explotaron y qué datos se comprometieron. Esta información es fundamental para mejorar las defensas y prevenir futuros incidentes.

- **Colaboración con la Comunidad de Seguridad:**
  Colaborar con otras organizaciones y participar en redes de intercambio de información sobre amenazas puede proporcionar valiosos conocimientos sobre nuevas vulnerabilidades y tácticas de ataque.

Por ende al igual que los señores de la guerra y traficantes de armas que venden herramientas de destrucción en conflictos bélicos, los vendedores de exploits Zero Day actúan en un entorno clandestino, proporcionando a sus compradores las herramientas necesarias para llevar a cabo ciberataques devastadores. Estos mercados en la darknet son los campos de batalla modernos, donde hackers, investigadores de seguridad y criminales compran y venden información sobre vulnerabilidades que no son de conocimiento público.

Tanto actores estatales como no estatales utilizan los exploits Zero Day para espionaje, sabotaje y otros fines malintencionados, lo que ha generado una carrera armamentista cibernética. La historia del espionaje y la guerra tradicional encuentra su paralelo en el ciberespacio, donde las vulnerabilidades de software son las nuevas armas de guerra y los hackers son los nuevos soldados.

Las organizaciones deben implementar medidas de seguridad robustas y reactivas, como el monitoreo continuo, planes de respuesta a incidentes y análisis forense, para protegerse contra estas amenazas. Además, la colaboración con la comunidad de seguridad y programas de recompensas por bugs son esenciales para descubrir y mitigar nuevas vulnerabilidades antes de que puedan ser explotadas. La proliferación de ataques Zero Day subraya la necesidad de estar siempre un paso adelante en esta nueva era de ciberconflictos, donde la información es poder y las vulnerabilidades son las armas del siglo XXI.

IX – Infraestructuras críticas

Las infraestructuras críticas son componentes esenciales para el funcionamiento de una sociedad moderna. Estas incluyen tanto sistemas físicos como virtuales que abarcan una amplia gama de sectores como las redes eléctricas, sistemas de agua potable, transporte, salud y telecomunicaciones. La seguridad de estas infraestructuras es vital, ya que cualquier interrupción en sus servicios puede tener consecuencias catastróficas para la seguridad nacional, la economía y la calidad de vida de los ciudadanos.

En la era digital, estas infraestructuras dependen cada vez más de la tecnología y las redes de información, lo que las hace especialmente vulnerables a los ciberataques. La digitalización ha mejorado significativamente la eficiencia y la capacidad de gestión de estas infraestructuras, pero también ha abierto nuevas brechas de seguridad que pueden ser explotadas por actores maliciosos, ya sean estados, organizaciones terroristas o ciberdelincuentes. Uno de los casos más emblemáticos que destaca la vulnerabilidad de las infraestructuras críticas es el ataque del gusano informático Stuxnet. Descubierto en 2010, Stuxnet fue diseñado específicamente

para atacar los controladores lógicos programables (PLC) de Siemens, utilizados en la planta de energía nuclear de Bushehr en Irán y las centrifugadoras en Natanz. Este malware fue altamente sofisticado, capaz de infiltrarse en sistemas informáticos y manipular equipos físicos controlados por computadoras.

Los ciberataques a infraestructuras críticas pueden tener consecuencias devastadoras. Estos ataques no solo pueden robar datos confidenciales, sino también sabotear sistemas completos. Por ejemplo, un ataque exitoso a una red eléctrica podría dejar a millones de personas sin electricidad, afectando todos los aspectos de la vida cotidiana, desde el suministro de agua hasta los servicios de emergencia. En el sector de la salud, los ataques a sistemas hospitalarios pueden comprometer tanto la privacidad de los pacientes como la capacidad de los hospitales para prestar servicios médicos.

Para proteger las infraestructuras críticas, los gobiernos y organizaciones deben invertir en medidas robustas de ciberseguridad. Esto incluye no solo la implementación de tecnologías avanzadas de defensa, sino también la formación continua de expertos en ciberseguridad. Además, la cooperación internacional es crucial. Los acuerdos sobre normas de comportamiento en el ciberespacio, la transparencia en las ciberoperaciones y la colaboración en la investigación de incidentes son pasos fundamentales para construir la confianza y garantizar la resiliencia de estas infraestructuras.

El campo de la ciberguerra se ha vuelto más sofisticado y generalizado, incentivando una carrera armamentista en el ciberespacio. Países de todo el mundo han desarrollado unidades especializadas en ciberseguridad y ciberdefensa, integrando estas capacidades en sus estrategias de defensa nacional. La atribución en el

ciberespacio es particularmente complicada, lo que plantea desafíos únicos para la legislación y la cooperación internacional. Identificar a los responsables de un ataque puede tomar meses o incluso años, y la incertidumbre en la atribución puede llevar a tensiones diplomáticas.

Los desafíos en la protección de infraestructuras críticas no se limitan a los ciberataques directos. También incluyen la seguridad física, la resiliencia ante desastres naturales y la capacidad de respuesta ante emergencias. La integración de sistemas y físicos crea nuevas vulnerabilidades que requieren un enfoque holístico de seguridad. Por ejemplo, un ciberataque podría ser combinado con un ataque físico para maximizar el impacto, una táctica conocida como "ataque híbrido".

Los ataques híbridos representan una de las amenazas más complejas y peligrosas para las infraestructuras críticas. Este tipo de ataques combinan elementos cibernéticos y físicos para crear un efecto sinérgico, aumentando significativamente el daño y la dificultad de respuesta. La coordinación entre un ataque cibernético y un ataque físico puede paralizar las defensas tradicionales que normalmente se centran en un solo vector de ataque.

Uno de los ejemplos más conocidos de un ataque híbrido es el ataque a la red eléctrica de Ucrania el 3 de diciembre de 2015. Se sospecha que el actor responsable fue el grupo Sandworm, y el servicio de seguridad ucraniano (SBU) culpó a Rusia del ataque. Los objetivos fueron las subestaciones de la compañía energética ucraniana. En el caso de la subestación Prykarpattyaoblenergo, los hackers lograron desconectar la red. Los sistemas objetivo estaban basados en Microsoft Windows. La primera parte del ataque utilizó una versión actualizada del malware BlackEnergy. El código malicioso fue enviado a través de correos electrónicos con

archivos adjuntos maliciosos, dirigidos a individuos específicos dentro de las distintas compañías energéticas para obtener credenciales de administrador y acceder a las redes de las subestaciones energéticas.

Durante la segunda parte del ataque, los actores activaron un malware destructivo KillDisk, capaz de borrar partes de los discos duros de las computadoras e impedir que los sistemas se reiniciaran, lo que llevó a los apagones. Finalmente, los hackers lanzaron un ataque TDoS (telephony denial of service) contra el centro de atención telefónica de los clientes, impidiendo que los usuarios reportaran el apagón. Este ataque resultó en apagones para casi 225.000 consumidores en el oeste de Ucrania. El malware desconectó las subestaciones eléctricas, causando el apagón. Para restaurar la actividad normal de las subestaciones fue necesaria la intervención manual de los operadores en el sitio, incluyendo el cambio del centro de control de despacho de "modo automático a manual", ya que los hackers habían infectado el firmware del fabricante del SCADA. Sin embargo, una vez restauradas, las infraestructuras impactadas continuaron funcionando bajo operaciones restringidas.

Este incidente en Ucrania es el primer ataque reconocido públicamente que utilizó un arma digital para golpear una red eléctrica y causar apagones. También es la primera vez que un ataque cibernético que causa interrupciones en la energía eléctrica se ha llevado a cabo de manera totalmente remota.

Este tipo de ataques requieren una planificación y ejecución meticulosa, ya que los atacantes deben coordinar varias actividades simultáneamente. El componente cibernético puede incluir la desactivación de sistemas de seguridad, la manipulación de datos o la introducción de malware para sabotear operaciones. Mientras tanto, el

componente físico podría involucrar acciones como la destrucción de equipos, la interrupción de comunicaciones o incluso el uso de armas para causar daño directo.

La interdependencia de los sistemas cibernéticos y físicos significa que las vulnerabilidades en uno pueden ser explotadas para atacar al otro. Por ejemplo, un ataque cibernético a un sistema de gestión de tráfico podría causar accidentes o interrupciones significativas en el transporte. Del mismo modo, un ataque físico a un centro de datos puede interrumpir servicios críticos y causar una cascada de fallos en los sistemas que dependen de esos datos.

La defensa contra ataques híbridos requiere una estrategia integrada que combine ciberseguridad y seguridad física. Las organizaciones deben implementar medidas que protejan tanto los sistemas cibernéticos como los activos físicos. Esto incluye la protección perimetral, la vigilancia física y la seguridad cibernética avanzada. Los planes de respuesta a incidentes deben considerar la posibilidad de ataques híbridos y preparar procedimientos para manejar situaciones en las que se combinan ciberamenazas y físicas.

Los sectores más críticos incluyen energía, agua, transporte y telecomunicaciones. La infraestructura energética, por ejemplo, es fundamental no solo para el funcionamiento de las viviendas y empresas, sino también para la operación de otras infraestructuras críticas. La interrupción de la energía eléctrica puede tener un efecto dominó, afectando a hospitales, sistemas de transporte, y comunicaciones. En el sector del agua, la contaminación de los suministros de agua potable o la interrupción del servicio puede poner en riesgo la salud pública y crear un pánico masivo.

El transporte es otro sector crucial. La seguridad de los sistemas de transporte, que incluye tanto aéreos como terrestres y marítimos, es esencial para la movilidad de personas y bienes. Los ataques a estos sistemas pueden tener un impacto económico significativo y causar interrupciones a gran escala. Los sistemas de control de tráfico aéreo, por ejemplo, son objetivos atractivos debido a la potencial gravedad de las consecuencias de un ataque exitoso.

Las telecomunicaciones también son esenciales, ya que facilitan la comunicación tanto a nivel personal como profesional y gubernamental. La interrupción de estos servicios puede afectar la coordinación de las respuestas de emergencia y la comunicación entre agencias gubernamentales y organizaciones internacionales. Los ataques a las redes de telecomunicaciones pueden incluir desde la interrupción de servicios hasta el espionaje y la manipulación de información.

La infraestructura crítica no solo es una preocupación a nivel nacional, sino también internacional. En un mundo globalizado, las redes y sistemas son interdependientes, y una interrupción en una región puede tener repercusiones a nivel global. Esto subraya la importancia de la cooperación internacional en la protección de infraestructuras críticas. Los marcos de colaboración internacional, como las alianzas y tratados, son esenciales para compartir información y recursos, y para coordinar respuestas a incidentes.

Las políticas y regulaciones juegan un papel fundamental en la protección de infraestructuras críticas. Los gobiernos deben establecer normativas que obliguen a las organizaciones a adoptar medidas de seguridad adecuadas. Esto incluye la creación de estándares de seguridad, la realización de evaluaciones de riesgo y la implementación de planes de respuesta a incidentes. Además, es crucial que las

políticas sean dinámicas y evolucionen para adaptarse a las nuevas amenazas y tecnologías.

La concienciación y formación también son elementos clave. Los empleados de organizaciones que operan infraestructuras críticas deben estar bien informados sobre las amenazas y capacitados en las mejores prácticas de seguridad. Los programas de formación deben incluir ejercicios de simulación de ciberataques y la formación en procedimientos de respuesta a incidentes. La educación continua es vital, dado el rápido ritmo de cambio en el panorama de amenazas.

La investigación y desarrollo en el campo de la ciberseguridad también es crucial. Las nuevas tecnologías, como la inteligencia artificial y el aprendizaje automático, ofrecen oportunidades para mejorar la defensa de infraestructuras críticas. Estas tecnologías pueden ayudar a identificar patrones de comportamiento inusuales y detectar ataques en sus etapas iniciales. La inversión en investigación permite desarrollar herramientas y técnicas avanzadas para proteger las infraestructuras críticas contra amenazas emergentes.

En resumen, la protección de infraestructuras críticas es una tarea compleja y multidimensional que requiere un enfoque coordinado y sostenido. La cooperación entre gobiernos, el sector privado y la comunidad internacional es esencial para asegurar la resiliencia de estos sistemas vitales. A medida que las amenazas evolucionan, también deben hacerlo nuestras estrategias y tecnologías de defensa, asegurando que estamos preparados para enfrentar los desafíos del futuro.

X – Desinformación masiva

“FAKE NEWS”. No hay que ser un experto o alguien adentrado en el tema para haberlas conocido de primera mano, es una realidad que todos hemos vivido. A día de hoy, internet está plagado de estas. Mayormente noticias falsas creadas con la finalidad de generar un par de clicks de más para lograr contribuir con el crecimiento de esa página, o en su peor versión generar repercusión mediática.

La repercusión mediática generada por una noticia falsa, claramente repercute a un gran nivel en la población sin importar el rango afectado, es decir, sin importar si hablamos de una noticia compartida entre dos personas por una red social o aquella transmitida por grandes medios de información que tal vez no confirmaron de manera correcta sus fuentes.

Las noticias falsas tienen el poder de moldear opiniones, influir en decisiones y, en algunos casos, incitar al odio o la violencia. La propagación de desinformación puede causar pánico, desacreditar a personas y organizaciones y distorsionar la percepción pública sobre temas importantes. Por ejemplo, durante eventos electorales, la difusión de fake news puede alterar el resultado de las votaciones al manipular la opinión pública.

Y es que aunque suene dramático, se puede decir que son una de las formas más eficaces de “contaminar” la democracia de un país. De ellas podemos tomar casos donde se han interferido campañas electorales de manera muy grave, como puede ser el de las elecciones parlamentarias ucranianas del 2014.

En octubre de 2014, poco antes de las elecciones parlamentarias en Ucrania, un grupo hacktivista pro-ruso denominado CyberBerkut, presuntamente vinculado al grupo de hackers GRU conocido como APT28 o Fancy Bear, llevó a cabo un ataque cibernético significativo contra el sistema electoral ucraniano. Este incidente se inscribe en el contexto más amplio del conflicto entre Rusia y Ucrania, que había comenzado con la anexión de la península de Crimea por parte de Rusia en febrero-marzo de 2014.

El ataque se ejecutó en varias fases críticas:

- **Compromiso del Sistema Electoral:** Cuatro días antes de las elecciones, el sistema central electoral de Ucrania fue comprometido. Los atacantes eliminaron archivos críticos, dejando inoperante el sistema de recuento de votos.

- **Publicación de Datos Exfiltrados:** Tres días antes de las elecciones, CyberBerkut publicó datos exfiltrados en internet como prueba de su éxito.

- **Instalación de Malware:** Se instaló malware diseñado para falsificar los resultados electorales, mostrando al candidato ultranacionalista Dmytro Yarosh como ganador con el 37% de los votos, y al candidato Petro Poroshenko con el 29%.

Inmediatamente después del cierre de las urnas, el sitio web de la Comisión Central Electoral de Ucrania fue derribado por un ataque de denegación de servicio distribuido (DDoS), que satura una red con solicitudes de comunicación,

ralentizándola o inhabilitándola. Este ataque fue calificado por funcionarios de seguridad ucranianos como parte de una guerra de información en curso contra el estado ucraniano.

A pesar de la gravedad del ataque, el sistema de recuento de votos fue restaurado mediante el uso de copias de seguridad tres días antes de las elecciones. Los expertos en ciberseguridad ucranianos lograron eliminar el malware 40 minutos antes de que los resultados electorales se hicieran públicos, evitando la difusión de resultados falsos. Sin embargo, los resultados de la elección se retrasaron por dos horas debido a estos problemas técnicos.

La Comisión Central Electoral describió el ataque como "un componente más en una guerra de información contra nuestro estado". Este incidente es parte de un patrón más amplio de ciberoperaciones y de desinformación que forman parte del conflicto entre Rusia y Ucrania.

Tras la restauración del sistema y la correcta publicación de los resultados electorales, los medios rusos, no obstante, informaron erróneamente que Dmytro Yarosh había ganado las elecciones, a pesar de que dichos resultados nunca fueron publicados oficialmente por Ucrania.

El ataque de 2014 fue un preludio a una serie de ciberataques posteriores contra Ucrania, incluyendo una operación significativa contra la red eléctrica en 2015. Para mitigar futuras amenazas, las autoridades ucranianas anunciaron en 2018 su intención de actualizar su infraestructura tecnológica antes de las elecciones presidenciales de 2019, reconociendo la necesidad de fortalecer la ciberseguridad ante la creciente sofisticación de las amenazas.

A su vez otro caso ocurrido fue el 5 de mayo de 2017 dónde se descubrió un ataque cibernético significativo contra el partido político francés En Marche, liderado por el entonces candidato presidencial Emmanuel Macron. Nuevamente el grupo de hackers conocido como APT28, fue señalado como el presunto responsable del ataque, según la inteligencia estadounidense.

El propósito aparente del ataque era influir en la opinión pública y afectar el resultado de la elección presidencial francesa de 2017. En el momento de la filtración, Emmanuel Macron lideraba las encuestas con una proyección de ganar con un 62-63% de los votos. Al introducir documentos falsos junto a los genuinos, los atacantes buscaban socavar la confianza en Macron y su partido, afectando potencialmente el voto de los ciudadanos.

A pesar de la filtración masiva de información y los intentos de manipular la percepción pública, Emmanuel Macron ganó la elección presidencial con un amplio margen, obteniendo el 66% de los votos frente al 34% de su oponente, Marine Le Pen, del partido Frente Nacional.

El hackeo durante la elección presidencial francesa de 2017 subrayó la creciente vulnerabilidad de los procesos electorales nacionales frente a las interferencias de actores no estatales y estados extranjeros. Este incidente no solo expuso la capacidad de los hackers para infiltrarse en sistemas críticos, sino que también reveló la necesidad urgente de mejorar la ciberseguridad para proteger la integridad de las elecciones y otros procesos democráticos.

La implicación de actores como APT28, vinculado al GRU ruso, en estas actividades cibernéticas, subraya la dimensión geopolítica de las ciberamenazas actuales. Las acciones emprendidas por estos grupos no solo buscan robar información, sino también desestabilizar procesos políticos y erosionar la confianza pública en las instituciones democráticas. La respuesta a estos desafíos requiere una combinación de medidas técnicas, políticas y diplomáticas para salvaguardar la soberanía de los procesos electorales en un mundo cada vez más digitalizado.

Las noticias falsas, o "fake news", no son un fenómeno nuevo, pero su proliferación ha sido exacerbada por la era digital. Las redes sociales y otras plataformas en línea permiten una difusión rápida y amplia de información, lo que hace que sea más fácil para las noticias falsas ganar tracción. Estas noticias suelen estar diseñadas para provocar una respuesta emocional fuerte, ya sea indignación, miedo o euforia, con el objetivo de captar la atención y ser compartidas masivamente.

El impacto de las noticias falsas puede ser devastador. Por ejemplo, durante la pandemia de COVID-19, se difundieron muchas informaciones erróneas sobre la eficacia de ciertos tratamientos y las medidas de prevención. Esto no solo confundió al público, sino que también llevó a prácticas peligrosas y a una resistencia contra las políticas de salud pública.
Combatir las noticias falsas y la desinformación requiere un enfoque multifacético. Algunas de las estrategias más efectivas incluyen:

- **Educación Mediática:** Fomentar la alfabetización mediática para que el público pueda identificar fuentes fiables y evaluar críticamente la información que encuentra en línea.

- **Regulación y Políticas:** Implementar regulaciones que obliguen a las plataformas digitales a ser más transparentes en sus algoritmos y prácticas de moderación, y que penalicen la difusión intencional de desinformación.

- **Innovación Tecnológica:** Desarrollar y utilizar herramientas avanzadas para detectar y mitigar las noticias falsas y los ciberataques. Esto puede incluir inteligencia artificial para la verificación de hechos y la identificación de patrones de comportamiento anómalos en línea.

La lucha contra las noticias falsas y la desinformación es una tarea continua y desafiante. Requiere un esfuerzo concertado de gobiernos, organizaciones internacionales, empresas tecnológicas y ciudadanos. Solo mediante la combinación de educación, regulación, innovación y colaboración se puede proteger la integridad de las democracias y asegurar que la información veraz prevalezca en la era digital.

XI – Un Ataque de magnitud internacional

He decidido nombrar a esta parte “Un Ataque de magnitud Internacional”, por el hecho que, a lo largo de este texto, nos hemos referido en su mayoría de ataques dirigidos contra objetivos específicos, y solo hemos hecho hincapié unas pocas veces de un ataque que puede ser una pesadilla para la ciberseguridad mundial. Pero que a diferencia de un mal sueño, que solo queda en el inconsciente de las personas, estos incidentes ya los hemos visto realizarse varias veces, aunque en una medida menor.

Con esto quiero hacer alusión a un ataque generalizado, la liberación de un mal que genere estragos, que no discriminen por nacionalidad, o empresas o civiles. Un ataque que se geste de manera masiva y exclusivamente internacional.

Este tipo de ataque podría manifestarse de diversas formas, desde un ataque coordinado contra infraestructuras críticas, como el suministro de energía o las redes de comunicaciones, hasta una campaña de desinformación masiva diseñada para socavar la confianza en las instituciones y en la sociedad en su conjunto.

El impacto de un ataque de esta magnitud sería devastador. Podría paralizar economías enteras, causar interrupciones en los servicios básicos, y sembrar el caos y la confusión en todas partes. Además, en un mundo cada vez más interconectado digitalmente, las repercusiones se sentirían en todos lados, sin importar la ubicación geográfica.

Una de las mayores preocupaciones con respecto a este tipo de ataques es su capacidad para superar las defensas tradicionales de ciberseguridad. A medida que los ciberdelincuentes se vuelven más sofisticados y aprovechan tecnologías

emergentes como la inteligencia artificial y el aprendizaje automático, las organizaciones se enfrentan a un enemigo cada vez más difícil de detectar y combatir.

Si bien suena alarmante, podemos pensar en casos que se podrían llegar a considerar como similares o posiblemente parecidos, aunque a una menor escala. Entre ellos podemos encontrar nuestros primeros casos a comentar cómo son en el 2017 los hechos ocurridos por WannaCry y NotPetya.

Los ciberataques masivos perpetrados por los ransomware WannaCry y NotPetya en 2017, marcaron un hito en la conciencia mundial sobre la vulnerabilidad de las infraestructuras digitales y la amenaza que representan los actores estatales y grupos de hackers en el ciberespacio.

El ataque de WannaCry en mayo de 2017 fue un punto de inflexión en la historia de la ciberseguridad, demostrando la capacidad devastadora de un ataque coordinado a gran escala. La propagación del malware comenzó como una serie de infecciones aisladas que rápidamente se convirtieron en una epidemia digital global, afectando a organizaciones de todos los tamaños y sectores en más de 150 países.

Una de las características más preocupantes de WannaCry fue su metodología de ataque altamente eficiente. El malware explotaba una vulnerabilidad en el protocolo de compartición de archivos de Windows, conocida como "EternalBlue", de la cual hemos hablado anteriormente.
Esta vulnerabilidad permitía a WannaCry propagarse rápidamente a través de las redes internas de las organizaciones, infectando computadoras en cuestión de minutos.

El impacto de WannaCry fue especialmente grave en el sector de la salud, con el NHS del Reino Unido siendo uno de los objetivos más prominentes. El malware paralizó los sistemas informáticos del NHS, obligando a cancelar citas médicas, retrasar cirugías y desviar ambulancias a hospitales no afectados. Además del sector de la salud, empresas multinacionales como Telefónica, Renault y FedEx también se vieron afectadas, experimentando interrupciones significativas en sus operaciones diarias.

La motivación detrás del ataque, según los expertos, fue principalmente financiera. Se estima que los hackers norcoreanos responsables de WannaCry buscaban obtener ganancias rápidas en un momento en que Corea del Norte enfrentaba crecientes sanciones económicas internacionales. El hecho de que el rescate exigido por el malware fuera relativamente bajo, alrededor de $300 dolares en bitcoins, sugiere que los atacantes estaban más interesados en obtener un volumen alto de pagos que en maximizar el valor de cada rescate individual.

Además del impacto económico, WannaCry generó una ola de preocupación en todo el mundo sobre la seguridad cibernética y la capacidad de los actores estatales para causar daño a gran escala en el ciberespacio. El incidente llevó a un aumento en la conciencia pública sobre la importancia de mantener actualizados los sistemas y aplicar parches de seguridad, así como a una mayor colaboración entre gobiernos y empresas para abordar las ciberamenazas.

Por otro lado, tenemos el ataque de NotPetya en junio de 2017 que fue otro golpe devastador para la ciberseguridad global, con consecuencias económicas y operativas que se sintieron en todo el mundo. Aunque inicialmente se pensó que

NotPetya era un ransomware diseñado para extorsionar dinero a las víctimas, investigaciones posteriores sugirieron que su verdadero propósito podría haber sido causar daños económicos y operativos a gran escala.

El malware se propagó inicialmente a través de una actualización comprometida del software de contabilidad fiscal MeDoc, utilizado por muchas empresas en Ucrania. Una vez dentro de una red corporativa, NotPetya se propagaba rápidamente, utilizando la misma vulnerabilidad "EternalBlue" que WannaCry para infectar computadoras en toda la organización. A diferencia de WannaCry, sin embargo, NotPetya no intentaba recuperar dinero de sus víctimas, en cambio, encriptaba los archivos de los usuarios de manera irreparable, causando daños económicos masivos y paralizando las operaciones comerciales.

El ataque afectó a empresas multinacionales de renombre, incluidas Maersk, Merck y FedEx, que experimentaron pérdidas económicas significativas y disrupciones operativas prolongadas. Además, el sistema de monitoreo de radiación en la planta de energía nuclear de Chernóbil fue desactivado por el malware, generando preocupaciones sobre la seguridad de las infraestructuras críticas.

Aunque inicialmente se sospechaba que Rusia estaba detrás del ataque, el gobierno ruso negó cualquier participación y las investigaciones posteriores no pudieron establecer una atribución definitiva. Sin embargo, el incidente provocó una intensificación de las tensiones geopolíticas y un renovado enfoque en la seguridad cibernética a nivel mundial.

Otro ejemplo de un ataque de estos niveles relacionados con el ransomware, fue SamSam, en el cual durante el primer trimestre de 2018, varios gobiernos locales

experimentaron incidentes significativos relacionados con el ransomware SamSam. Este software malicioso, cuyas primeras versiones datan de 2015, también era conocido en ese momento como Samas y SamsamCrypt .

La filial de Dell, Secureworks Inc, asoció el ransomware SamSam con el actor de amenazas conocido como Gold Lowell . Este grupo, o red de actores estrechamente afiliados, es conocido por usar tácticas de escaneo y explotación de vulnerabilidades . En noviembre de 2018, dos iraníes fueron acusados en relación con el ransomware SamSam .

El ransomware SamSam se dirigió principalmente a gobiernos locales, hospitales y empresas de registros de salud. Entre los objetivos específicos se encontraban gobiernos municipales en Colorado y Nuevo México, así como asociaciones médicas en Indiana, Virginia, Nueva York y Buffalo . Un ataque particularmente destacado fue el de marzo de 2018 contra los servicios municipales de Atlanta .

Los ataques de SamSam se infiltraron en los sistemas explotando vulnerabilidades en los protocolos de escritorio remoto y otros componentes de red pública, o adivinando contraseñas . Estos ataques se caracterizaron por una supervisión meticulosa y una capacidad de adaptación a los esfuerzos de remediación de las víctimas . SamSam se actualizaba frecuentemente para escapar de la detección de antivirus y otras defensas de los puntos finales . Los atacantes exigían un rescate pagado en Bitcoin .

El propósito de los ataques era puramente financiero. El monto del rescate se establecía cuidadosamente para que fuera asequible para la víctima pero rentable para los atacantes . Los atacantes ofrecían descifrar un sistema no esencial de forma gratuita para demostrar su capacidad de liberar los datos si se pagaba el rescate .

Entre diciembre de 2017 y marzo de 2018, el ransomware SamSam recaudó aproximadamente un millón de dólares, aunque la cantidad exacta dependía del valor fluctuante del Bitcoin . En el caso de Atlanta, los atacantes exigieron un rescate de aproximadamente $51,000 dólares en Bitcoin, pero la ciudad se negó a pagar. El daño total incurrido por la ciudad superó los $17 millones de dólares . Los analistas señalaron que las víctimas a menudo prefieren pagar el rescate en lugar de enfrentar el daño y los riesgos de un tiempo de inactividad prolongado en los servicios .

El último caso a exponer es el del ataque de ransomware en la red satelital KA-SAT de Viasat, el cual el 24 de febrero de 2022, entre las 5 am y las 9 am EEST, se produjo un ciberataque significativo que afectó a la red satelital KA-SAT de Viasat. Este incidente fue atribuido a hackers rusos, según afirmaciones de Víctor Zhora, jefe adjunto del Servicio Estatal de Comunicaciones Especiales y Protección de la Información de Ucrania, y fue investigado por analistas de inteligencia estadounidenses como un posible ataque patrocinado por el estado ruso .

Los analistas de ciberseguridad y agencias de inteligencia de EE. UU. sugirieron que la agencia de inteligencia militar de Rusia (GRU) podría estar detrás del ataque . La firma de ciberseguridad SentinelOne indicó que el malware utilizado, un tipo raro de wiper, mostró similitudes de desarrollo con el "VPNFilter", previamente atribuido al grupo APT28 (también conocido como "Fancy Bear") por el FBI en 2018 y

posteriormente al grupo Sandworm por la NSA, ambos supuestamente respaldados por el GRU ruso .

El 10 de mayo de 2022, el Centro Nacional de Seguridad Cibernética del Reino Unido, el Departamento de Estado de EE. UU. y el Consejo de la UE atribuyeron oficialmente el ataque a Rusia, aunque este país ha negado repetidamente llevar a cabo ciberoperaciones ofensivas.

El ataque afectó a usuarios de módems en la red satelital KA-SAT de Viasat, especialmente en Ucrania, pero también impactó a un número considerable de clientes en toda Europa . Los sistemas específicos atacados incluyeron la infraestructura de red terrestre de KA-SAT, particularmente el sistema de gestión de la red y el sistema de archivos de los módems .

Según Viasat, el ataque fue un incidente de dos fases: primero, un ataque de denegación de servicio dirigido proveniente de módems y equipos de clientes ubicados en Ucrania que dejó fuera de línea a varios módems; y segundo, una disminución gradual de los módems conectados en el sistema . Los atacantes explotaron una "configuración incorrecta en un dispositivo VPN" para obtener acceso remoto a un segmento de gestión de la red terrestre y luego se movieron lateralmente a un segmento utilizado para operar la red, ejecutando comandos de gestión legítimos en un gran número de módems residenciales simultáneamente, sobrescribiendo datos clave en la memoria flash de los módems e impidiéndoles acceder a la red .

El 31 de marzo, la firma de ciberseguridad SentinelOne presentó un análisis alternativo, afirmando que los atacantes probablemente llevaron a cabo un ataque a

la cadena de suministro y utilizaron el malware wiper genérico "AcidRain" diseñado para sobrescribir los datos clave en la memoria flash de los módems y en los archivos del sistema, antes de intentar destruir los datos y reiniciar los dispositivos, dejándolos inoperativos .

El ataque tenía como objetivo interrumpir el servicio al dejar inoperables los módems de un conjunto específico de clientes, sin comprometer el satélite KA-SAT en sí ni la infraestructura terrestre de soporte, y sin evidencia de acceso a los datos de los usuarios o equipos personales . Funcionarios públicos señalaron que el propósito era interrumpir las comunicaciones satelitales en Ucrania en medio de la intensificación del conflicto en la región el 24 de febrero de 2022 . Expertos afirmaron que la red de Viasat también proporcionaba servicios de comunicación a las fuerzas militares y de seguridad ucranianas, y que el ataque podría haber tenido la intención de impactar "aspectos del comando y control militar en Ucrania" .

El ataque dejó inoperables miles de módems de banda ancha satelital KA-SAT de Viasat en Ucrania, incluidos aquellos utilizados por agencias militares y gubernamentales, causando una gran pérdida de comunicación por internet . También impactó a decenas de miles de clientes en toda Europa, incluyendo usuarios de internet satelital en Polonia, Alemania, Reino Unido, Francia y la República Checa . El derrame del ataque incluyó la interrupción del monitoreo remoto y control de 5,800 turbinas eólicas en Alemania operadas por Enercon, que estuvieron fuera de línea durante varias semanas .

Aunque los módems no se volvieron permanentemente inoperables, solo podían ser restaurados mediante un reinicio de fábrica. Viasat no proporcionó información

precisa sobre el número de dispositivos afectados, pero afirmó que "casi 30.000 módems nuevos ya habían sido enviados a distribuidores para restaurar a los clientes". La Agencia de Ciberseguridad de la UE informó que al menos 27.000 dispositivos fueron impactados .

Sin embargo, el ataque no comprometió a los usuarios de otras redes de Viasat a nivel mundial, incluyendo aerolíneas u otros usuarios gubernamentales de la red satelital KA-SAT. Tampoco dañó el satélite ni la infraestructura de red, y no hubo evidencia de impacto en los datos de los usuarios o acceso a los equipos personales de los clientes .

A pesar de que las acciones de mitigación y recuperación para estabilizar la red y restaurar el servicio comenzaron de inmediato, miles de clientes seguían sin conexión en mayo de 2022 . El portavoz de la compañía afirmó que la prioridad en la recuperación se dio a la "infraestructura crítica y asistencia humanitaria" . Viasat afirmó que, aunque en ciertos casos los módems recibieron actualizaciones de software "por aire" de manera oportuna, se enviaron alrededor de 30.000 módems nuevos para restaurar efectivamente la funcionalidad del servicio, y continuó el suministro según la solicitud de los distribuidores. Además, destacó que estaba trabajando en la mejora de la seguridad de la red .

El 30 de marzo de 2022, Reuters informó que Viasat aún estaba presenciando algunos intentos repetidos de interferir con los servicios satelitales, pero que estos estaban siendo frustrados por medidas defensivas . En mayo de 2022, el ataque estaba siendo investigado por firmas de ciberseguridad contratadas por Viasat y múltiples agencias de inteligencia y seguridad, incluidas la Agencia de Seguridad

Nacional de EE. UU., la agencia de ciberseguridad francesa y la inteligencia ucraniana .

Hemos analizado la amenaza que representan los ciberataques de escala internacional, destacando su capacidad para causar estragos indiscriminados en infraestructuras críticas, economías y servicios básicos en todo el mundo. Ejemplos históricos como los ataques de WannaCry, NotPetya, SamSam y el reciente incidente con Viasat, evidencian la evolución y sofisticación de estos ciberataques. Estos incidentes subrayan la vulnerabilidad de nuestras infraestructuras digitales y la necesidad urgente de fortalecer las defensas a nivel global. Es crucial aumentar la colaboración entre gobiernos y sectores privados para desarrollar estrategias de prevención y respuesta efectivas, así como mantener un enfoque constante en la actualización y protección de los sistemas tecnológicos.

XII - Bloqueo de Internet

Consideremos un escenario que supone uno de los mayores temores que podría generar caos en la población de niveles realmente elevados: la posibilidad de un bloqueo masivo de la red de redes, Internet.

Un bloqueo de internet en una región determinada, podría sembrar un caos que llevaría al declive parcial de esa sociedad. Pero primero partamos de un ejemplo más básico, el S24[5] planteado por el proyecto "International Cyber Law: Interactive toolkit". Este plantea que:

En respuesta a crecientes protestas ciudadanas que han captado la atención global, el gobierno del Estado A decide implementar un apagón total de internet en su territorio. Esta medida drástica tiene un impacto significativo en la vida diaria de sus ciudadanos, interrumpiendo sus comunicaciones y actividad económica.

El apagón incluye una orden a todas las redes y proveedores de servicios de internet en el Estado A para que detengan el intercambio de tráfico de internet con redes de otros países. El Estado A adopta esta medida sin informar previamente a otros Estados de su intención de suspender el tráfico internacional de internet. Con plena conciencia de que estas acciones obstaculizarán la conectividad a internet en el vecino Estado B, el Estado A no toma medidas para mitigar este impacto.

El Estado B, con solo un proveedor de servicios de internet (ISP), depende en gran medida del intercambio de tráfico con un ISP líder en el Estado A. Debido a la exigencia gubernamental de aislar su red de internet, el Estado B sufre una

[5] Scenario 24: Internet blockage. (2023, February 4). International cyber law: interactive toolkit

interrupción repentina y generalizada de internet, que persiste durante todo el tiempo que dura el apagón en el Estado A. Esto desconecta a una gran parte de la población del Estado B de internet, mientras que el resto de la población experimenta conexiones extremadamente lentas.

Los habitantes del Estado B dependen de la conectividad con redes globales para llevar a cabo actividades diarias y económicas esenciales. Como resultado del apagón, oficinas gubernamentales y servicios esenciales en el Estado B, incluidos hospitales, bancos y fuerzas del orden, se ven significativamente limitados en su capacidad de funcionar. No obstante, otras infraestructuras críticas dentro del Estado B, como la red eléctrica, instalaciones militares y satelitales, y el control de tráfico aéreo, continúan operando normalmente durante el periodo del apagón.

En este caso de ejemplo podemos vislumbrar un escenario donde un corte de internet generado de manera intencional ha afectado de manera significativa el desempeño de funciones públicas y privadas de un estado, y de manera indirecta, solo porque su país vecino ha decidido realizar un bloqueo masivo del internet para socavar las protestas originadas en su territorio, ha afectado al estado B.

Suena alarmante cuando nos planteamos una situación así, y vemos que tantos organismos requieren internet para el correcto funcionamiento de sus actividades. Ahora imaginemos por un minuto que el bloqueo de internet no se da por un estado que lo regule hacia su población, como método de aminorar daños causados por protestas, y tampoco se da una disminución hacia el estado B, es más eliminemos este estado del escenario. Solo dejemos el estado A, el cual diremos que sufre un ataque de actores estatales o no estatales que logran bloquear el acceso completo a internet al estado A ¿qué ocurriría?.

En este escenario hipotético, el impacto de un ataque cibernético que bloquea completamente el acceso a internet en el Estado A tendría consecuencias caóticas en múltiples niveles:

Comunicaciones: La interrupción total de internet desactivaría los principales canales de comunicación utilizados por ciudadanos y empresas, como correos electrónicos, aplicaciones de mensajería instantánea y plataformas de videoconferencia. Esto aislaría a los individuos, dificultando la comunicación incluso dentro del mismo país y complicando la coordinación de respuesta ante la crisis.

Economía: La economía moderna está intrínsecamente ligada a la conectividad a internet. Sectores clave como la banca, el comercio electrónico, y los mercados financieros dependen del acceso continuo a internet. Un bloqueo podría resultar en la paralización de transacciones financieras, la interrupción de cadenas de suministro y la imposibilidad de realizar operaciones comerciales, causando pérdidas económicas masivas.

Servicios Públicos y Gobierno: Muchos servicios públicos, incluyendo la administración gubernamental, la sanidad y la seguridad pública, utilizan internet para operar eficientemente. La falta de acceso a internet podría desestabilizar la prestación de servicios esenciales. Por ejemplo, los sistemas de gestión hospitalaria que dependen de internet para acceder a registros médicos, coordinar tratamientos y gestionar recursos enfrentarían serios desafíos.

Seguridad Nacional: En un contexto de bloqueo completo de internet debido a un ciberataque, la capacidad de respuesta del Estado A ante amenazas tanto internas como externas se vería gravemente afectada. La coordinación entre agencias de seguridad, la comunicación con aliados y la gestión de la defensa nacional dependen en gran medida de las redes de comunicación digital.

Infraestructura Crítica: La interrupción del internet afectaría también a otras infraestructuras críticas que dependen de la conectividad digital para su operación y control. Sistemas de control industrial, plantas de energía, redes de agua potable y sistemas de transporte podrían experimentar fallos o interrupciones en sus operaciones. Un colapso en estas infraestructuras podría llevar a apagones masivos, escasez de agua y caos en el transporte público y aéreo, afectando gravemente la vida cotidiana y la seguridad de los ciudadanos.

En pocas palabras, se podría considerar que la sociedad empezaría a actuar en declive, los ciudadanos y las empresas entran en un estado de desorientación y pánico. La falta de información clara y confiable exacerba la situación, y comienzan a circular rumores y desinformación. El gobierno y las agencias de seguridad intentan coordinar una respuesta utilizando métodos de comunicación alternativos, como radios, sistemas de comunicación por satélite y redes móviles no basadas en internet. Sin embargo, la eficacia de estas medidas es limitada debido a la falta de preparación y recursos. Es decir nos encontraríamos frente a un desastre devastador.

Un escenario así recuerda mucho a la novela "Leave the World Behind" de Rumaan Alam donde se explora las consecuencias de una catástrofe tecnológica y cómo afecta a un grupo de personas en un entorno aislado. En el contexto del bloqueo total de internet en el Estado A, hay paralelismos claros que se pueden extraer de la

narrativa de Alam para ilustrar cómo una sociedad podría enfrentar y adaptarse a tal crisis.

En conclusión, un bloqueo total de internet podría desatar una cadena de eventos que paralizarían la vida moderna, desde la economía y los servicios públicos hasta la seguridad y el bienestar social. La dependencia extrema de la tecnología y la falta de preparativos adecuados podrían llevar a una situación de caos y desintegración social, subrayando la necesidad de desarrollar estrategias robustas para mitigar los impactos de tales desastres tecnológicos.

Pero ¿hemos vivido algo parecido a esta novela de ficción? La realidad es que afortunadamente aún no hemos vivido una situación de esos niveles pero hemos enfrentados otras, como en el año 2008, donde se registró un incidente cuyo actor no ha sido identificado, con Bangladesh como la víctima, que afectó los sistemas objetivos de cables submarinos que conectaban Bangladesh con otras partes del mundo. El método utilizado implicó el daño o la ruptura de un cable submarino. El propósito detrás de este acto no ha sido especificado. Como resultado, se produjo una interrupción en la conectividad a Internet en varios países, incluyendo Bangladesh.

Otro caso fue el 23 de noviembre de 2019, donde Irán se convirtió en el actor principal en un incidente que implicó un apagón de Internet en el país. Los sistemas objetivo fueron los proveedores de servicios de Internet en Irán. Este apagón se produjo como respuesta a protestas internas, siendo ordenado por el gobierno iraní y extendiéndose a lo largo de una semana. Algunas redes retiraron completamente sus rutas de tráfico, mientras que otras simplemente bloquearon el mismo. Es

importante destacar que, durante el apagón, la “red nacional de información” de Irán, es decir, la infraestructura de red interna, se mantuvo y seguía siendo accesible.

El propósito de este apagón fue sofocar las protestas internas. Aunque los iraníes se vieron profundamente afectados, no se ha informado ampliamente si el apagón afectó a otras jurisdicciones.

Como vemos estos casos no son comparables a la novela de Alam, pero nos demuestran que la situación es un hecho latente. En el mundo interconectado en el que vivimos, la idea de un bloqueo total de internet puede parecer una premisa de ciencia ficción. Sin embargo, como hemos visto en los incidentes reales que han afectado a países como Bangladesh e Irán, la vulnerabilidad de nuestras redes digitales es una realidad que no podemos ignorar.

La narrativa distópica de "Leave the World Behind" de Rumaan Alam nos ofrece una visión especulativa pero inquietantemente plausible de cómo podría ser un mundo sin internet. Aunque aún no hemos experimentado un escenario de esa magnitud, los incidentes pasados nos advierten sobre la fragilidad de nuestras infraestructuras digitales y la facilidad con la que pueden ser atacadas o manipuladas.

Imaginemos un mundo donde la conectividad digital es abruptamente interrumpida. Las repercusiones serían catastróficas en todos los aspectos de la vida moderna. Desde la comunicación y la economía hasta la seguridad nacional y la infraestructura crítica, todos estos pilares se verían amenazados por un bloqueo total de internet.

Conclusión

La evolución de la guerra al ciberespacio no solo ha transformado las tácticas y estrategias de conflicto, sino que ha redefinido los conceptos de seguridad, soberanía y poder en la era digital, afectando a todos los niveles de la sociedad global.

La guerra, en su evolución histórica, ha adoptado múltiples formas impulsadas por avances tecnológicos. En la era digital, la guerra se ha trasladado al ciberespacio, una arena invisible pero omnipresente, donde las batallas se libran por el control de la información y la infraestructura digital.

El ciberespacio ha emergido como un nuevo campo de batalla donde las guerras no se libran con armas convencionales, sino con bits y bytes. Esta transformación ha llevado a un replanteamiento profundo de lo que significa la seguridad en el siglo XXI. Los ciberataques pueden originarse en cualquier parte del mundo, cruzando fronteras sin ser detectados hasta que es demasiado tarde. Este escenario globalizado y deslocalizado complica la defensa y la atribución de los ataques, planteando nuevos desafíos a las naciones y organizaciones.

Los actores en el ciberespacio son diversos y van desde estados nacionales y sus ejércitos cibernéticos hasta hackers independientes y organizaciones criminales. Cada uno con sus propias motivaciones, ya sean políticas, económicas o ideológicas. Esta variedad de actores incrementa la complejidad del panorama de amenazas, ya que las tácticas y objetivos pueden variar drásticamente.

Los estados han reconocido rápidamente el potencial del ciberespacio como una extensión de su poder nacional. Las naciones utilizan ciberoperaciones para obtener

ventajas estratégicas, recolectar inteligencia, y ejercer presión política y económica. En este contexto, el ciberespacio se convierte en un nuevo campo de batalla donde las reglas tradicionales de la diplomacia y el conflicto no siempre se aplican. Los estados emplean una variedad de tácticas, desde el espionaje cibernético hasta los ataques directos a infraestructuras críticas de sus adversarios, con la meta de alcanzar sus objetivos geopolíticos.

Además de los estados, una variedad de actores no estatales también ha emergido en el ciberespacio. Grupos de hackers, organizaciones criminales y colectivos hacktivistas operan con agendas propias, a veces en colaboración con estados y otras veces de forma independiente. Estos actores pueden influir en la política internacional al desestabilizar gobiernos, revelar información sensible y llevar a cabo ataques que impactan la economía global.

El ciberespacio también ha alterado las dinámicas de seguridad global. La facilidad con la que los ataques cibernéticos pueden ser lanzados y la dificultad para atribuirlos han hecho que las estrategias de disuasión convencionales sean menos efectivas. Los estados ahora deben desarrollar nuevas estrategias para prevenir y responder a las ciberamenazas. Estas estrategias incluyen mejorar las capacidades de ciberdefensa, establecer alianzas internacionales para la cooperación en ciberseguridad, y participar en ciberdiplomacia para establecer normas y acuerdos internacionales que regulen el comportamiento en el ciberespacio.

La ciberseguridad, por lo tanto, no es solo una cuestión técnica, sino también una cuestión de política y diplomacia internacional. Los estados deben navegar en este complejo entorno para proteger sus intereses nacionales, al mismo tiempo que trabajan juntos para mantener la estabilidad y la seguridad global. La cooperación

internacional y la confianza mutua son esenciales para desarrollar un ciberespacio seguro y estable.

El impacto del ciberespacio en las relaciones internacionales también se refleja en la necesidad de marcos legales y normativos adecuados. La creación de leyes internacionales que regulen el comportamiento en el ciberespacio es fundamental para prevenir conflictos y garantizar la responsabilidad. Sin embargo, la rápida evolución de la tecnología y la diversidad de actores implicados complican la implementación de estas normas.

El ciberespacio seguirá evolucionando y su impacto en las relaciones internacionales y la seguridad global será cada vez más significativo. A medida que las tecnologías avanzan y se integran más profundamente en todos los aspectos de la vida cotidiana, las amenazas y oportunidades en el ciberespacio también se multiplicarán.

Las innovaciones tecnológicas, como la inteligencia artificial (IA), el Internet de las cosas (IoT) y el blockchain, están cambiando rápidamente el panorama del ciberespacio. Estas tecnologías ofrecen enormes beneficios, pero también presentan nuevos riesgos y desafíos de seguridad. La IA, por ejemplo, puede utilizarse tanto para mejorar las ciberdefensas como para llevar a cabo ataques más sofisticados. El IoT, con su creciente red de dispositivos interconectados, amplía la superficie de ataque y crea nuevas vulnerabilidades. El blockchain, aunque promete mejorar la seguridad y la transparencia, también puede ser explotado por actores malintencionados.

La capacidad de adaptarse a estas innovaciones tecnológicas y mitigar las amenazas emergentes será crucial para la seguridad en el ciberespacio. Los estados y

organizaciones deberán invertir en investigación y desarrollo, así como en la formación continua de su personal, para mantenerse a la vanguardia de estos avances.

El desarrollo de capacidades en ciberseguridad es una prioridad para todos los estados y organizaciones. Esto incluye la construcción de infraestructuras seguras, la implementación de políticas y procedimientos de seguridad eficaces, y la capacitación de profesionales en ciberseguridad. Además, es esencial fomentar una cultura de ciberseguridad en la sociedad en general, para que todos los ciudadanos comprendan la importancia de la seguridad en línea y adopten prácticas seguras.

La resiliencia es otra dimensión crucial. Las organizaciones deben ser capaces de resistir y recuperarse de los ciberataques. Esto implica no solo la prevención y la detección temprana, sino también la capacidad de respuesta rápida y la recuperación eficiente. Los planes de continuidad de negocio y la capacidad de restaurar sistemas y datos después de un ataque son componentes esenciales de una estrategia de resiliencia.

El ciberespacio también plantea importantes cuestiones éticas y de derechos humanos. La privacidad, la libertad de expresión y el acceso a la información son derechos fundamentales que deben protegerse en el entorno digital. Los estados y empresas tienen la responsabilidad de garantizar que sus acciones en el ciberespacio respeten estos derechos.

La vigilancia masiva, la censura y el uso de tecnologías para el control social son prácticas que deben ser cuidadosamente reguladas para evitar abusos. El desarrollo de políticas y marcos éticos que guíen el uso responsable de las tecnologías digitales

es crucial para asegurar que el ciberespacio siga siendo un lugar de libertad y oportunidad para todos.

Aquí se destaca la necesidad urgente de abordar los desafíos complejos y multifacéticos que presenta el ciberespacio. La idea de que el ciberespacio ha creado un nuevo terreno de poder y diplomacia se confirma a través de los análisis y ejemplos presentados. La protección y gestión eficaz del ciberespacio requieren un enfoque integrado que combine la innovación tecnológica, la cooperación internacional, el desarrollo de capacidades, la resiliencia y el respeto por los derechos humanos.

Solo a través de un esfuerzo concertado y colaborativo podremos asegurar que el ciberespacio se mantenga como un dominio seguro, justo y beneficioso para todas las naciones y actores involucrados. El futuro del ciberespacio depende de nuestra capacidad para enfrentar estos desafíos con determinación, creatividad y un compromiso inquebrantable con los valores fundamentales de libertad, seguridad y justicia.

Bibliografía

Alvarado, R., & Morales, R. (2012). Cibercrimen. IUS Ediciones

Annan, K. (2003). El Secretario General Discurso pronunciado en la Conferencia "La lucha contra el terrorismo en pro de la humanidad: una conferencia sobre las raíces del mal" (Nueva York, 22 de septiembre de 2003). United Nations. https://www.un.org/es/sg/annan_messages/2003/sgmessage_terror.htm

Baezner, M., & Robin, P. (2017). Stuxnet (No. 4). ETH Zurich.

Bangladesh internet outage (2008). (2021, September 17). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Bangladesh_internet_outage_(2008)?oldid=2828.

Byung-Chul Han. (2014). Psicopolítica. Herder

Carol V. Evans, Chris Anderson, Malcom Baker, Ronald Bearse, Salih Biçakci, Steve Bieber, Sungbaek Cho, Adrian Dwyer, Geoffrey French, David Harell, Alessandro Lazari, Raymond Mey, Theresa Sabonis-Helf, and Duane Verner, Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 1) (Carlisle, PA: US Army War College Press, 2022), https://press.armywarcollege.edu/monographs/955

Center for Strategic and International Studies. (2024). Significant Cyber Events Since 2006. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cloudflare. (-). What are Petya and NotPetya?. Cloudflare. https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/

Council on Foreign Relations. (n.d.). Cyber operations tracker. Retrieved May 31, 2024, from https://www.cfr.org/cyber-operations/

Cyber attacks against Estonia (2007). (2021, September 17). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007)?oldid=2812.

Eugene Kaspersky. (2012). The Flame That Changed the World.. EUGENE KASPERSKY – OFFICIAL BLOG. https://eugene.kaspersky.com/2012/06/14/the-flame-that-changed-the-world/#more-2717

Europol (2023), Informe sobre la situación y las tendencias del terrorismo en la Unión Europea - Resumen Ejecutivo, Oficina de Publicaciones de la Unión Europea, Luxemburgo.

French presidential election leak (2017). (2021, June 4). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/French_presidential_election_leak_(2017)?oldid=2404.

Georgia-Russia conflict (2008). (2021, September 17). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008)?oldid=2814.

George Chaya. (2019). Los grupos terroristas vuelven a impulsar el uso de las redes para reclutar nuevos miembros. Infobae. https://www.infobae.com/america/mundo/2019/11/10/los-grupos-terroristas-vuelven-a-impulsar-el-uso-de-las-redes-para-reclutar-nuevos-miembros/

Gómez, A. P. (2020). Ciberterrorismo, ¿una nueva amenaza?. bie3: Boletín IEEE, (19), 386-400

Illaro, E. L. (2014). Ciberguerra, los escenarios de confrontación. Pre-bie3, (1), 40.

Infobae. (2024). La ciberguerra en Ucrania es tan crucial como la batalla en las trincheras. Infobae. https://www.infobae.com/economist/2024/03/21/la-ciberguerra-en-ucrania-es-tan-crucial-como-la-batalla-en-las-trincheras/

José Levy. (2017). Terror: Alerta ISIS. Planeta

Kumar, Animesh, Zero Day Exploit (January 13, 2014). Available at SSRN: https://ssrn.com/abstract=2378317 or http://dx.doi.org/10.2139/ssrn.2378317

Mele, S. (2013). Cyber-weapons: legal and strategic aspects (Version 2.0). Available at SSRN 2518212.

NotPetya (2017). (2022, November 14). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)?oldid=3620.

Paula Las Heras. (2022). ¿Cómo recluta el ISIS a sus miembros?. Universidad de Navarra. https://www.unav.edu/web/global-affairs/como-recluta-el-isis-a-sus-miembros

Power grid cyberattack in Ukraine (2015). (2023, October 29). International cyber law: interactive toolkit. Retrieved 16:10, May 31, 2024 from https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015)?oldid=3949.

Sain, G. (2015). Historia de internet (I). Revista pensamiento penal.

SamSam ransomware incidents (2018). (2021, July 20). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/SamSam_ransomware_incidents_(2018)?oldid=2458.

Scenario 24: Internet blockage. (2023, February 4). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Scenario_24:_Internet_blockage?oldid=3724.

Silva, F. (2018). StuxNet–El software como herramienta de control geopolítico. revistapuce.

State University of New York. (s.f.). Ciberconflictos internacionales [Curso en línea]. Coursera. Recuperado de https://www.coursera.org/learn/cyber-conflicts

Trigo Santiago, Castellote Martín, Podestá Ariel, Ruiz de Angeli Gonzalo, Lamperti Sabrina, Constanzo Bruno. (2017). Ransomware: seguridad, investigación y tareas forenses. SEDICI. http://sedici.unlp.edu.ar/handle/10915/65216

Ukrainian parliamentary election interference (2014). (2021, July 6). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Ukrainian_parliamentary_election_interference_(2014)?oldid=2435.

Viasat KA-SAT attack (2022). (2022, May 29). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022)?oldid=3408.

WannaCry (2017). (2021, June 3). International cyber law: interactive toolkit. Retrieved from https://cyberlaw.ccdcoe.org/wiki/WannaCry_(2017)?oldid=2405.

Wolf, G. (2018). Funcionamiento de una Red Anonimizadora: La red Tor. Software Gurú, (56), 40-41.