Benemérita Universidad Autónoma de Puebla

Facultad de Derecho y Ciencias Sociales

Licenciatura en Relaciones Internacionales

El Ciberespacio Como Nueva Expresión De Poder En Las Relaciones Internacionales: El Caso del Ciberataque NotPetya a Ucrania en 2017

Alumno:
Alejandro Nava Chan

Matrícula: 201522155

Directora:
Dra. María Patricia Moreno Rosano

Fecha de Examen Profesional: 12/22

Dedicada a:

Mi madre, de quien admiro su gran fortaleza, resiliencia y capacidad de enfrentar los problemas con una sonrisa. A quien agradezco su apoyo incondicional en cada una de las metas que me planteo.

Mi padre, quien siempre ha sido un gran soporte para mí y mi familia, y que siempre tiene las palabras adecuadas que uno necesita escuchar. A quien espero asemejarme algún día por el cariño y calidez que brinda.

Mi hermana, por ser mi cómplice incondicional, mi apoyo y mi gran compañera de aventuras desde que éramos niños. Por ser mi compañera de equipo en las buenas y en las malas, y de quien admiro mucho su empatía y capacidad de ver por el prójimo.

Mis abuelitas, Elvira, Beta y Nene, por la atención, cuidado, amor y cariño que me han brindado desde que era niño, y cuyas experiencias y anécdotas me continúan enriqueciendo a cada día.

Mis amigos, y a cada una de las maravillosas personas que conocí durante la universidad, que, sin su compañía, apoyo y sonrisas dentro y fuera de las aulas, simplemente no sería la misma persona que soy ahora.

Mis tíos, Lety y Luis, por su apoyo y motivación en cada proyecto en el que me he aventurado.

Drako y Luca, por ser mis fieles compañeros en las noches de desvelo.

Agradecimientos

Agradezco a mi alma máter, la Benemérita Universidad Autónoma de Puebla, por haberme abierto las puertas para formarme en ella y por todas las oportunidades y apoyos que me ha brindado en mi educación, que me han permitido desarrollarme y crecer de manera académica, profesional y personal.

Agradezco enormemente a la Dra. María Patricia Moreno Rosano por ser una gran mentora antes y durante el proceso de investigación de esta tesis. Sus conocimientos y consejos los mantendré siempre presentes. Agradezco su compromiso con este proyecto y su apoyo en mi desarrollo académico y profesional, puesto que, sin él, no habría podido perseguir ciertas metas y sueños.

Les doy las gracias a la Mtra. Marcela Álvarez Pérez y al Mtro. Eduardo Talavera Sardaneta, quienes no sólo dejaron un impacto muy positivo en mí por los conocimientos compartidos durante sus clases, sino que sus comentarios y observaciones han sido importantes para el desarrollo de este trabajo de investigación.

A cada uno de los docentes de Licenciatura en Relaciones Internacionales de quienes tuve la oportunidad de aprender mucho de la disciplina, y en particular a aquellos profesores que tuvieron un gran impacto en mi desarrollo: Víctor Manuel Elías Miranda, Rafael Priesca Mastretta, Cristina Cruz Carvajal, Guillermo Alberto Rodríguez Ortiz, Myrna Rodríguez Añuez, Marisol Pérez Díaz y Jazmín García Gómez.

A la Ludwig-Maximilians-Universität de Múnich, que me acogió durante un periodo de intercambio, en el que descubrí nuevas perspectivas de la disciplina. Al Dr. Moritz Weiss, cuyas clases despertaron en mí el interés y pasión por la ciberseguridad y su relación a las Relaciones Internacionales.

Muchas gracias.

ÍNDICE

ÍNDICE DE TABLAS

RESUMEN

El ciberespacio se ha consolidado como un elemento indispensable en la vida actual, convirtiéndose en una infraestructura esencial de la sociedad. Las Tecnologías de la Información les ha permitido a los actores internacionales explorar nuevas maneras de conseguir sus objetivos y también, ha modificado la manera en la que interactúan entre ellos. Bajo este contexto es que ocurre NotPetya, un ciberataque de tipo ransomware dirigido a Ucrania en 2017 que no sólo neutralizó por completo al Estado, sino que cruzó múltiples fronteras, afectando a miles de víctimas alrededor del mundo. Este trabajo busca mostrar como el ciberespacio ha permitido a los actores internacionales tener nuevas expresiones de poder y como el caso de NotPetya puede ser utilizado para observarlas.

Palabras clave

Poder, Ciberpoder, Ciberseguridad, Ciberespacio, Ciberguerra, NotPetya, Ransomware, Influencia, Ucrania, Rusia.

ABSTRACT

Cyberspace has become a necessary component of today's life, becoming an essential infrastructure for society. Information technology has enabled international actors to explore new ways to achieve their goals and has also changed the way in which they interact with each other. It is in this context that NotPetya took place in 2017, a ransomware-like cyberattack on Ukraine, which not only completely neutralized the state, but also crossed many borders, affecting thousands of victims worldwide. This paper seeks to show how cyberspace has allowed international actors to have new expressions of power and how the case of NotPetya can be used to observe them.

Keywords

Power, Cyberpower, Cybersecurity, Cyberspace, Cyberwar, NotPetya, Ransomware, Influence, Ukraine, Russia.

Siglas y abreviaturas.

ASEAN: *Association of Southeast Asian Nations.* Asociación de Naciones de Asia Sudoriental.

ARPANET: *Advanced Research Projects Agency Network*. Red de la Agencia de Proyectos de Investigación Avanzada.

APT: *Advanced Persistent Threat*. Amenaza Persistente Avanzada.

CERT: *Computer Emergency Response Team***.** Equipo de Respuesta ante Emergencias Informáticas.

COI: Comité Olímpico Internacional.

DoS: *Denial of Service.* Denegación de Servicio.

DDoS: *Distributed Denial of Service.* Denegación Distribuida de Servicio.

MIT: *Massachusetts Institute of Technology*. Instituto Tecnológico de Massachussets.

MFT: *Master File Table.* Tabla Maestra de Archivos.

MBR: *Master Boot Record.* Registro de Arranque Principal.

NHS: *National Health Service*. Servicio Nacional de Salud del Reino Unido.

NASA: *National Aeronautics and Space Administration***.** Administración Nacional de Aeronáutica y el Espacio.

NSA: *National Security Agency*. Agencia de Seguridad Nacional de los Estados Unidos.

Ping: *Packet Internet Groper*. Buscador de Paquetes de Internet.

RAT: *Remote Access Tool.* Herramienta de Acceso Remoto.

SHAC: *Stop Huntingdon Animal Cruelty***.** Alto a la Crueldad Animal de Huntingdon.

SMB: *Server Message Block*. Bloque de Mensajes del Servidor.

SO: Sistema Operativo.

TI: Tecnologías de la Información.

TIC: Tecnologías de la Información y la Comunicación.

TSB: The Shadow Brokers.

VBS: Visual Basic Script.

Glosario.

Adware: Es la abreviación en inglés de "*advertising software*" y es un programa diseñado para recopilar la información del usuario de una computadora para bombardearlo de anuncios dirigidos de acuerdo con su perfil.

Amenaza Persistente Avanzada: Campaña de ciberataques dirigidos a objetivos específicos, conducida y dirigía por un equipo coordinado de expertos especializados, combinando organización, inteligencia, complejidad y paciencia.

Backdoor: Interpretado al español como "puerta trasera", se refiere a los métodos utilizados por usuarios no autorizados para obtener acceso a un sistema determinado, ya sea una computadora, una red o un programa específico.

Biometría: Medidas biológicas, o características físicas, que se pueden utilizar para identificar a las personas, por ejemplo, la clasificación de huellas dactilares, el reconocimiento facial y los exámenes de retina.

Black Hat Hacker: Ver Hacker de Sombrero Negro.

Buscador de Emociones: Son personas que pretenden atacar sistemas computacionales, simplemente para probarse a sí mismos, aprender o experimentar. No están interesados en dañar los sistemas o crear consecuencias negativas significativas en las redes a las que se introducen, pero pueden provocar problemas sin darse cuenta o querer hacerlo.

Caballo de Troya: Es un *software* que afirma realizar una actividad específica, pero que, en realidad, está realizando otras actividades sin que el usuario lo sepa. Cuando infectan un equipo pueden provocar daños similares a los virus y gusanos, pero a diferencia de ellos, los troyanos no buscan propagarse, por lo que se mantienen en la misma computadora. Están diseñados para que los usuarios los descarguen por voluntad propia, ya que aparentan ser un programa legítimo, pero

poseen múltiples características ocultas que se activan una vez que el programa logra instalarse en el equipo.

Carga Útil: Se refiere a la capacidad de transporte de un paquete u otra unidad de datos de transmisión. En el caso de ciberseguridad y de programas maliciosos, se refiere al código malicioso que causa daño a la víctima objetivo.

Ciberamenaza: Actividad destinada a comprometer la seguridad de un sistema informático, alterando la disponibilidad, integridad o confidencialidad de un sistema o la información que contiene.

Cibercrimen: Actividad ilícita realizada con apoyo de herramientas del ciberespacio.

Cibercriminal: Persona que realiza actividades ilícitas utilizando herramientas del ciberespacio.

Ciberguerra: Conflicto entre dos Estados en el que el triunfo o derrota depende directamente del uso de medios digitales o infraestructura del ciberespacio para realizar actividades clave, como el ataque y la defensa, en el transcurso de todos los enfrentamientos.

Ciberespacio: Dominio operacional enmarcado por el uso de electrónicos para aprovecharse de la información a través de los sistemas interconectados y la infraestructura asociada.

Cibernauta: Individuo que navega por el ciberespacio.

Ciberterrorismo: Término que surge tras la unión de dos de las problemáticas modernas más comunes: Los ataques a través del uso de tecnología y los ataques "terroristas" tradicionales. Se ha convertido en una etiqueta utilizada subjetivamente por los gobiernos y organizaciones. Los grupos señalados como "terroristas" en un conflicto, son considerados como “héroes” o “luchadores por la libertad” por sus partidarios, por lo que es complejo determinar si una organización es "terrorista". Se considera generalmente en este término a acciones que inciten

terror a la población a través del uso de computadoras para impulsar su ideología y utilizando el miedo para impulsar objetivos políticos

Componente: En términos generales, un componente es un elemento de un grupo más grande. Por lo tanto, las partes más grandes de una computadora, como la CPU y el disco duro, también pueden denominarse componentes de la computadora. Sin embargo, técnicamente, los componentes son las partes más pequeñas que componen estos dispositivos. Las computadoras se componen de muchas partes diferentes, como una tarjeta madre, CPU, RAM y disco duro. Cada una de estas partes está compuesta de partes más pequeñas, llamadas componentes.

Componentes Ciberpersonales: Hacen referencia a los perfiles en redes sociales y en otros tipos de servicios, en los que se introducen información personal, incluyendo biometría, para crear cuentas únicas e individuales asociadas la persona real.

Computadora Virtual: Ver Máquina Virtual.

Cortafuegos: Sistema diseñado para para prohibir o permitir el acceso desde o hacia una red. Un firewall puede ser físico o digital (virtual), es decir, puede estar en un dispositivo dedicado o trabajar cómo cortafuegos o como un programa software.

Darknet: Ver Dark Web.

Dark Web: Traducido como "Red Oscura". Muchas veces confundida con la *Deep Web*, aunque forma parte de ella, la *Dark Web* es ese fragmento de Internet al que sólo se puede acceder mediante aplicaciones específicas. Porción de Internet que está intencionalmente oculta a los motores de búsqueda, usa direcciones IP enmascaradas y es accesible sólo con un navegador web especial

Datos Biométricos: Ver "Biometría".

Deep Web: También conocida como *Invisible Web* (Red Invisible) o *Hidden Web* (Red Oculta), la *Deep Web* (Red Profunda), engloba toda esa información que está en línea, pero a la

que no puedes acceder de forma pública. Por una parte, pueden tratarse de páginas convencionales que han sido protegidas por un *paywall*, pero también archivos guardados en Dropbox o correos electrónicos guardados en los servidores de nuestro proveedor. El ~90% del contenido de la red no es accesible a través de motores de búsqueda estándar y conforman a la *Deep Web*.

Equipo: Dispositivo electrónico que almacena y procesa información para después mostrarla en una interfaz a la disposición del usuario, permite una interacción del hardware (parte tangible) con el software (parte intangible). Suelen ser parte de estos equipos, el conjunto de elementos conocidos como periféricos: Teclado, ratón, monitor, adaptadores de video, etc.

Exploit: Es una palabra derivada del inglés "*exploitation*" que significa explotar o aprovechar. Hace referencia a herramientas informáticas o *software* que es utilizado para aprovecharse de vulnerabilidades de seguridad de un equipo, programa o sistema determinado

Firewall: Ver “Cortafuegos”

Gusano: Programa malicioso que rea copias de sí mismo y las esparce a otras computadoras dentro de una red para tener un alcance mayor. Las copias poseen las mismas funciones que el archivo original, y mantienen comunicación con él, también son capaces de ejecutar las mismas funciones, aumentando sus capacidades de expansión.

Hacker: Término utilizado originalmente para referirse a los expertos con conocimientos técnicos en informática que realizaban lo que deseaban a través del ciberespacio, incluso cuando implicara quebrar las reglas. En la actualidad, el término ha evolucionado para referirse a todos los individuos que detectan vulnerabilidades en sistemas, programas, o redes computacionales para aprovecharse de ellas, no necesariamente con intenciones maliciosas.

Hacker de Sombrero Blanco: Un hacker de sombrero blanco, o hacker ético, es una persona que utiliza sus conocimientos de hackeo para identificar las vulnerabilidades de seguridad en el hardware, el software o las redes de alguna organización o persona específica. A diferencia

de los hackers de sombrero negro, los hackers de sombrero blanco revelan completamente todas las vulnerabilidades que encuentran a la empresa o al propietario del producto que es responsable de arreglar los defectos para que los problemas puedan ser resueltos antes de que sean explotados por hackers maliciosos.

Hacker de Sombrero Negro: Un tipo hacker que irrumpe en las redes informáticas con intenciones maliciosas. También pueden liberar programas maliciosos que destruyen archivos, mantienen los ordenadores como rehenes o roban contraseñas, números de tarjetas de crédito y otros datos personales.

Hacktivismo: Término creado a partir de la combinación de las palabras "activismo" y "hackear". El término se desprende de la palabra "*hacktivism*" en inglés que posee el mismo sentido. Consiste en el uso de la computación en forma de protesta o ataque, principalmente con el objetivo de incitar a la desobediencia civil con respecto a temas sociales.

Hacktivista: Unión de las palabras "hacker" y "activista". Son personas que buscan impulsar causas específicas o ideologías, a través acciones que van en contra de las reglas de seguridad computacional y que les permitan obtener mayor exposición.

Hardware: Aquellos elementos físicos o materiales que constituyen una computadora o un sistema informático. Es decir, son aquellas partes físicas de un sistema operativo tales como sus componentes eléctricos, electrónicos, electromecánicos, mecánicos y cualquier elemento físico que esté involucrado.

Industria 4.0: Es considerado como un nombre alternativo a la actual revolución industrial, que está caracterizada por la inclusión de nuevas tecnologías como la robótica, la analítica, la inteligencia artificial, las tecnologías cognitivas, la nanotecnología y el *Internet of Things* (IoT), entre otros, a los procesos de producción.

Killswitch: Término utilizado comúnmente como “interruptor de emergencia”. Se refiere a acciones o elementos que pueden interrumpir súbitamente el funcionamiento de un programa informático.

Malware: Término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

Malware Modular: Programa malicioso con la capacidad de atacar a su objetivo en diferentes etapas, de una manera más sutil y de forma gradual.

Máquina Virtual: Programa computacional que emula el funcionamiento de una computadora física. Se podría describir como “tener una computadora, dentro de una computadora”. Debido a que usualmente se encuentran aisladas del sistema, son utilizadas comúnmente por los trabajadores de la seguridad informática para poner a prueba programas maliciosos sin infectar una computadora real.

P5+1: Grupo conformado por los cinco miembros permanentes del Consejo de Seguridad de la Organización de Naciones Unidas, Estados Unidos, China, Rusia, Reino Unido y Francia, además de Alemania.

Parche de Actualización: Actualización para una pieza de software o programa para corregir un bug o una vulnerabilidad, y para mejorarlo. El concepto es el mismo que el de cubrir un agujero en un neumático, pero aplicado al mundo digital.

Payload: Efectos que un virus, troyano o gusano está diseñado a ocasionar en una computadora en específico.

Phishing: Es un término conformado por un juego de palabras en inglés, en el que intencionalmente se deletrea erróneamente la palabra "*fishing*", que en español es pescar. Es un tipo de cibercrimen cuyo propósito es el robo de información confidencial de una computadora a través de técnicas de ingeniería social, por ejemplo, la suplantación de identidad.

Ping: Es la abreviación de *Packet Internet Groper*, que en español puede ser interpretado como "Buscador de Paquetes de Internet". Es un tipo de programa que le permite a los usuarios comprobar la existencia de una dirección IP específica. Es una herramienta utilizada comúnmente para el diagnóstico de conexiones de una computadora.

Protocolo: Conjunto de reglas y de procedimientos específicos que deben ser seguidos para transmitir información entre dispositivos y para que ésta puede ser leída entre ellos.

Protocolo de Comunicación: Ver "Protocolo".

Protocolo de Red: Ver "Protocolo".

Ransomware: Tipo de programa malicioso, a través del cual, un atacante restringe a un usuario el acceso a sus archivos, o incluso a su equipo, usando una variedad de métodos, como, por ejemplo, la encriptación. Posteriormente, solicita un pago a cambio del desbloqueo de los archivos. Una analogía que podría utilizarse, es que el atacante "secuestra" la información del usuario y exige un "rescate" a cambio de ella.

Red Privada Virtual (RPV): Es un software que oculta la dirección IP de un ordenador dejando que la red la redirija a través de un servidor remoto especialmente configurado y gestionado por un host VPN. El servidor VPN se convierte en la fuente de los datos y terceros, como el proveedor de servicios de Internet, no pueden ver qué sitios web se visitan o qué datos se envían y reciben en línea.

Script: Es un archivo que posee una lista de comandos o una serie de acciones que deben ser ejecutados por un programa específico.

Servidor: Un servidor es un programa o dispositivo informático que proporciona un servicio a otro programa informático y a su usuario, también conocido como cliente. En un centro de datos, el ordenador físico en el que se ejecuta un programa de servidor también suele

denominarse servidor. Esa máquina puede ser un servidor dedicado o puede utilizarse para otros fines.

Servidor Remoto: Los servidores remotos le permiten al usuario acceder a los datos e información que son compartidos en una red específica.

Sistema Operativo: Conjunto de programas que permiten manejar la memoria, disco, medios de almacenamiento de información y los diferentes periféricos o recursos de una computadora. Dicho de otra manera, es el programa más importante, puesto que es quien controla todas las aplicaciones dentro de un dispositivo electrónico.

Software: Es la parte no física que hace referencia a un programa o conjunto de programas de cómputo que incluye datos, reglas e instrucciones para poder comunicarse con el ordenador y que hacen posible su funcionamiento.

Software Privativo: Es un tipo de programa el cuál posee restricciones de uso, modificación y copia establecidos por sus creadores. El programa está compuesto de código cerrado para evitar la descompilación o cambios en el código.

Spyware: Es un programa malicioso diseñado para realizar un seguimiento de las acciones realizadas por el usuario en un equipo infectado. Su origen proviene de las palabras en inglés "*spying software"* y existe una gran variedad de programas que recopilan diferente información, como el registro de pulsaciones de teclas, el acceso a micrófono y cámara web, el monitoreo de los hábitos de navegación y la captura de usuarios y contraseñas de diversos sitios

Troyano: Ver "Caballo de Troya".

Virus: Tipo de programa que ocasiona efectos secundarios en los equipos a los que infecta y modifica los programas del sistema operativo en el que residen, para causar daños a la computadora. Los virus no son necesariamente maliciosos, pero los efectos secundarios que

ocasionan pueden ser indeseados, puesto que éstos ocurren comúnmente sin el conocimiento de la víctima.

Vulnerabilidad: Debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas y pueden ser explotadas o utilizadas por intrusos o atacantes.

White Hat Hacker: Ver Hacker de Sombrero Blanco.

Wiper: Un tipo de programa malicioso cuyo objetivo es borrar, total o parcialmente, los datos del disco duro de la computadora a la que infecta.

Introducción

En cuestión de décadas, el ciberespacio se ha consolidado como uno de los elementos fundamentales en el desarrollo de la gran mayoría de actividades de la vida diaria, sobre todo aquellas esenciales para el funcionamiento de la sociedad. La llegada del internet trajo consigo alternativas de comunicación, nuevas maneras de comerciar y grandes beneficios, al acelerar y facilitar una diversidad de procesos, que pueden ir desde encontrar un restaurante en una zona determinada de una ciudad, hasta la distribución de agua potable o la gestión de las redes de electricidad de un país entero. El acelerado proceso industrial del Siglo XXI y las nuevas tecnologías que han surgido en los últimos años gracias a él, han brindado una gran variedad de opciones para facilitar el acceso a este recurso, por lo que sus usuarios aumentan significativamente cada año. Sin embargo, a pesar de que el uso de los recursos del ciberespacio es un fenómeno muy común en la actualidad, se requieren de más estudios dentro de la disciplina de las Relaciones Internacionales para poder explicar claramente el actuar de los múltiples actores internacionales dentro de este nuevo campo.

El ciberespacio fue ocupado rápidamente por todo tipo de actores que influencian directamente el panorama internacional, como individuos particulares, que han destacado gracias al uso de nuevas herramientas tecnológicas; grandes empresas transnacionales, que han incursionado en el comercio digital y han generado importantes ganancias económicas; los Estados y sus dependencias gubernamentales, que deben adaptarse a un nuevo dominio para alcanzar sus intereses; grupos de activismo y asociaciones, que buscan difundir mensajes a través del Internet; o incluso el crimen organizado y grupos extremistas, que han encontrado una manera de realizar sus actividades reduciendo el riesgo de ser detenidos.

Personalidades como Jeff Bezos, Bill Gates, Mark Zuckerberg, y Elon Musk se colocaron en importantes posiciones que les brindan capacidades de influir en asuntos internaciones, al acumular riquezas que sobrepasan los miles de millones de dólares provenientes de grandes empresas de tecnología cuyos productos utilizan el ciberespacio y son distribuidos en todo el mundo. Empresas como Amazon, Microsoft, Facebook, Tesla, SpaceX, Google, Twitter y Apple dominan el mercado internacional e influyen directa, o indirectamente, en la toma de decisiones políticas alrededor del planeta (Stiglitz 2019).

Países como Reino Unido, Estados Unidos y Francia son líderes mundiales en aspectos de ciberseguridad, al poseer capacidades destacadas en el ciberespacio y tener medidas legales, técnicas, organizacionales y de cooperación sólidas (International Telecommunication Union 2019). Grupos activistas han recurrido al ciberespacio, e incluso a medidas como el hackeo, para transmitir su mensaje de una manera más efectiva[1], como Anonymous o Stop Huntingdon Animal Cruelty (SHAC), los cuales organizaron sus campañas de protesta a través de las redes, logrando una mayor difusión a su mensaje (Singer y Friedman 2014).

Y, así como los Estados y las agencias gubernamentales, también los grupos criminales y extremistas han aprovechado las nuevas tecnologías para alcanzar sus objetivos, haciendo uso principalmente de redes sociales para buscar y reclutar nuevos elementos, difundir sus ideologías o planear ataques a distancia, facilitando sus actividades y reduciendo su riesgo (Albahar 2019).

Podemos observar un fenómeno importante del Sistema Internacional actual: Que los actores internacionales han desarrollado nuevas capacidades debido al surgimiento del

[1] Singer y Friedman (2014) expresan que a la combinación de "activismo" y "hackear" se le denomina hacktivismo, o *hacktivism* en inglés, y consiste en el uso de la computación en forma de protesta o ataque, principalmente con el objetivo de incitar a la desobediencia civil con respecto a temas sociales.

ciberespacio y que, gracias a éstas, han encontrado nuevas maneras de interactuar entre ellos, teniendo un impacto en el esquema internacional contemporáneo.

A través de estos ejemplos se puede denotar que en la actualidad existen actores internacionales que en el pasado no tenían las capacidades suficientes para participar en el Sistema Internacional, pero que ahora, a través del ciberespacio, pueden compartir el "escenario" y competir mano a mano con las grandes potencias internacionales. A este fenómeno se le conoce como la "difusión" de poder, un concepto clave que debe ser entendido para poder comprender a profundidad la realidad de las relaciones internacionales actuales.

La difusión de poder es el fenómeno en el que los Estados se mantienen como el actor dominante, pero se les dificulta controlar e influir a los demás actores del Sistema Internacional. En la actualidad, la difusión de poder está siendo provocada por la "Revolución Informática[2]" y el avance de la tecnología que le ha permitido a una mayor parte de la población tener acceso a la información, y al poder que ésta conlleva, provocando que se utilice para diversos fines y que ha llegado a poner en riesgo los intereses de los Estados y de otros actores internacionales (Nye 2011).

Planteamiento del objeto de estudio

En la actualidad, el mundo ha alcanzado un alto nivel de interconexión a través de las Tecnologías de la Información y Comunicación (TIC) que facilitan el contacto entre personas, grupos, organizaciones y gobiernos de distintos países. Esta conexión ha brindado importantes beneficios a los diferentes actores del Sistema Internacional que no hubieran sido posible en décadas anteriores. Los gobiernos han mejorado la comunicación al interior de sus territorios, así como al

[2] Nye (2011) considera a la Revolución Informática como la "Tercera Revolución Industrial" en la que la comunicación se ha acelerado gracias a las nuevas tecnologías, y se han generado importantes ventajas, como la facilidad de compartir información en grandes cantidades, de forma inmediata y con casi ningún intermediario.

exterior, y han estimulado el desarrollo económico y social de su población gracias a estas facilidades. Sin embargo, a pesar de que las TIC han brindado una gran cantidad de ventajas, éstas también han provocado nuevos problemas que no habían existido con anterioridad, los cuales deben ser enfrentados con nuevas estrategias, propias de esta época de la información.

Uno de los temas que siempre ha sido prioritario para la supervivencia del Estado es la ejecución de una apropiada estrategia de Seguridad Nacional, y en el caso del ciberespacio, este no es la excepción. Con el ciberespacio, los gobiernos dependen en gran medida de dispositivos e infraestructura esencial, conectada al internet o redes locales, que son fundamentales para las actividades diarias, y cuya disrupción significaría una pérdida económica significativa, la interrupción de servicios indispensables o incluso poner en riesgo a la población. Esta gran dependencia del ciberespacio ha sido detectada como un punto muy vulnerable para el Estado, debido al riesgo que representa ser víctimas de un ciberataque que provoque consecuencias importantes dentro de su territorio, por lo que los expertos en seguridad se han inclinado a crear nuevas estrategias de seguridad que incluyen al ciberespacio[3] para salvaguardar la supervivencia del Estado.

Fenómenos como la dependencia hacia las TIC, la facilidad de explotar vulnerabilidades de estructuras esenciales, la dificultad de crear una estrategia de ciberdefensa adecuada y lo interconectado que se encuentran las diferentes instituciones del Estado han provocado que los actores del Sistema Internacional comiencen a presentar nuevas expresiones de poder que no se habían presenciado con anterioridad, y que surjan nuevos tipos de amenazas con potencial de dañar severamente países enteros. Tal fue el caso del ciberataque "NotPetya" ocurrido en 2017, en el que Ucrania fue el país más afectado.

[3] Comúnmente denominadas estrategias de ciberseguridad.

NotPetya es un virus informático que fue creado y lanzado para realizar un ataque de tipo *ransomware*, el cual puede ser definido como la situación en la que el "atacante toma el control del equipo infectado y "secuestra" la información del usuario cifrándola, de forma que resulta ilegible si no se dispone de una clave para descifrarla". Usualmente este tipo de ataques se realizan con la intención de obtener grandes cantidades de dinero de las víctimas a cambio del "rescate" de sus documentos, por lo que tienden a ser dirigidos a la mayor cantidad de personas posible (Grupo de Trabajo de Ciberriesgos de AGERS - ISMS FORUM 2017, 16; Fayi 2018).

Sin embargo, el ciberataque NotPetya no fue un *ransomware* común debido a la complejidad de su código y los severos efectos que ocasionó en Ucrania y el mundo entero. El 27 de junio de 2017, NotPetya fue difundido a través de las computadoras de Linkos Group, una pequeña empresa de tecnología ubicada al este de Kiev que se encontraba a cargo de publicar actualizaciones periódicas del software M. E. Doc, un programa de contaduría requerido por el gobierno ucraniano para realizar negocios y declarar impuestos, por lo que todas las empresas que hicieran negocios en o con Ucrania, debían utilizar este programa. De esta forma, los creadores de NotPetya lograron infectar a miles de computadoras de diversas empresas nacionales e internacionales, así como de instituciones de gobierno creando efectos económicos, políticos y sociales muy importantes (Greenberg 2019).

En cuestión de segundos, NotPetya fue capaz de infectar redes enteras y a empresas alrededor del mundo, que reportaron eventos similares a lo ocurrido en Ucrania: En las pantallas de sus computadoras aparecía un mensaje que expresaba que sus archivos ya no eran accesibles y que se encontraban encriptados, por lo que el equipo era inutilizable hasta que se pagara el equivalente a $300 dólares en Bitcoin como rescate. Si bien el ataque comenzó en Ucrania y una gran parte de su infraestructura se vio duramente afectada, NotPetya logró propagarse a 64 países

más llegando a múltiples empresas alrededor del mundo y convirtiendo a Estados Unidos en el segundo país con más casos, desencadenado toda clase de efectos (Fayi 2018).

El caso de lo ocurrido en Ucrania con NotPetya es la prueba de que un ciberataque puede ocasionar efectos importantes y que las consecuencias que se generan de él pueden presenciarse no sólo en el dominio del ciberespacio, sino que también pueden impactar el mundo físico que nos rodea. Los ciberataques de esta magnitud pueden poner en riesgo la infraestructura esencial de una sociedad y pueden imposibilitar el acceso a recursos básicos al interrumpir hospitales, bancos, escuelas, universidades, departamentos del gobierno o incluso simplemente al dejar inutilizables los medios de comunicación existentes en un territorio determinado (Lika et al. 2018).

La gran variedad de actores, y la difusión del poder que ha facilitado su participación en el Sistema Internacional ha originado nuevas interacciones que no habían sido contempladas en las teorías clásicas de las Relaciones Internacionales, puesto que la llegada del ciberespacio también implicó el surgimiento de situaciones que no podían haberse considerado anteriormente. De esta manera, actores no tradicionales han podido perseguir sus intereses haciendo uso de sus nuevas capacidades, y al mismo tiempo, han generado nuevas maneras de ejercer su poder.

Delimitación

Ya que el tema central de esta investigación es examinar expresiones de poder a través del ciberespacio, específicamente en el caso del ciberataque NotPetya en 2017 a Ucrania y los efectos que tuvo en sus objetivos, se priorizó estudiar los sucesos que ocurrieron dentro del territorio ucraniano en las fechas cercanas al incidente. Sin embargo, como se explicará a lo largo del trabajo, debido a la estrecha interconexión del mundo existente hoy en día, los efectos producidos por el programa malicioso cruzaron múltiples fronteras y afectaron a todo tipo de actores, por lo que fue imposible determinar un área geográfica exclusiva para el estudio del tema. Por esta razón, si bien

se buscó centrarse en los sucesos en Ucrania, el enfoque se expandió a los actores internacionales que se vieron afectados por NotPetya fuera del país, tomando en cuenta que los efectos sufridos por ellos fueran relevantes para el tema.

De igual manera, debido a la acelerada evolución tecnológica y la rápida transformación del panorama de la ciberseguridad, se tomó en cuenta el periodo 2015-2017 como el principal enfoque de esta investigación, siendo éstos los años en los que ocurrieron la gran mayoría de eventos relacionados a NotPetya. Sin embargo, se tomaron en cuenta algunos eventos sucedidos hasta el año 2021, que eran relevantes para mostrar la manera en que los casos legales relacionados al tema han evolucionado. No se tomaron en cuenta los eventos posteriores a 2021, por lo que el estallido del conflicto bélico entre Rusia y Ucrania a principios del 2022 se encuentra fuera de los alcances.

Con respecto a los actores internacionales estudiados, por la manera en que el ciberespacio se desarrolla, la investigación no se centró exclusivamente en actores estatales, puesto que la participación de los actores no estatales era esencial para examinar la manera en que el poder ha evolucionado con la llegada del ciberespacio. Sin embargo, se debe resaltar que la mayoría de actores no estatales estudiados son empresas transnacionales, grupos y organizaciones.

Dentro de las limitaciones encontradas en esta investigación, se debe mencionar que, debido a la complejidad del ciberespacio y a la facilidad existente para ocultar el origen de un ciberataque, el identificar con total certeza al creador de NotPetya es imposible. Sin embargo, se tomaron en cuenta diversos factores para compartir al más probable autor del ciberataque.

Una última consideración que debe ser mencionada es la diversidad de fuentes. Si bien, el caso de NotPetya es conocido y ha sido divulgado por diversas fuentes de información a través de los años, la obra del escritor Andy Greenberg es una referencia citada comúnmente por ellas. Este autor viajó a Ucrania y Rusia para entrevistar gente relevante al caso y realizar investigación de

primera mano, componiendo un libro relatando todos sus descubrimientos sobre NotPetya y *Sandworm*. A lo largo de este proyecto de investigación, se buscó obtener una diversidad de fuentes para lograr una visión objetiva del caso, sin embargo, en muchas ocasiones la obra de Greenberg fue elegida como una fuente principal debido a lo completa y detallada que es la información compartida en su libro. A pesar de esto, siempre se buscaron fuentes adicionales para complementar o verificar la información del autor, asegurándonos de siempre utilizar datos certeros.

Justificación

El estudio de la Ciberseguridad en las Relaciones Internacionales no es tan común en la actualidad, y el fenómeno resulta muy novedoso para las teorías clásicas de la disciplina que deben de ser adaptadas al continuo avance tecnológico, a la rapidez en que pueden suceder los eventos, y al hecho de que un ciberataque puede provenir de cualquier lado y atacar a cualquier objetivo. Sin embargo, se cree que una investigación de este tipo puede ser de gran importancia y que puede generar conocimiento importante para estudios futuros, por lo que a continuación se expondrán algunas razones que justifican la realización de este proyecto.

El ciberespacio es hoy en día crucial para toda actividad humana, ya que la gran mayoría de necesidades básicas de los países dependen de él, es por esto que cualquier actividad que ponga en riesgo este espacio, puede tener un grave impacto en la sociedad local, nacional e internacional. En este sentido, los Estados hoy en día diseñan estrategias para asegurar su supervivencia y poderse defender ante cualquier ataque. Los enfrentamientos modernos han evolucionado y el ciberespacio se suma como el Quinto Dominio de Guerra, agregándose a los cuatro existentes (Tierra, Mar, Aire y Espacio) y transformando la manera en que los conflictos ocurren. De esta forma podemos observar nuevas expresiones de poder que no habían sido contempladas con anterioridad y que

deben de ser estudiadas para comprender la compleja interacción que ocurre entre los diferentes actores del Sistema Internacional actual.

Otro hecho que debe ser considerado es que, a través del ciberespacio cualquier actor puede participar e intervenir en eventos de gran magnitud, creando una difusión de poder importante en el Sistema Internacional que se ve reflejado en las capacidades desarrolladas por Estados que son suficientes para enfrentarse a las grandes potencias. Este importante cambio debe ser estudiado, puesto que ilustra el nuevo comportamiento que tienen las grandes potencias hacia otros actores, incluso aquellos que no son Estados o no pertenecen a él, como empresas, ONG, grupos extremistas e incluso personas en particular.

Asimismo, se considera que este proyecto puede ayudar a difundir la gran importancia que tiene la ciberseguridad y a contribuir con conocimiento a la investigación mexicana en idioma español de la disciplina de las Relaciones Internacionales. Esto genera un gran valor teórico importante al proponer nuevos enfoques utilizando teorías ya conocidas o incluso buscando nuevas teorías que ayuden a comprender el fenómeno estudiado.

Esta investigación surge tras experiencias personales en el extranjero, particularmente en Alemania, en dónde se dio un acercamiento a las perspectivas teóricas sobre la ciberseguridad y su gran importancia con las Relaciones Internacionales. Al profundizar en el tema, se ha notado una carencia de trabajos de investigación desde una interpretación latinoamericana, siendo las visiones europea y estadunidense las que dominan el campo teórico sobre lo que sucede en el mundo. Al ser un fenómeno global cotidiano, este trabajo de investigación busca contribuir a la generación de conocimiento de un tema aún en fase exploratoria, enriqueciendo no sólo a la academia mexicana, sino a la licenciatura en Relaciones Internacionales de esta universidad y de manera personal.

Preguntas de investigación

Pregunta principal

¿De qué manera las acciones dirigidas a Ucrania a través del ciberataque NotPetya en 2017 y los efectos que tuvo en sus objetivos pueden ser consideradas como nuevas expresiones de poder en el Sistema Internacional?

Preguntas secundarias

1. ¿Por qué las acciones realizadas a través del ciberespacio pueden tener un impacto importante en el Sistema Internacional, particularmente los ciberataques?
2. ¿Cómo se llevó a cabo el ciberataque NotPetya en 2017?
3. ¿Cuáles fueron las principales consecuencias de NotPetya en los objetivos a los que impactó?

Objetivos

Objetivo general

Examinar expresiones de poder que pueden ser observadas en las acciones realizadas a través del ciberespacio, específicamente en el caso del ciberataque NotPetya en 2017 a Ucrania y los efectos que tuvo en sus objetivos.

Objetivos particulares

1. Explicar los efectos que las acciones realizadas a través del ciberespacio pueden tener en las Relaciones Internacionales, específicamente los efectos provocados por ciberataques, y cómo éstos pueden configurar la forma de actuar de los diferentes actores internacionales.

2. Describir el proceso llevado a cabo por los autores del ciberataque para crear y liberar a NotPetya.

3. Destacar los efectos producidos por NotPetya en los objetivos a los que infectó, así como sus alcances.

Hipótesis

Las acciones dirigidas a Ucrania a través del ciberataque NotPetya en 2017 pueden ser consideradas como nuevas expresiones de poder en el Sistema Internacional debido a que los autores del ciberataque lograron desarrollar suficientes capacidades en el ciberespacio para aprovecharse de vulnerabilidades que no habían sido detectadas, produciendo consecuencias importantes en los objetivos que atacó y afectando al país económica, política y socialmente, por lo que fue una seria amenaza para su seguridad nacional e influyó directamente en la forma de actuar de Ucrania.

Metodología

Para efectuar este estudio, se realizó una investigación documental con una revisión de la literatura existente con respecto al tema, y debido a lo novedoso que resulta la adición del ciberespacio para describir la realidad en la disciplina de las Relaciones Internacionales, se propuso un estudio de orden exploratorio. Asimismo, se planteó el uso de un enfoque deductivo, estudiando ampliamente el caso de NotPetya, para posteriormente generar posturas teóricas llevando un proceso de lo general a lo particular, observando en primer lugar lo que sucede dentro del campo del ciberespacio a nivel general para después concentrar el estudio en este caso en específico.

El primer capítulo se ha denominado “La importancia de la ciberseguridad en el Sistema Internacional actual” y explica de forma general el funcionamiento del ciberespacio y su relación

con el Sistema Internacional, el alcance que los diferentes actores internacionales ahora tienen gracias a sus nuevas capacidades y las diferentes herramientas con las que cuentan para alcanzar sus objetivos.

Dentro de este mismo capítulo se exponen dos teorías de las Relaciones Internacionales, cuyas ideas ayudan a explicar el fenómeno en cuestión: El neorrealismo y el constructivismo. Del neorrealismo se considera la lucha por la información para obtener poder, la modificación de conductas de otros actores para perseguir intereses propios y el estado de anarquía del Sistema Internacional y del internet. Mientras que del Constructivismo destacan las ideas relacionadas con las identidades de los actores internacionales definidas por la estructura global, la capacidad que tienen ciertos actores de modificar las conductas de otros por el papel que adoptan y, de la misma manera, el estado anárquico del Sistema Internacional. Se conjuntaron estas dos teorías puesto que se complementan adecuadamente, particularmente en la manera en que observan al ciberespacio: Como una herramienta utilizada por los actores internacionales dominantes para ejercer su poder y mantener su papel dentro del Sistema Internacional actual.

En el segundo capítulo titulado "La creación de NotPetya y su difusión en Ucrania y el mundo" se realizará, en primer lugar, un recorrido histórico de los incidentes cibernéticos más relevantes para la disciplina, para posteriormente mostrar los antecedentes del programa malicioso, tomando como referencia los ciberataques predecesores, cuyos funcionamientos fueron utilizados como base para el diseño de NotPetya. Posteriormente se abordará el proceso que los autores siguieron para la construcción del virus y el método que utilizaron para difundir el malware en Ucrania y el mundo, tomando en cuenta los aspectos técnicos, la infiltración en Linkos Group y la rápida propagación del virus a otros objetivos localizados en diferentes partes del mundo.

El tercer capítulo, llamado "Las consecuencias provocadas por NotPetya y sus efectos en Ucrania y el mundo", se compone de tres partes en las que se profundiza en los efectos provocados

por el malware, incluyendo aquellos involuntarios o inesperados, comenzando por las consecuencias políticas, económicas y sociales producidas en Ucrania; continuando con el impacto que el virus tuvo en el panorama internacional, haciendo un énfasis en las posturas gubernamentales de los países afectados y de las grandes empresas transnacionales que sufrieron pérdidas importantes; y finalizando con la explicación de las propuestas existentes sobre el autor de NotPetya, así como las motivaciones detrás de su creación y el estado del caso en la actualidad. Este proyecto de investigación terminará con la exposición de las conclusiones obtenidas y se verificará si la hipótesis general planteada fue comprobada o refutada para alcanzar el objetivo general.

Capítulo 1. La importancia de la ciberseguridad en el Sistema Internacional actual.

A continuación, se profundizará en las nuevas formas de poder que han sido detectadas en el Sistema Internacional actual, después se expondrá la manera en que el ciberespacio se encuentra siendo utilizado como un nuevo dominio de guerra; posteriormente, se desarrollará brevemente el tema de los virus informáticos, su funcionamiento y se concluirá exponiendo el riesgo que representan para los actores internacionales.

1.1. Nuevas formas de poder

Antes de comenzar a discutir las nuevas maneras en que los actores internacionales ejercen el poder a través del ciberespacio, es pertinente comenzar con una breve discusión sobre el poder y su evolución a ciberpoder, así como sus implicaciones.

A pesar de ser un concepto ampliamente estudiado y esencial en la disciplina de las Relaciones Internacionales, el poder puede ser complicado de definir, y aún más, de medir y comparar, por lo que continuamente se generan debates con respecto a su significado. Para Nye (2011), el poder está directamente relacionado con la influencia que un sujeto tiene sobre otro, y la manera en que la usa para alcanzar sus propios objetivos. Resalta que para que exista el poder, también es necesaria a su vez un objetivo al cual ejercerlo, por lo que debe existir una relación entre dos o más sujetos, ya que la interacción entre ellos es lo que genera esa influencia.

Complementando las ideas de Nye, Foucault indica de una manera similar, que el poder puede ser considerado como la capacidad que tienen los actores de prohibir ciertas acciones a otros, utilizando diferentes mecanismos. El autor considera que, de esta manera, un actor toma la "soberanía" de otro, o, en otras palabras, su capacidad de decidir sobre sí mismo, y establece las acciones que desea sean evitadas. Cuando el actor incumple con la prohibición, es acreedor a un

castigo, implementado por el primer actor a través de diversos mecanismos que le permiten, desde un principio, ser capaz de imponer estos límites. Similar a Nye, el poder para Foucault es ejercido para modificar las conductas y acciones de otros actores (Foucault 1979).

Este tipo de interacción entre actores puede ser de diferentes maneras, y Nye (2005) principalmente considera dos: El *Hard Power*[4], que consiste principalmente en medidas militares y económicas que utilizan los actores internacionales, comúnmente los Estados, para obligar a otros a cambiar su conducta. Algunas medidas que se pueden realizar para lograrlo son otorgando estímulos para que otro actor acceda a realizar una acción a cambio de algo, o a través de amenazas y acciones coercitivas, para obtener el objetivo por la fuerza. Por otro lado, el *Soft Power*[5], consiste en obtener los resultados buscados a través de métodos indirectos. Esto ocurre cuando un actor no necesita obligar a los demás para que realicen una conducta deseada, ya que ellos la realizan por voluntad propia, al admirar los valores del actor ejerciendo el poder, y, por ende, buscando imitarlo para asemejarse a él.

De las definiciones de Nye podemos resaltar dos importantes características del poder, la primera, que es utilizado por los actores para alcanzar sus objetivos, transformando las conductas de los demás; y la segunda, que el poder puede tener diferentes formas, y que no es ejercido exclusivamente a través de medidas coercitivas.

Por otro lado, tenemos la interpretación de Kenneth Waltz, quien consideraba que el Sistema Internacional se encuentra en un estado de anarquía, en el que los actores participan para obtener el poder con el objetivo principal de garantizar su supervivencia. Para el autor, el poder no es el medio, sino el fin de los Estados, puesto que es necesario para asegurar que las condiciones que requieren para sobrevivir sean satisfechas. De esta forma, Waltz determina que se puede medir

[4] "Poder Duro" en inglés
[5] "Poder Suave" en inglés

la capacidad que tiene un Estado de obtener el poder a través del tamaño de su población y territorio, la dotación de recursos con los que cuenta, su capacidad económica, su fortaleza militar, su estabilidad política y su competencia (Waltz 1979).

Si bien Waltz no da una definición concreta del poder como tal, el concepto es una parte fundamental de su teoría, y podemos decir que no solamente es importante tener poder, sino que también es esencial lo que se realiza con él. Para el autor, el poder es fundamental para garantizar la supervivencia del Estado, por lo que los diferentes actores internacionales se mantienen en una lucha continúa para obtenerlo en el Sistema Internacional anárquico. A diferencia de Nye, esta interpretación se enfoca en gran medida en los Estados, y, como veremos posteriormente, en la actualidad existen un gran número de actores internacionales con importantes capacidades para competir en el plano internacional.

Una reflexión adicional en torno al concepto de poder que se debe tomar en cuenta, es la interpretada a través de la obra de Alexander Wendt, en la cual se afirma que los actores internacionales presentan los mismos comportamientos que los individuos tienen dentro de la sociedad, ya que el Sistema Internacional, así como las diferentes instituciones y actores presentes en él, son construcciones sociales que se van adaptando de acuerdo a los cambios que ocurren con el paso del tiempo (Wendt 2009).

Para Wendt (2009), las conductas adoptadas por los diferentes actores internacionales dependen directamente del significado que han conformado con el paso del tiempo de lo que representa el Sistema Internacional para ellos. Esta concepción surge a través de la identidad que han construido y aprendido a lo largo de la historia, a través de la interacción que han tenido con otros Estados o actores internacionales. Esto quiere decir que, si un Estado se identifica con otro, es muy probable que logren objetivos mutuos a través de la cooperación, y, por lo contrario, si un

Estado no se identifica con ninguno, se genera un estado de anarquía en el Sistema Internacional. Wendt resume esta idea con la frase "La anarquía es lo que los Estados hacen de ella" (142).

Si bien, Wendt no se enfoca particularmente en definir el poder, sí comparte su visión de él, y el papel que juega en Sistema Internacional. Para el autor, la estructura internacional en la que conviven los actores internacionales determina las características y propiedades que cada uno de ellos posee, por lo que adoptan ciertos "papeles" o "roles" en ella y conforman una identidad que les indica la manera en que deben ejercer el poder, y hacia cuales actores deben hacerlo.

Tomando en cuenta estas afirmaciones, el poder del Constructivismo de Wendt proviene de la identidad conformada, puesto que un actor puede transformar la conducta de otro, de acuerdo a la relación que mantienen ambos, determinada por sus identidades. Similar a lo que el autor dice sobre la anarquía, también se puede decir que el poder, es lo que los actores internacionales hacen de él. Por ejemplo, la decisión de Estados Unidos de enviar tropas a Vietnam y Corea puede ser comprendida por la identidad adoptada por Estados Unidos como potencia capitalista cuyo deber era evitar la expansión de una ideología contraria, con la cual no se identificaban. Estados Unidos ejerció poder, para intentar transformar la identidad de la URSS y para evitar la transformación de la identidad de Corea y Vietnam.

A través de esta interpretación, podemos observar el poder como una característica intrínseca de los actores internacionales, que adoptan una identidad de superioridad, ya sea militar, institucional, cultural o política, sobre los demás actores, dentro de la estructura del Sistema Internacional. El poder, entonces, es ejercido por aquellos actores que "pueden" hacerlo, y, así como las ideas de los demás autores estudiados, es utilizado también para transformar actitudes de los demás actores.

Con estas ideas, podemos conformar una definición propia de poder, que será utilizada a lo largo de este trabajo. Podemos decir que el concepto de poder se refiere a la capacidad de un actor

internacional de alcanzar sus objetivos y perseguir sus intereses, ya sea a través de recursos y medios físicos, o por la transformación de la conducta de otros actores por medio de diferentes acciones.

Con esta definición se tiene una concepción un poco más clara de lo que es el poder, pero es necesario también describirlo, señalando algunas características que posee con el propósito de mostrar su complejidad. A través de la obra de Michel Foucault, podemos señalar algunas características del poder que, en un principio, parecen contradictorias, pero que, si las analizamos a detalle, lo describen adecuadamente.

Foucault afirma que, el poder puede ser considerado como enigmático, debido a su gran complejidad, que provoca que en ocasiones no se pueda apreciar tan fácilmente quién ejerce el poder y hacia quién se ejerce. Indica también, que es visible e invisible al mismo tiempo, puesto que su ejercicio puede ser observado claramente a través de instituciones creadas para favorecer a un grupo en específico, por ejemplo, con las instituciones de policía a nivel nacional que favorecen al gobierno, o las organizaciones internacionales, cuyas acciones pueden favorecer a ciertos Estados; y al mismo tiempo es invisible, ya que se puede ejercer el poder de una manera casi indetectable, a través de mecanismos que pasan desapercibidos o que están incorporados de tal manera en la estructura, que no son notados como una herramienta para el ejercicio del poder, como el sistema de salud y penitenciario a nivel nacional, o a nivel internacional a través de regulaciones de instituciones como el Fondo Monetario Internacional o la Organización Mundial de la Salud (Foucault 1979).

El autor añade que el poder está presente y oculto, puesto que existen actores que lo ejercen a través de métodos explícitos y que son conscientes de su uso, por ejemplo, con el uso de fuerzas armadas y otros métodos coercitivos para alcanzar sus objetivos, mientras que también hay actores que lo ejercen de una manera desapercibida y nada notoria, como con regulaciones y condiciones

impuestas a otros actores para poder comerciar[6]. Por último, especifica que el poder se encuentra presente en todas partes, puesto que, en todo tipo de relaciones, se ejerce de alguna manera (Foucault 1979).

Después de esta recolección de ideas y la conformación de una definición de poder, podemos discutir ahora la naturaleza del ciberpoder, uno de los temas centrales de este estudio. Y, así como se expuso anteriormente, a continuación, se exponen algunas definiciones de ciberpoder brindadas por diferentes autores, para posteriormente conformar la propia (Foucault 1979).

Para Nye, el ciberpoder es el "poder basado en recursos informáticos", y explica que es la suma del concepto "poder" más el prefijo "ciber", que expresa relación con actividades de computación o con el uso de electrónicos. También afirma que es el poder ejercido a través del ciberespacio, al que considera como un "dominio operacional enmarcado por el uso de electrónicos para aprovecharse de la información a través de los sistemas interconectados y la infraestructura asociada" (Nye 2011, 122).

También afirma que, una característica esencial del ciberespacio es que es un dominio artificial creado por el hombre, y que, al ser un medio creado recientemente en el contexto de la Revolución Informática, cuenta con cambios tecnológicos más acelerados que los demás dominios. Agrega que, debido a la “baja” barrera de acceso al ciberespacio, es fácil para cualquier individuo participar en él y que, por la misma razón, actores no estatales y Estados pequeños o con pocos recursos, pueden competir al mismo nivel que las grandes potencias (Nye 2011).

Nye realiza un énfasis especial en el uso de la información para ejercer el poder, puesto que considera que es el recurso primordial en el ciberespacio y que su control es lo que determina qué actores poseen mayores ventajas sobre de otros. Algunas interpretaciones del poder expresadas por

[6] Ambas características son muy similares a los dos tipos de poder señalados por Nye, el poder duro y el suave.

Foucault, complementan esta idea, quien señalaba que existía un control directo sobre el conocimiento producido por parte de grupos de élite a los que llamaba "*círculos reservados del saber*". Estos grupos dominantes son dueños de la información, y no solo la utilizan y se aprovechan de ella para su propio beneficio, sino también son los que establecen las reglas para que el resto de la población la use (Foucault 1979).

Si bien, Foucault se refiere a los medios de comunicación masivos unidireccionales, tradicionalmente utilizados por el Estado para propagar información, como la televisión, la radio y el periódico, en la actualidad, esta interpretación también puede ser aplicada con los medios de comunicación bidireccionales contemporáneos, como las plataformas digitales o las redes sociales. A pesar de que la tecnología actual permite una comunicación más fluida entre sus usuarios, los proveedores de estos servicios son los que, a través de sus términos y condiciones, pueden determinar la información que es transmitida y la manera en que es distribuida, obteniendo un verdadero control de ella.

Por ejemplo, las compañías de telecomunicación, comúnmente proveedoras de servicio de internet, pueden bloquear el acceso a ciertas páginas web; las redes sociales mantienen reglas y términos que deben ser cumplidos por sus usuarios para utilizar el servicio; e incluso otro tipo de empresas de tecnología, como Google o manufactureros de teléfonos inteligentes, proveen sus servicios a cambio de información privada, incluyendo datos biométricos, que son utilizados para múltiples fines. Como lo expresa Foucault, estos grupos no sólo son dueños de la información, sino también la utilizan y se aprovechan de ella, brindándoles directamente la capacidad de ejercer el poder de una manera muy efectiva.

Betz y Stevens coinciden con Nye en que la palabra ciberpoder no transforma el significado del concepto de poder, sino que el prefijo "ciber" hace referencia un lugar, medio o espacio, por lo que el ciberpoder hace referencia al ejercicio del poder dentro del dominio del ciberespacio. Los

autores agregan que el ciberpoder puede ser considerado en situaciones de ciberseguridad como “el uso, o la amenaza de uso, del ciberespacio y otros recursos para lograr objetivos estratégicos en y a través del ciberespacio contra la resistencia o la voluntad de otros” (Betz y Stevens 2011, 43).

van Haaster nos brinda una definición más completa sobre el concepto de ciberpoder al señalar que éste "comprende la variedad de poderes que afectan a los componentes geográficos, lógicos y ciberpersonales[7], de la red física, que en consecuencia dan forma a las experiencias de los actores estatales y no estatales que actúan en y a través del ciberespacio". Además, brinda algunos ejemplos sobre el uso del ciberpoder, como el uso de redes sociales para transformar conductas, el uso de equipo digital para exponer o comprometer un sistema esencial o el uso de fuerza pública, como policía o ejército, para establecer el control físico de una infraestructura (van Haaster 2016, 14).

Por otro lado, Demchak (2012, 128) interpreta a la ciberseguridad como una parte importante de los conflictos actuales, caracterizados por el uso del ciberespacio para el combate, por lo que define al ciberpoder como “la capacidad de los líderes e instituciones de una nación, que enfrenta un conflicto cibernético, de mantener la incertidumbre generalizada, sobre los sistemas cibernéticos nacionales, a niveles tolerables, para satisfacer las expectativas de bienestar de sus ciudadanos”.

El autor considera que el conflicto a través del ciberespacio y la existencia de vulnerabilidades en los sistemas esenciales son inevitables, por lo que deben de mantenerse ocultos a la población en general para no ocasionar pánico y evitar que intervengan en ciberoperaciones. De esta manera, el autor asegura que el ciberpoder, ejercido por un jefe de Estado se ve reflejado

[7] Los componentes ciberpersonales hacen referencia a los perfiles en redes sociales y en otros tipos de servicios, en los que se introducen información personal, incluyendo biometría, para crear cuentas únicas e individuales asociadas a la persona real.

en su capacidad de determinar correctamente qué información de la estrategia ciberseguridad nacional puede ser compartida a la población, y cuál debe mantener oculta, para que los intereses nacionales puedan ser perseguidos.

Añade también, que una efectiva estrategia para ejercer el ciberpoder, es la eliminación y reducción de ventajas que un actor externo puede obtener a través del ciberespacio a partir de vulnerabilidades detectadas en los sistemas nacionales, puesto que, gracias a ellas, un rival puede diseñar ataques efectivos en contra de la infraestructura esencial de un país, incluso si los ataques no hacen uso de computadoras, o dispositivos electrónicos. Al reducir las capacidades que posee un atacante determinado, así como la información que tiene sobre el país, será más sencillo defender los ataques que pudieran ocurrir (Demchak 2012).

Este argumento tiene gran importancia para la ciberseguridad, ya que el ciberespacio, si bien es un "mundo virtual", también depende de una infraestructura física, cuyo adecuado funcionamiento debe mantenerse para realizar todas las actividades digitales, por lo que ambos "mundos" se encuentran fuertemente ligados. De esta forma, se pueden producir efectos importantes en el "mundo real" por sucesos ocurridos en el "mundo virtual", de una forma inmediata y desde cualquier lugar del mundo. Además, el ciberespacio puede funcionar no sólo como dominio de enfrentamiento, sino también como herramienta para la obtención de información con el objetivo de diseñar otro tipo de ataques a través de otros medios (Gartzke y Lindsay 2015).

Después de haber recolectado esta serie de definiciones, así como se realizó con el concepto de poder, podemos crear una definición de ciberpoder que será utilizada a lo largo de este trabajo. Entendemos como ciberpoder a las capacidades, basadas en los recursos informáticos y digitales, que poseen los actores internacionales, estatales y no estatales, de realizar acciones dentro del ciberespacio, que pueden tener un impacto tanto en el mundo virtual, como en el físico y que tienen

como objetivo transformar la forma de actuar de otros actores para alcanzar sus objetivos y perseguir sus intereses.

Con esta definición podemos notar que el concepto de poder llega a evolucionar a ciberpoder sin realmente modificar su esencia, sino que incluye ahora al ciberespacio para describir un nuevo plano en el que es ejercido. Similar a la definición, podemos notar que las características del poder expresadas por Foucault, anteriormente expuestas, también pueden describir claramente al ciberpoder.

El ciberpoder es enigmático, puesto que para ejercerlo es necesario hacerlo a través del ciberespacio, un mundo conformado por equipo tecnológico avanzado cuyo funcionamiento es comprendido por expertos en el área. Es visible, puesto que se pueden observar sus efectos en los equipos computacionales y dispositivos digitales en los que es ejercido, pero al mismo tiempo es invisible, puesto que la mayor cantidad de interacciones se dan a través del "mundo virtual". Se encuentra presente en la gran mayoría de actividades realizadas en el día a día actual, incluyendo actividades esenciales, pero también se encuentra oculto, puesto que, en el mundo físico, sólo son observables sus efectos, más no su ejercicio. Finalmente, se encuentra investido en todas partes, puesto que la red satelital existente alrededor del mundo permite que la geografía no sea un obstáculo para las actividades dentro del ciberespacio.

Lo que queda muy claro es, que el ejercicio del poder a través del ciberespacio en la actualidad, se da a través de las diferentes herramientas tecnológicas que nos permiten explorarlo. Esta característica del poder es observable a lo largo de la historia, puesto que las fuentes de donde surge se han transformado con el paso del tiempo gracias a los avances tecnológicos y los descubrimientos que se han realizado. En la actualidad, Nye (2005) resalta que para consolidar el poder en el escenario internacional, se debe prestar atención en las capacidades de los actores internacionales, particularmente en las de los Estados, como su desarrollo tecnológico, la educación

y el crecimiento económico. También considera que la era de la información ha provocado que el ciberespacio sea la manera principal para alcanzar los niveles de desarrollo necesarios en cada una de estas áreas.

De esta forma podemos decir que las nuevas formas de poder pueden ser observadas por el nuevo tipo de interacciones que se dan entre los diversos actores internacionales a través del ciberespacio. Esto puede ser por acciones ofensivas y coercitivas, como los ciberataques, las campañas de ciberespionaje, los sabotajes y la disrupción. Pero también pueden ser observadas a través de los campos que Nye menciona, como el rápido desarrollo de nuevos dispositivos electrónicos, el comercio electrónico, los servicios gubernamentales digitales, la difusión de información, las redes sociales y la aplicación de tecnología perteneciente a la Industria 4.0 que le proveen de importantes capacidades a los actores de alcanzar sus objetivos y transformar el de los demás.

Similar a lo que menciona Waltz, podemos decir que la importancia de las nuevas formas de poder, particularmente el ciberpoder, no es tener las capacidades de ejercerlo, ni poseer la infraestructura necesaria, sino en lo que se hace con estas capacidades. Y en la actualidad se puede observar que, en los tres niveles de análisis de la disciplina, se ha comenzado a ejercer el ciberpoder para alcanzar objetivos.

A nivel individual, se puede observar que las personas hacen uso diariamente de servicios y dispositivos que dependen del mundo del ciberespacio, creando una huella digital que va en aumento. Es de resaltar que, en los últimos años, la cantidad de personas que poseen un teléfono inteligente ha aumentado considerablemente, por lo que la sociedad depende cada vez más de las redes que los hacen funcionar.

A nivel estatal, podemos observar cómo han surgido preocupaciones por parte de los Estados de ser vulnerables a algún ciberataque crítico, o incluso, que desde el ciberespacio surjan

movimientos sociales que pongan en riesgo el funcionamiento del gobierno. Por esta razón, han adoptado fuertes políticas de ciberseguridad, por ejemplo, el "Gran Cortafuegos"[8] de China o los casos de vigilancia y espionaje de la Agencia de Seguridad Nacional de Estados Unidos hacia sus propios ciudadanos y extranjeros, con el objetivo de salvaguardar su existencia.

A nivel internacional, el ciberespacio es una de las herramientas más importantes para la interacción entre sus actores, pues se utiliza para el intercambio de información, transacciones económicas, coordinación de instituciones, conferencias a través de servicios de video, o incluso, como se verá en la sección siguiente, para los conflictos y combates.

A pesar de que los Estados han enfocado sus esfuerzos en el desarrollo de capacidades que les permitan aprovecharse del ciberespacio, la cantidad de usuarios en él y las múltiples actividades que se pueden realizar utilizándolo, han provocado que una sola dependencia no pueda ser capaz de monitorear todas las actividades que ocurren, por lo que han surgido empresas tecnológicas que se han encargado de cumplir con estas necesidades, incrementando su importancia para el funcionamiento del Estado.

Grandes empresas multinacionales enfocadas en la seguridad informática se han dedicado a la detección continua de nuevos programas maliciosos y la búsqueda de maneras de contrarrestarlos, con el objetivo de mantener los incidentes al mínimo. Este tipo de instituciones se han encargado de detectar los ciberataques con mayor impacto y propagación alrededor del mundo, y liderar la respuesta para mantener sus daños al mínimo.

Casos como el de WannaCry, Duqu, o incluso el mismo NotPetya, de los cuales se hablará posteriormente, fueron detectados por primera vez por instituciones privadas dedicadas a la

[8] En inglés es llamada "*The Great Firewall of China"* hacienda referencia a la Gran Muralla China, realizando un juego de palabras con el término informático "*firewall*", cortafuegos en español, un elemento de una red informática que evita el acceso no autorizado de tercero y monitorea que las comunicaciones que ocurren dentro de la red sean únicamente las autorizadas.

seguridad informática, y fue gracias a su alerta que se comenzó a trabajar en su respuesta. La especialización de este tipo de organizaciones en temas de ciberseguridad les ha permitido no sólo mantenerse a la vanguardia en temas tecnológicos y de programas maliciosos, sino también ha provocado que sean los responsables de salvaguardar la seguridad de millones de equipos informáticos y sistemas ligados a infraestructura esencial, labor que usualmente recaía en las fuerzas armadas de los Estados.

Sin embargo, las empresas no son los únicos actores no estatales que han adquirido mayor poder económico y estratégico con el ciberespacio, puesto que también han surgido ciertos actores que se han beneficiado económicamente con él. Si las empresas de informática han logrado crecer gracias a la detección y defensa de ciberataques, también han aparecido hackers que, de manera independiente o en grupo, se dedican a lo opuesto: la creación, lanzamiento y propagación de programas maliciosos.

Este tipo de actores han generado importantes ganancias económicas, ya sea al utilizar sus propias herramientas y programas malicioso para realizar crímenes para su propio beneficio, como el robo de información privada o el chantaje; o al vender sus "servicios" al mejor postor y diseñar programas de acuerdo a lo que sus clientes requieren. En ocasiones, estos mismos grupos realizan actividades para favorecer los intereses de diferentes Estados, por lo que no siempre son perseguidos legalmente.

El surgimiento de empresas privadas y hackers independientes son una prueba de la importancia que los actores no estatales han adquirido rápidamente, y como sus actividades pueden tener un impacto político, económico y social a nivel internacional. Debido a la creciente actividad de estos actores, han surgido intentos por crear legislación en torno al tema, con el objetivo de establecer reglas que determinen las actividades permitidas en el ciberespacio y perseguir judicialmente a aquellos individuos que las rompan. Sin embargo, así como con diversos aspectos

dentro del ciberespacio, también se han presentado algunas dificultades para determinar con claridad las formas en las que una persona puede ser sentenciada, especialmente por la dificultad de determinar con precisión la identidad a través de la red. Sobre las implicaciones legales del ciberespacio y la responsabilidad social de las empresas y grupos de hackers se profundizará en mayor medida en el tercer capítulo de este trabajo.

A continuación, se explicará como el ciberespacio le ha brindado una nueva dimensión a los conflictos y la manera en que este nuevo recurso implica la adaptación de las fuerzas armadas a un nuevo entorno.

1.2. El ciberespacio como quinto dominio de guerra

A lo largo de la historia, la humanidad ha atravesado periodos de conflicto, y, ya sea a pequeña o gran escala, parece ser que siempre han sido una característica del Sistema Internacional que no parece desaparecer. Waltz (2018), afirma que la guerra es una herramienta utilizada por los Estados para conseguir paz, y que, a pesar de que hay diversas maneras para alcanzarla, existen razones arraigadas en los tres niveles de análisis que provocan que el camino elegido sea el conflicto. Incluso habiendo periodos de paz prolongada, éstos culminan súbitamente con un nuevo enfrentamiento, que usualmente es provocado por Estados en la búsqueda de alcanzar su interés principal, el poder.

El territorio es una de las razones más importantes y comunes para el inicio de conflictos armados, principalmente en casos en los que dos o más grupos o Estados proclaman ser dueños de la misma tierra, ya sea por los recursos naturales que existen en ella, por razones estratégicas o incluso por motivaciones religiosas (Johnson y Toft 2014). Pero, para Waltz (2018), la razón principal detrás de la guerra, es la anarquía que caracteriza al Sistema Internacional, puesto que

provoca que los Estados busquen obtener poder a través de una redistribución de recursos que les brinde mayores capacidades, y por lo tanto, sea más sencillo para ellos asegurar su supervivencia.

Sin duda alguna, la guerra es utilizada por los actores internacionales para alcanzar sus intereses y, sin importar el detonante de la misma, una de sus características más importantes es el uso de la tecnología aplicada para el combate. La guerra está limitada por el tipo de tecnología que es utilizada por los combatientes, ya que define las capacidades que los Estados poseen y por lo mismo, el alcance que el conflicto puede llegar a tener (Van Creveld 1991).

Los caminos construidos, los vehículos diseñados, los mapas utilizados y las líneas de comunicación establecidas han facilitado el movimiento de tropas y han brindado mayor información a los estrategas, y una vez finalizado el conflicto, han beneficiado a la sociedad en general. Muchos de estos avances tecnológicos fueron diseñados con el objetivo de ser aplicados en el combate, o incluso son adaptaciones de objetos ya existentes para brindar ventajas estratégicas a los combatientes (Van Creveld 1991).

La creación de nuevas armas, más efectivas y poderosas, le brindaron grandes ventajas a los que las utilizaban por primera vez, puesto que sus efectos eran desconocidos en ese momento, imposibilitando la creación de un contrataque por parte del rival. La incertidumbre de los alcances que nuevos armamentos podían tener, motivaba a los enemigos a acelerar el fin de la guerra para evitar mayores pérdidas y realizar acuerdos que quizá no hubieran aceptado en otras condiciones (Van Creveld 1991).

De esta forma se puede decir que, mientras la tecnología es más avanzada, los conflictos tienen una duración más corta. Desde el punto de vista estratégico, el avance de la tecnología ha provocado cambios importantes, por lo que se han tenido que generar nuevas tácticas en el combate para adaptarse a estos cambios. El rápido avance tecnológico no sólo abarca a los nuevos tipos de armas que fueron surgiendo con el tiempo, sino que abarca también todo tipo de infraestructura de

guerra utilizada, como la que facilita la comunicación y el transporte, que ha acortado los tiempos de combate (Van Creveld 1991).

Los avances tecnológicos y su impacto en la guerra pueden notarse fácilmente a través de la evolución de las estrategias utilizadas en el combate. Lindsay y Gartzke (2020) consideran que la tecnología militar dota a sus combatientes de características muy particulares para actuar en espacios determinados y los engloba bajo el término "dominios operacionales". Los autores también agregan que las propiedades de cada dominio dependen del "ambiente" en el que se desenvuelven, por lo que los clasifican en cuatro dominios físicos: tierra, mar, aire y espacio; y un quinto dominio virtual, el ciberespacio.

A lo largo de la historia, los Estados que han generado la tecnología adecuada para mantener su superioridad en los dominios de guerra han sido los que han obtenido mayor influencia a nivel internacional. En sus inicios, la guerra se limitaba a enfrentamientos terrestres entre tropas, pero con el paso de tiempo se fue incursionando en la exploración de los océanos y el dominio de los mares se convirtió en una ventaja inigualable. Un ejemplo claro es el dominio de Reino Unido en el S. XIX, que por su poder naval y las grandes redes comerciales construidas a través de sus rutas marítimas se consolidaron como la principal potencia del mundo.

Posteriormente, la llegada del avión y la capacidad de dominar el espacio aéreo transformó la forma en que se combatía, y trajo nuevas ventajas a los diferentes países, siendo la principal, la reducción de tiempos de transporte y la habilidad de alcanzar territorios de difícil acceso. Podemos destacar el caso de los Estados Unidos, que colocó una gran cantidad de bases aéreas y fortaleció su fuerza aérea, lo que le brindó grandes ventajas al combatir en el Pacífico durante la Segunda Guerra Mundial.

Durante la Guerra Fría también podemos notar el avance de la tecnología y su uso estratégico para la obtención de influencia, siendo los Estados Unidos y la Unión Soviética los que

la producían para perseguir sus intereses. La carrera espacial y la generación de las primeras armas atómicas cambiaron nuevamente la forma de combatir, y provocaron que ambos países tuvieran grandes zonas de influencia en el mundo, al ser los únicos capaces de generar y utilizar esa tecnología.

El ciberespacio llega como un nuevo espacio que no es completamente físico, ni completamente virtual. Y, así como ha sucedido a lo largo de la historia, aquellos actores que han generado la tecnología adecuada para mantener su presencia en él, han comenzado a tener una gran influencia en el mundo.

Pero, como se mencionó anteriormente, las tecnologías comenzaron a ser desarrolladas para la navegación de los cuatro dominios físicos, que están limitados por las restricciones de desplazamiento y de coordinación producidas por las características geográficas del entorno. Se pueden colocar vías férreas para un rápido transporte de tropas a largas distancias, construir grandes flotas marinas, bases aéreas o incursionar en el viaje espacial para facilitar el movimiento dentro de los cuatro dominios físicos, pero, sin importar cuantas mejoras tecnológicas surjan, siempre existirán características geográficas fijas que deberán ser consideradas al tomar decisiones tácticas (Lindsay y Gartzke 2020).

Un Estado suele tener presencia militar en los dominios físicos para obtener ventajas comparativas que le faciliten alcanzar objetivos estratégicos y le faciliten combatir a otros Estados. Algunas de estas ventajas son, la implementación de acciones coercitivas más efectivas, disuasión a terceros de realizar ataques, agilización de logística y transporte, aumento de capacidades de defensa de fuerzas externas y recopilación de inteligencia (Lindsay y Gartzke 2020).

Por otro lado, el ciberespacio es un dominio de información caracterizado por ser un entorno virtual que depende directamente de una infraestructura física localizada en los cuatro dominios físicos. Es un "entorno flexible, construido por los humanos y gobernado

institucionalmente", que posee una barrera de entrada muy baja, provocando que la presencia en él, no sea exclusiva de los Estados o de sus fuerzas militares, sino que miles de personas pueden interactuar a través de él sin tener la necesidad de utilizar equipos sofisticados (Lindsay y Gartzke 2020, 22).

Para defenderse en los cuatro dominios físicos, un Estado debe de prestar atención a las capacidades y acciones realizadas por otros Estados, particularmente las grandes potencias o aquellos con capacidades suficientes de comenzar un ataque. En el ciberespacio, todos pueden participar, por lo que Estados con menos recursos, actores no estatales e individuos, pueden tomar parte en el conflicto, provocando que la guerra no sea exclusiva del ejército.

Por lo anterior, se puede considerar que el ciberespacio surgió como una nueva innovación tecnológica, cuya aplicación en la guerra fue inevitable debido a las grandes ventajas que les brinda a los combatientes. No sólo aumenta las capacidades de los actores internacionales, sino que provoca que el conflicto sea más acelerado y dinámico, trayendo nuevas situaciones y escenarios que no habían sido contemplados anteriormente.

Así como la guerra tradicional, la ciberguerra sirve como un medio para alcanzar los objetivos, y para obtener nuevas capacidades que le brindan poder a los actores internacionales. Sin embargo, a diferencia de los conflictos tradicionales, los ataques realizados a través del ciberespacio no dependen de la ubicación geográfica, por lo que se pueden provocar severos daños, desde una distancia segura, sin exponer la identidad del atacante y dificultando la implementación de medidas de retribución (Demchak 2012).

El ciberespacio también les permite a los actores internacionales realizar actividades con discreción, a bajo costo y con rapidez, por lo que el combate es de poca duración y los ciberataques son muy fáciles de realizar. También les permite engañar a los demás actores y confundirlos sobre

los verdaderos objetivos que buscan alcanzar, por lo que facilita realizar campañas de ciberespionaje y recolectar inteligencia sin ser detectados (Lindsay y Gartzke 2020).

Los dispositivos electrónicos también son utilizados en la guerra como soporte a los dominios físicos, puesto que las fuerzas militares modernas dependen de ellos y de redes digitales para ser desplegadas. La ciberguerra entonces está caracterizada por el aprovechamiento de vulnerabilidades en equipos digitales para generar sabotaje, disrupción y desinformación en los sistemas rivales, que puedan provocar daños en diferentes sectores. Al mismo tiempo, el ciberespacio también funciona para proveer información a las fuerzas de los otros dominios y para coordinar ataques híbridos en los que se involucren las fuerzas de todos los dominios (Lindsay y Gartzke 2020).

El uso de recursos basados en Tecnologías de la Información (TI) para la guerra es estudiado comúnmente por los expertos, pero existe un debate acerca del término "ciberguerra", ya que algunos académicos afirman que las actividades realizadas en el ciberespacio no tienen un impacto suficiente para ser considerados guerra, sino que se debe considerar únicamente como un tipo de combate.

Demchak (2012), considera que la ciberguerra es aquella en la que el triunfo o derrota depende directamente del uso de medios digitales o infraestructura del ciberespacio para realizar actividades clave, como el ataque y la defensa, en el transcurso de todos los conflictos. También considera que es altamente probable que los conflictos a través del ciberespacio terminen evolucionando a enfrentamientos a través de los otros dominios de guerra, por lo que afirma que los recursos cibernéticos son utilizados como apoyo a ataques simultáneos de otro tipo.

Gartzke (2013) considera que el conflicto a través del internet no puede ser considerado guerra, puesto que usualmente las actividades realizadas en el ciberespacio sirven para auxiliar otro tipo de actividades, comúnmente realizadas por un ejército presente en alguno de los dominios

físicos. Además, agrega que el conflicto en el ciberespacio no puede ser considerado aisladamente como una característica del Sistema Internacional anárquico, debido a que los Estados dependen de los otros dominios para alcanzar el poder.

El autor también afirma que un ataque suficientemente poderoso a través del ciberespacio puede provocar daños inesperados e inimaginables, y debido a la profunda interconexión del mundo, estos daños pueden ocurrir incluso en infraestructura propia. Para evitar generar afectaciones imprevistas, las capacidades del ciberespacio son utilizadas usualmente para implementar ciberataques dirigidos a objetivos específicos e intentando limitar los daños a los mismos (Gartzke 2013).

Gartzke (2013) también nos brinda características del conflicto a través del ciberespacio, expresando que comúnmente los daños ocasionados por ciberataques son sumamente costosos, pero que son temporales y su reparación es rápida. También afirma que los ciberataques de mayor importancia son aquellos que producen consecuencias políticas, y no económicas, puesto que generan cambios en la distribución de poder de los actores internacionales, y puede contribuir a generar otro tipo de conflicto más tradicional.

Nye (2005) agrega que otra característica de los conflictos a través del ciberespacio es la difusión de poder, lo que quiere decir que, en la escena internacional actual, los ciberataques pueden ser diseñados por un amplio espectro de actores no tradicionales, que pueden ir de gobiernos, a grupos e individuos, o una combinación de ellos, que anteriormente no solían participar en la escena internacional.

También afirma que este tipo de conflictos, y toda la actividad en el ciberespacio en general, se concentran en la obtención y el uso de información, para posteriormente realizar acciones que faciliten la obtención de poder y la búsqueda de intereses. Por esta razón, la información se clasifica en tres dimensiones distintas, con características propias: El flujo de datos,

que engloba principalmente a las noticias e información general para todo público y que es de fácil acceso. La información utilizada como ventaja en situaciones competitivas, la cual es obtenida a través de la investigación y exploración científica, por lo que brinda ventajas a aquellos que la descubren primero. Y, por último, la información estratégica, que es el conocimiento obtenido de los actores rivales, usualmente a través de espionaje y acciones secretas de inteligencia (Nye 2005).

Una diferencia esencial que hay que resaltar entre la ciberguerra y la guerra tradicional, es que la primera no ha ocasionado víctimas mortales y su impacto se mide a través de los daños materiales y económicos que produce. Como se ha mencionado anteriormente, los combatientes se mantienen a una distancia segura, y, a pesar de que exista la posibilidad de que un ciberataque produzca daños irreparables a una infraestructura determinada que desencadene en la pérdida de vidas, esto no ha ocurrido (Kello 2013).

Sin embargo, incluso si un ciberataque no ocasiona destrucción física, no quiere decir que no sean peligroso para todos los actores que interactúan a través del ciberespacio. La capacidad de producir daños económicos, políticos y sociales, a través de recursos digitales, sin tener que hacer uso de violencia, le brinda un amplio abanico de opciones a los actores internacionales, que pueden hacer uso de diferentes estrategias a través del ciberespacio para alcanzar sus objetivos (Kello 2013).

Como se ha observado en los párrafos anteriores, la guerra se va adaptando a las condiciones existentes en el momento en que estalla, y los participantes de ella utilizan todos los recursos a su alcance para salir vencedores. El ciberespacio es por lo tanto un nuevo dominio que debe ser considerado al hablar del conflicto moderno, porque, ya sea de forma directa o indirecta, es un elemento utilizado por los actores internacionales.

Ya sea para provocar sabotaje, para difundir propaganda, obtener información confidencial, o tan sólo coordinar el movimiento de las fuerzas armadas, los equipos digitales se han consolidado

como infraestructura esencial de todos los Estados de un Sistema Internacional que debe incluir a actores que no habían sido considerados con anterioridad y que ahora tienen el poder de influir en los eventos del mundo.

La importancia de la ciberguerra en el escenario internacional actual recae en su uso continuo para obtener ventajas estratégicas sobre otros actores. Finalmente, el objetivo del conflicto a través del ciberespacio es obtener y ejercer poder para mantener una mayor influencia en el Sistema Internacional que el resto de los actores.

Tras haber detallado las características de la ciberguerra y haber expuesto la importancia de ésta para las Relaciones Internacionales, a continuación, se expondrán los diferentes riesgos existentes para los cibernautas[9], así como los principales ciberataques utilizados actualmente.

1.3. Los riesgos del ciberespacio

El ciberespacio es un vasto mundo lleno de posibilidades para todos sus usuarios. La gran cantidad de información que se transmite diariamente permite que las personas puedan realizar una diversidad de actividades con el uso de dispositivos digitales. Y de la misma manera en la que los criminales se aprovechan de oportunidades en el mundo físico para beneficiarse personalmente, también sucede lo mismo en el ciberespacio.

Los equipos conectados a la red están expuestos a diferentes amenazas que pueden afectar su correcto funcionamiento sin el conocimiento del usuario. Se pueden llegar a infectar por diferentes tipos de virus, pueden estar siendo monitoreados para recabar información o incluso pueden estar siendo utilizados para otro tipo de actividades que no necesariamente son deseadas.

[9] Aquellas personas que navegan por el ciberespacio.

Este tipo de actividades son realizadas usualmente por individuos denominados "hackers", término utilizado originalmente para referirse a los expertos con conocimientos técnicos en informática que realizaban lo que deseaban a través del ciberespacio, incluso cuando implicara quebrar las reglas. En la actualidad, el término ha evolucionado para referirse a todos los individuos que detectan vulnerabilidades en sistemas, programas, o redes computacionales para aprovecharse de ellas, no necesariamente con intenciones maliciosas (Singer y Friedman 2014).

Existen diversas categorías de hackers, pero se pueden destacar los denominados "*white hat hackers",* o hackers de "sombrero blanco", quienes se especializan en el aspecto de defensa en la ciberseguridad, pues intentan detectar las vulnerabilidades de un sistema para corregirlas antes de que puedan aprovecharse de ellas. Mientras que por otro lado, existen los *"black hat hackers"*, o hackers de "sombrero negro", quienes buscan penetrar las redes con intenciones maliciosas o para beneficio personal (Singer y Friedman 2014).

Por esta razón, la rápida evolución y adaptabilidad de las amenazas del ciberespacio es uno de los retos más grandes para la ciberseguridad actual, ya que continuamente surgen nuevas y complejas técnicas de hackeo que comprometen sistemas en cuestión de segundos, provocando que, para defender efectivamente un sistema, la respuesta deba ser inmediata. (The Small Business Innovation Research (SBIR) y Small Business Technology Transfer (STTR) 2021).

Para poder defenderse de las diferentes amenazas, es importante conocerlas, y esto es un gran reto para los especialistas en ciberseguridad, puesto que pueden originarse desde múltiples direcciones y, aun cuando la amenaza es conocida, puede tener un grado de sofisticación muy elevado y estar dirigida a un objetivo muy específico, por lo que el evitar sufrir de ella puede resultar inevitable (Choo 2011).

De forma general, podemos decir que una ciberamenaza es "una actividad destinada a comprometer la seguridad de un sistema informático, alterando la disponibilidad, integridad o

confidencialidad de un sistema o la información que contiene". Son creadas por actores que buscan detectar vulnerabilidades en los equipos de sus víctimas para aprovecharse de ellas de forma desapercibida y obtener acceso a su información personal y sus redes (Canadian Centre for Cyber Security 2020, 2).

1.3.1. Tipos de ciberamenazas.

Las ciberamenazas pueden tomar una gran variedad de formas y pueden ser modificadas de acuerdo con el objetivo que se desea atacar, pero la gran mayoría de técnicas utilizadas hacen uso de programas maliciosos, o *malware*, que funcionan como la herramienta principal para aprovecharse de las vulnerabilidades de un equipo determinado. Dentro de los *malware* podemos considerar a los virus computacionales, gusanos, caballos de troya, *spyware*, *adware*, y otros tipos de *software* no deseados, que realizan diferentes tareas de acuerdo a los propósitos planteados (Seemma, Nandhini, y Sowmiya 2018).

Los virus informáticos son de las amenazas más comunes en el ciberespacio, y su facilidad de creación y difusión generan importantes retos para los expertos en ciberseguridad. Un virus informático es un tipo de programa que ocasiona efectos secundarios en los equipos a los que infecta y modifica los programas del sistema operativo en el que residen, para causar daños a la computadora. Los virus no son necesariamente maliciosos, pero los efectos secundarios que ocasionan pueden ser indeseados, puesto que éstos ocurren comúnmente sin el conocimiento de la víctima (Horton y Seberry 1997).

Algunos efectos producidos por virus informáticos son la eliminación de archivos y programas, la corrupción del almacenamiento del equipo y la falla del sistema operativo, lo que puede llevar a que el equipo sea inutilizable (Canadian Centre for Cyber Security 2020). Los virus son muy comunes en el internet y el usuario común está expuesto a infectarse fácilmente. Las

empresas de ciberseguridad dedicadas a proveer servicios de antivirus y detección de amenazas actualizan constantemente sus servidores con una lista de virus que se expande continuamente.

Los virus pueden ser fácilmente confundidos con los gusanos, pero es importante aclarar que no son lo mismo. Mientras un virus informático busca neutralizar un equipo en específico e infecta a los archivos dentro de una computadora en particular, un gusano busca expandirse a través de una red para afectar un sistema entero (Horton y Seberry 1997).

El gusano crea copias de sí mismo y las esparce a otras computadoras dentro de una red para tener un alcance mayor. Las copias poseen las mismas funciones que el archivo original, y mantienen comunicación con él, también son capaces de ejecutar las mismas funciones, aumentando sus capacidades de expansión. Cuando el gusano logra estar presente en toda la red, puede aprovecharse de los recursos de las computadoras o dañarlas para crear afectaciones en el sistema entero (Canadian Centre for Cyber Security 2020).

Otras de las amenazas más comunes y efectivas en el ciberespacio son los caballos de troya, también llamados troyanos, los cuales son programas maliciosos "disfrazados" de programas verdaderos. Es un *software* que afirma realizar una actividad específica, pero que, en realidad, está realizando otras actividades sin que el usuario lo sepa. Cuando infectan un equipo pueden provocar daños similares a los virus y gusanos, pero a diferencia de ellos, los troyanos no buscan propagarse, por lo que se mantienen en la misma computadora (Canadian Centre for Cyber Security 2020).

Los troyanos están diseñados para que los usuarios los descarguen por voluntad propia, ya que aparentan ser un programa legítimo, pero poseen múltiples características ocultas que se activan una vez que el programa logra instalarse en el equipo. Los troyanos pueden ser utilizados para posteriormente instalar virus o gusanos y aumentar los daños, por lo que su peligro es significativo dentro de la ciberseguridad (Horton y Seberry 1997).

Dentro de las amenazas presentes en la red también existen los *adware* y los *spyware*. *Adware* es la abreviación en inglés de "*advertising software*" y es un programa diseñado para recopilar la información del usuario de una computadora para bombardearlo de anuncios dirigidos de acuerdo con su perfil. Por otro lado, el *spyware* es un programa malicioso diseñado para realizar un seguimiento de las acciones realizadas por el usuario en un equipo infectado. Su origen proviene de las palabras en inglés "*spying software"* y existe una gran variedad de programas que recopilan diferente información, como el registro de pulsaciones de teclas, el acceso a micrófono y cámara web, el monitoreo de los hábitos de navegación y la captura de usuarios y contraseñas de diversos sitios (Canadian Centre for Cyber Security 2020).

Tanto el *adware* como el *spyware* son programas diseñados para la captura de información de un equipo sin el consentimiento del usuario y usualmente su peligro recae en lo que se hace posteriormente con esa información, ya que puede ser vendida a terceros o ser utilizada para el diseño de ataques más sofisticados.

Las amenazas descritas anteriormente conforman una gran parte de las amenazas presentes en la red, pero, sin duda alguna, en los últimos años, la presencia de las infecciones con programas de tipo *ransomware* han sido cada vez más notorias. En la actualidad, es uno de los principales problemas de la ciberseguridad, ya que sus víctimas pertenecen a diversos sectores de la sociedad, que van desde grandes empresas multinacionales a dependencias gubernamentales.

Un *ransomware* es un tipo de programa malicioso, a través del cual, un atacante restringe a un usuario el acceso a sus archivos, o incluso a su equipo, usando una variedad de métodos, como, por ejemplo, la encriptación. Posteriormente, solicita un pago a cambio del desbloqueo de los archivos. Una analogía que podría utilizarse, es que el atacante "secuestra" la información del usuario y exige un "rescate" a cambio de ella (Seemma, Nandhini, y Sowmiya 2018).

Para que el usuario pueda obtener nuevamente acceso a su información, debe pagar el rescate, usualmente con alguna criptomoneda que sea difícilmente rastreable. En los casos más recientes de *ransomware*, se ha notado que la criptomoneda de preferencia de los cibercriminales es el Bitcoin (Canadian Centre for Cyber Security 2020).

El objetivo esencial del *ransomware* es bloquear el acceso a la información para provocar pánico y miedo en la víctima, y lo logra a través de diferentes métodos que afecten el desempeño del equipo. Para lograr conseguir el pago del rescate, los atacantes usualmente amenazan al usuario con revelar información sensible, personal o vergonzosa en caso de que el pago no sea realizado. Este tipo de programas son usualmente instalados a través del uso de troyanos o gusanos que descargan el programa sin aviso (Canadian Centre for Cyber Security 2020).

La rápida propagación de ciberataques de tipo *ransomware* se debe a que los cibercriminales pueden obtener importantes ganancias económicas con un riesgo muy bajo y de una forma rápida. Usualmente las víctimas optan por pagar el rescate a arriesgarse a que su información quede expuesta o a perder sus archivos. Además, los equipos infectados normalmente son parte esencial del funcionamiento de la red afectada, por lo que la urgencia de reestablecerlos orilla a las víctimas a pagar (Mansfield-Devine 2017).

Usualmente son utilizados de dos maneras, la primera como se ha mencionado anteriormente, para obtener dinero a cambio del rescate de la información, en donde no importa el objetivo atacado, por lo que se intenta infectar a la mayor cantidad de personas posible. En segundo lugar, se utiliza para crear disrupción, puesto que los atacantes lo único que buscan es crear inestabilidad, detener operaciones y dañar los equipos, sin tener verdaderamente las intenciones de "devolver la información" tras el pago del rescate (Mansfield-Devine 2017).

1.3.2. Tipos de actores de ciberamenazas

Los diferentes tipos de riesgos existentes en el ciberespacio representan un gran peligro a la ciberseguridad por sí mismos, pero se convierten en mayores amenazas cuando son utilizados para realizar ataques sofisticados a objetivos específicos por parte de actores con grandes capacidades económicas e intereses particulares.

Debido a la baja barrera de acceso existente en el ciberespacio, con el paso del tiempo hay cada vez una mayor diversidad de actores que recurren a las ciberamenazas para alcanzar sus objetivos. En la siguiente tabla se exponen algunos de los actores principales que participan en la creación y uso de ciberamenazas y las motivaciones detrás de ello:

Tabla 1.

Actores que participan en ciberamenazas y sus motivaciones.

Actores	**Motivaciones**
Estados y hackers patrocinados por gobiernos	Obtener inteligencia y ventajas estratégicas. Alcanzar intereses geopolíticos. Mermar las capacidades de fuerzas opuestas.
Cibercriminales	Obtener ganancias económicas y beneficios personales.
Hacktivistas	Difundir ideologías, apoyar movimientos sociales y favorecer causas específicas.
Grupos Extremistas	Difundir ideologías, reclutar nuevos adeptos, entrenar reclutas, expandir su alcance geográfico y crear caos o daños en objetivos rivales.
Buscadores de Emociones	Satisfacción y sentido de autorrealización.

Actores Internos	Descontento con la situación en la que se encuentra. Venganza.

Los actores internacionales poseen diferentes motivaciones para participar en ciberamenazas ya que le brindan ventajas para alcanzar sus objetivos. *Tabla elaborada con información obtenida de Canadian Centre for Cyber Security (2020).*

1.3.2.1 Estados y hackers patrocinados por el Estado

Los ciberataques realizados por actores estatales o por hackers patrocinados por el Estado usualmente poseen un grado muy elevado de sofisticación al poseer una gran cantidad de recursos, infraestructura y personas preparadas para llevar a cabo operaciones que necesitan de una planeación y coordinación extensa (Canadian Centre for Cyber Security 2020).

El objetivo principal de este tipo de actores es realizar actividades que favorezcan el cumplimiento de los intereses nacionales y usualmente sus operaciones son secretas para evitar conflictos con otros Estados (Ablon 2018). Algunas de estas actividades son la recolección de inteligencia, la infiltración a redes de otros Estados, el ciberespionaje, sabotaje estratégico, disrupción de sistemas y más recientemente, la interferencia en los procesos electorales de otros países (Sailio, Latvala, y Szanto 2020).

El ciberespionaje es, sin duda alguna, una de las principales actividades realizadas por los Estados, ya que les brinda grandes ventajas estratégicas y oportunidades de diseñar ciberoperaciones posteriores. La información recabada es utilizada exclusivamente por el Estado para sus propios beneficios y no es compartida en la red. Sin embargo, se han dado casos en los que se pueden encontrar en el mercado negro, las herramientas que utilizaron para aprovecharse de las vulnerabilidades de los sistemas de otros Estados, por lo que surgen nuevas amenazas, más sofisticadas y fácilmente distribuibles (Ablon 2018).

Otra de las estrategias utilizadas por los actores estatales es el sabotaje estratégico, en el que buscan reducir o eliminar las capacidades que tienen otros Estados, usualmente para prevenir

un posible ataque o para evitar que la competencia los supere. Se profundizará del uso del sabotaje por el Estado más adelante, ya que su entendimiento es esencial para este estudio (Sailio, Latvala, y Szanto 2020).

Una de las razones por las que los Estados recurren a la realización de ciberoperaciones es evitar sanciones internacionales, puesto que pueden hacer actividades que no son aprobadas por la comunidad internacional sin ser castigados. Usualmente las ciberoperaciones tienen objetivos similares a las realizadas por otros medios, particularmente militares, pero evitan una escalada de violencia que puede evolucionar en un conflicto (Sailio, Latvala, y Szanto 2020).

Asimismo, las ciberoperaciones son muy difíciles de atribuir a actores específicos debido a las complicaciones de determinar con exactitud la ubicación geográfica de su origen, además de que existe una facilidad de negar las acusaciones por falta de pruebas precisas. E incluso, si se lograra determinar con precisión el origen de un ciberataque, no existe una base legal sólida a nivel internacional para castigar a los culpables (Sailio, Latvala, y Szanto 2020).

Se debe de destacar la disparidad entre la retórica de los líderes de Estado y las acciones que realizan, puesto que, en múltiples ocasiones, jefes de Estado han condenado ciberataques realizados en contra de sus países, pero al mismo tiempo mantienen operaciones en el ciberespacio a través de sus dependencias gubernamentales en contra de otros países. Los Estados no consideran que sus acciones en el ciberespacio sean "ilegales", sino que favorecen la idea de que actúan de acuerdo a su propio marco legal y con el propósito de favorecer a su país, por lo que la gran mayoría ha aceptado el uso de ciberoperaciones que les benefician como una medida legítima en la búsqueda de sus intereses, pero denuncian las mismas acciones cuando son realizadas en contra de ellos (Ablon 2018).

Un ejemplo son los reclamos del gobierno ruso en contra de Estados Unidos, acusándolos de ser responsables de un ciberataque dirigido a su red eléctrica en 2019 y desaprobando las

acciones. Sin embargo, se cree que Rusia ha realizado las mismas acciones en contra de la red eléctrica de Ucrania, casos de los que se hablará posteriormente. Se puede observar claramente como las acciones de Rusia contradicen al discurso planteado sobre los ciberataques que había sufrido.

La infraestructura utilizada para aprovecharse del ciberespacio le proporciona grandes ventajas estratégicas a los Estados para perseguir sus intereses, sin la necesidad de tener repercusiones desfavorables a nivel internacional, por lo que son uno de los actores de ciberamenazas principales.

1.3.2.2. Cibercriminales

Uno de los riesgos más comunes e importantes dentro del ciberespacio es el cibercrimen, que es la realización de actividades ilícitas a través del ciberespacio, usualmente dirigidas a cibernautas comunes (Seemma, Nandhini, y Sowmiya 2018). Los cibercriminales están motivados por ganancias económicas, siendo su único interés verdadero el obtener dinero, por lo que buscan acceder a la información personal de sus víctimas con el propósito de "monetizarla". Esto puede realizarse de múltiples maneras, desde robar información financiera para obtener acceso a cuentas bancarias, o venderla en mercados negros del internet. También pueden prestar sus servicios a terceros y realizar este tipo de actividades a cambio de una remuneración económica (Ablon 2018).

Este tipo de actores cuentan con un nivel de sofisticación moderado, pero, pueden llegar a ocasionar daños importantes a un gran número de personas si cuentan con un grado elevado de planeación y soporte, además de capacidades técnicas especializadas que les permitan crear *software* sofisticado. Asimismo, si poseen una estructura sólida establecida y los recursos suficientes, en lugar de hacer un único ciberataque, pueden realizar largas campañas de ciberataques para alcanzar sus objetivos, este tipo de amenazas son conocidas como amenazas

persistentes avanzadas[10] (APT por sus siglas en inglés) y representan un riesgo mayor para sus víctimas (Canadian Centre for Cyber Security 2020).

Los cibercriminales buscan ejecutar sus acciones sin enfrentar consecuencias legales, por lo que las herramientas que utilizan, así como los mercados en donde venden la información recolectada, se mantienen en un constante cambio, evolucionando rápidamente e innovando a un ritmo acelerado. También utilizan diferentes técnicas para encubrir sus comunicaciones y sus transacciones, como el uso de redes privadas virtuales[11], encriptación y el uso de criptomonedas (Ablon 2018).

Los cibercriminales son la primera fuente de incidentes en el mundo, y debido a la amplia variedad de actividades que pueden realizar, se pueden clasificar en tres categorías (Sailio, Latvala, y Szanto 2020):

1. *Estafas Masivas y Hackeo Automático*: Este tipo de cibercriminales buscan infectar la mayor cantidad de computadoras, sin importar su ubicación o identidad. A través del uso de programas maliciosos, obtienen información privada para venderla o utilizarla para acceder a cuentas bancarias (Sailio, Latvala, y Szanto 2020).
2. *Proveedores de Infraestructura Criminal*: Buscan infectar a una gran cantidad de equipos para posteriormente utilizarlos en otro tipo de actividades ilícitas. Los cibercriminales pueden vender el uso de esta red de equipos infectados a terceros para que realicen ciberataques específicos. Los equipos infectados mantienen el mismo funcionamiento y es difícil notar que están siendo utilizados para otras

[10] Las amenazas persistentes avanzadas provienen del término en inglés "*Advanced Persistent Threat"* y Singer y Friedman (2014) lo definen como "una campaña de ciberataques dirigidos a objetivos específicos, conducida y dirigida por un equipo coordinado de expertos especializados, combinando organización, inteligencia, complejidad y paciencia".

[11] El término original en inglés es *"Virtual Private Network (VPN)"*

actividades, hasta que son catalogados en una lista negra pública por actividades maliciosas (Sailio, Latvala, y Szanto 2020).

3. *Cazadores de Caza Mayor:* Son cibercriminales que realizan grandes esfuerzos para atacar a uno, o pocos, objetivos, muy específicos y de muy alto valor. Diseñan programas maliciosos especializados para penetrar las redes del objetivo a atacar y estudian por largos periodos de tiempo las actividades realizadas por sus víctimas para planear sus ciberataques (Sailio, Latvala, y Szanto 2020).

Para la seguridad nacional de un país determinado, los cibercriminales deben ser considerados como una de las principales amenazas, tanto por su continua actividad, como por el impacto que tienen en sus víctimas y en el sistema a corto y largo plazo, puesto que un evento individual puede desencadenar una serie de actividades que pueden poner en riesgo redes enteras.

A corto plazo, un cibercrimen tiene principalmente consecuencias económicas muy importantes, no sólo por el dinero que se puede llegar a perder por un ciberataque, sino por la inversión que debe ser realizada para restaurar el funcionamiento de los dispositivos afectados. Las empresas y las oficinas gubernamentales deben detener operaciones para asegurarse del correcto funcionamiento de sus redes y, si bien, estas afectaciones pueden ser fáciles de eliminar o reparar, deben asignar recursos adicionales para la recuperación de sus equipos o para la restauración de las funciones perdidas, por lo que el costo de sufrir un cibercrimen puede llegar a ser muy elevado (Choo 2011).

Por otro lado, a largo plazo el impacto de un cibercrimen puede tener mayor gravedad y provocar consecuencias más severas. Se puede producir un descontento social generalizado en las instituciones gubernamentales producido por la pérdida de la confianza al no haber evitado una brecha de seguridad importante. O incluso, se puede dar la pérdida de propiedad intelectual, lo que

puede afectar el desempeño y competencia de las empresas en el mercado, o reducir las ventajas estratégicas de gobierno y ejército (Choo 2011).

El cibercrimen continúa siendo una de las actividades más atractivas para generar dinero rápidamente, puesto que se pueden obtener grandes cantidades de dinero a través de programas maliciosos. Kaspersky Lab estima que las ganancias de un cibercriminal van de $10,000 a $72,200 USD por cada 100 víctimas, dependiendo del tipo actividades que realiza y las herramientas que utiliza, por lo que la pérdida total anual provocada por el cibercrimen ronda los 400 mil millones de dólares a nivel mundial, siendo una actividad altamente redituable (N. Lee 2015; Kaspersky Lab 2014).

De acuerdo a un reporte anual realizado por IBM, se estima que, tras un ciberataque, una empresa puede llegar a perder en promedio 4 millones de dólares por cuatro razones principales: El dinero perdido por el cese de operaciones o por el robo de fondos ocasionado directamente por el incidente; el costo de actividades realizadas para detectar la intrusión a los sistemas y el manejo inmediato del incidente; el costo de notificar a clientes y socios la exposición de información privada y los costos legales que implica la pérdida de información confidencial, y por último, los costos de restablecer operaciones para el regreso de actividades normales. Con estos datos, se estima que un cibercriminal puede llegar a obtener hasta $2,000,000 USD anuales (IBM Corporation 2020).

1.3.2.3. Hacktivistas

Los hacktivistas son grupos de personas que buscan impulsar causas específicas, a través acciones que van en contra de las reglas de seguridad computacional y que les permitan obtener mayor exposición (Sailio, Latvala, y Szanto 2020). Las causas que los hacktivistas tienden a

apoyar, suelen tener una carga ideológica y buscan crear cambios políticos, económicos y sociales, ya sea dentro de un territorio específico, o a nivel global (Ablon 2018).

Sin embargo, los hacktivistas pueden estar involucrados en todo tipo de temáticas, desde la defensa de los derechos humanos y las protestas en contra de empresas transnacionales por derechos laborales, hasta la publicación de información privada de celebridades o simplemente la persecución de otras ideologías con las que no concuerdan (Ablon 2018).

Los hacktivistas usualmente se encuentran en un nivel muy bajo de sofisticación, puesto que utilizan herramientas de fácil obtención en el ciberespacio y sus ciberataques no requieren de altos niveles de habilidad para ser desplegados. El uso de herramientas poco sofisticadas también se realiza con la intención de que cualquier miembro del movimiento pueda utilizarlas, ya que los ciberataques son tan sólo una herramienta adicional para transmitir su mensaje, y no su medio principal (Canadian Centre for Cyber Security 2020).

De la misma manera, sus ataques no suelen crear daños o impactos severos en los objetivos que atacan, puesto que la motivación principal es transmitir un mensaje y difundir una ideología, y no generar daños. Aunque, no se descarta que un grupo de hacktivistas pueda crear un ciberataque con consecuencias de este tipo con el propósito de crear un mayor impacto y difusión (Canadian Centre for Cyber Security 2020).

Las ciberamenazas creadas por hacktivistas abarcan la publicación de información sensible de personas particulares, incluyendo información confidencial y propiedad intelectual, como símbolo de apoyo a la libertad de expresión; denegar el acceso a sitios web de organizaciones a las

que protestan a través de ataques de tipo DoS[12] y DDoS[13]; y el uso de diversos métodos que les permitan recibir un mayor número de seguidores, usualmente a través de redes sociales (Ablon 2018).

Debido a que los hacktivistas se pronuncian abiertamente en contra de las instituciones que buscan transformar, tienden a ser claramente identificados, tanto por las mismas instituciones, como por diferentes gobiernos. Debido a lo anterior, las instituciones suelen monitorearlos continuamente para tener conocimiento de sus actividades, y encontrarse preparados para reparar rápidamente los daños producidos de un inminente ciberataque de un grupo hacktivista (Sailio, Latvala, y Szanto 2020).

Los hacktivistas se mantienen bajo la vigilancia de las instituciones de seguridad por el impacto que pueden tener en la red. Si bien, sus ciberataques se encuentran dirigidos a objetivos muy específicos, y buscan producir efectos muy focalizados que no llegan a impactar a otros actores, sus acciones se deben de tomar en cuenta al momento de estudiar los diferentes tipos de amenazas existentes en la red.

1.3.2.4. Grupos Extremistas

Los ciberataques por grupos extremistas suelen ser catalogados en la literatura existente como "ciberterrorismo", término que surge tras la unión de dos de las problemáticas modernas más comunes: Los ataques a través del uso de tecnología y los ataques "terroristas" tradicionales. Las ciberamenazas creadas por grupos extremistas tienen una fuerte motivación política, y buscan

[12] DoS son las siglas en inglés de "*Denial of Service"* que traducido al español significa Denegación de Servicio. En un tipo de ciberataque en el que el atacante busca saturar un sistema en específico al realizar miles de solicitudes de servicio simultáneamente, provocando que el sistema colapse y deje de funcionar (Grupo de Trabajo de Ciberriesgos de AGERS - ISMS FORUM 2017).

[13] DDoS son las siglas en inglés de "*Distributed Denial of Service"* que traducido al español significa Denegación Distribuida de Servicio. Es una variante de DoS en la que el ciberataque proviene de múltiples fuentes, usualmente desde cientos de equipos controlados por terceros. Provoca que una red específica deje de funcionar al saturarse de solicitudes (Grupo de Trabajo de Ciberriesgos de AGERS - ISMS FORUM 2017).

intimidar, coaccionar o influenciar a una población, forzar a realizar un cambio político o provocar miedo y daños físicos en un territorio específico (Ablon 2018).

El término "ciberterrorismo" se ha convertido en una etiqueta utilizada subjetivamente por los gobiernos y organizaciones. Los grupos señalados como "terroristas" en un conflicto, son considerados como “héroes” o “luchadores por la libertad” por sus partidarios, por lo que es complejo determinar si una organización es "terrorista". Sin embargo, un gran número de autores concuerda que los actores que participan en este tipo de amenazas están dispuestos a realizar acciones que inciten terror a la población a través del uso de computadoras para impulsar su ideología y utilizando el miedo para impulsar objetivos políticos (Sailio, Latvala, y Szanto 2020).

Un ciberataque dirigido a una población en específico puede producir pérdida económica significativa, impacto psicológico, e incluso la pérdida de vidas humanas. Cuando un ciberataque ocasiona impactos psicológicos negativos en la población y daña el funcionamiento de la sociedad, se le considera “basado en efectos”. Cuando un ciberataque se lleva a cabo para lograr objetivos políticos o ideológicos, sin impactar directamente a la población, se le considera "basado en intención" (Albahar 2019).

Es importante aclarar que un ciberataque, que haya provocado consecuencias significativas y daños importantes en una sociedad nunca ha ocurrido, y que los grupos extremistas suelen utilizar al ciberespacio más como una herramienta de soporte, que como un medio principal para generar ataques. Este tipo de actores, participa en ciberamenazas que le permitan obtener información estratégica, propagar su ideología, reclutar, conocer y conectar con personas con el mismo pensamiento, difundir propaganda y entrenar adeptos (Ablon 2018).

En la actualidad, los grupos extremistas no poseen niveles elevados de sofisticación, puesto que se mantienen utilizando otros métodos, normalmente en el mundo físico, para provocar el miedo en la población (Canadian Centre for Cyber Security 2020). Sin embargo, si estos grupos

llegaran a desarrollar capacidades tecnológicas avanzadas y obtuvieran los recursos económicos necesarios, podrían realizar ciberataques que provoquen daños importantes a la infraestructura esencial de una población y caos en el funcionamiento de una sociedad en específico, como detener las redes ferroviarias, dañar el sistema de agua y drenaje o incluso alterar las luces de tráfico de las ciudades (Ablon 2018).

Los grupos extremistas representan una seria amenaza a la ciberseguridad de los países. En la actualidad, por las fuerzas que pueden ir sumando a través del ciberespacio y la rapidez y facilidad que poseen para propagar sus ideologías. Y, a futuro, en los posibles ciberataques con altos niveles de sofisticación que podrían generar y que podrían poner en riesgo el funcionamiento de sociedades enteras.

1.3.2.5. Buscadores De Emociones

Los buscadores de emociones fueron de los primeros actores en participar activamente en la creación de ciberamenazas a través de la historia. Son la razón por la cual se creó el término "hacker" y en los inicios del internet, su interés primordial era entender el funcionamiento de los dispositivos digitales e incrementar sus habilidades tecnológicas (Betz y Stevens 2011)

Los buscadores de emociones son personas que pretenden atacar sistemas computacionales, simplemente para probarse a sí mismos, aprender o experimentar. No están interesados en dañar los sistemas o crear consecuencias negativas significativas en las redes a las que se introducen, pero pueden provocar problemas sin darse cuenta o querer hacerlo (Sailio, Latvala, y Szanto 2020).

Este tipo de actores no suele tener altos niveles de sofisticación, puesto que suelen ser personas que están aprendiendo a utilizar herramientas digitales y no han descubierto todas las actividades que pueden realizar en el ciberespacio. Suelen utilizar herramientas ya conocidas y no poseen las habilidades suficientes para desarrollar ciberataques detallados, por lo que no son

catalogados como una ciberamenaza de alto impacto para los Estados, pero sí pueden provocar problemas a las empresas y actores no estatales (Canadian Centre for Cyber Security 2020).

Si bien, anteriormente, para aprovecharse de vulnerabilidades o penetrar las defensas de sistemas enteros se requería de mucha habilidad y conocimiento computacional, los nuevos hackers ahora pueden descargar protocolos[14] y scripts[15] desde internet y lanzar diferentes ciberataques, usualmente con intenciones de aprender su funcionamiento. La baja barrera de acceso permite que cualquier persona pueda realizarlo, por lo que el riesgo de este tipo de actores recae en que pueden producir consecuencias no esperadas o no deseadas, por el desconocimiento que tienen de los sistemas (Reveron 2012).

Los buscadores de emociones no destacan en la lista de actores participantes en ciberamenazas, pero deben de ser considerados en todo momento por las diferentes instituciones de seguridad. No sólo porque las consecuencias que pueden producir son impredecibles debido a su desconocimiento del tema, sino porque también existen hackers con mayor experiencia y conocimiento que suelen realizar ataques "por gusto". A pesar de que no buscan crear daños, el aprovechamiento de vulnerabilidades y la penetración de sistemas puede provocar que otros actores utilicen esas brechas para generar sus propios ataques, por lo que se deben de considerar como un actor participante en ciberamenazas.

1.3.2.6. Actores Internos

Los actores internos son individuos que se encuentran dentro de una organización específica y poseen las credenciales y permisos necesarios para acceder a las redes internas de sus sistemas e

[14] Un protocolo informático es una serie de reglas y formatos que determinan la manera en que se intercambian comunicaciones entre dispositivos electrónicos (Singer y Friedman 2014).

[15] Es un archivo que posee una lista de comandos o una serie de acciones que deben ser ejecutados por un programa específico (Butterfield, Ngondi, y Kerr 2016).

información confidencial. Debido a que el acceso es una de las partes esenciales para crear una ciberamenaza, este tipo de actores posee una ventaja estratégica muy importante, puesto que no necesitan utilizar otras medidas para obtenerlo. Los actores internos pueden estar relacionados con otros tipos de actores y pueden colaborar con ellos para crear ataques sofisticados, proveyendo información detallada "desde adentro", pero también pueden actuar por su cuenta motivados por razones y experiencias personales (Canadian Centre for Cyber Security 2020).

Los actores internos pueden ser clasificados en dos categorías distintas: Los "mercenarios" que buscan vender la información o el acceso a una red a otro actor para que sea utilizada a su beneficio. Y los "empleados" descontentos, que sienten que no han sido tratados adecuadamente por la institución a la que pertenecen y buscan crear problemas a la organización como medida de represalia (Sailio, Latvala, y Szanto 2020).

Los actores internos son una de las principales fuentes de información para la creación de ciberataques. No necesitan tener conocimientos ni habilidades computacionales muy desarrolladas para llevar a cabo sus actividades, puesto que el conocimiento detallado de los sistemas de sus objetivos les es suficiente para obtener acceso no restringido que puede facilitar la creación de daños o el robo de información (Reveron 2012).

Este tipo de actores suele obtener grandes ganancias económicas por la venta de la información y es difícil prevenir sus acciones, puesto que son personas que llevan un largo tiempo dentro de una organización y no se espera que actúen en contra de ella (Sailio, Latvala, y Szanto 2020).

1.3.3. Ciberamenazas estatales

Las ciberamenazas mencionadas en las secciones anteriores, así como los actores que participan en ellas, son fundamentales para explicar la manera en que acciones realizadas a través

del ciberespacio han configurado la manera de actuar de los diferentes actores internacionales. Y uno de los que tenemos que hablar necesariamente es el Estado, al continuar siendo el principal actor internacional en el Sistema Internacional.

Los Estados incursionan en el ciberespacio participando en los diferentes tipos de ciberamenazas de los que se ha hecho referencia en los fragmentos anteriores. Y se destaca que, el actuar del Estado en el ciberespacio, está fuertemente ligado a la búsqueda de sus intereses nacionales. Por lo que las operaciones que puedan realizar en este dominio, están orientadas normalmente a alcanzar objetivos que los beneficien a corto, mediano y largo plazo.

Recordemos que usualmente los ciberataques ligados a actores estatales, ya sea los que son creados por ellos o los que son dirigidos a ellos, poseen un muy alto nivel de sofisticación, al ser el actor con mayor cantidad de recursos, tanto económicos, como de personal e infraestructura. Esto quiere decir que las herramientas y programas computacionales utilizados no son tan sencillos de utilizar o crear, y el impacto de éstos puede ser mucho mayor en comparación a los creados por otro tipo de actores.

También se debe destacar, que por la cantidad de recursos que poseen, los Estados suelen tomar parte en operaciones cibernéticas de muy larga duración. Pueden llevar a cabo largas campañas de ciberataques a actores específicos por semanas, meses e incluso años, y la posible ventaja estratégica que pueden obtener de ellas, representa una suficiente justificación para asignar la cantidad de recursos requerida para realizarlas.

El ciberespacio les brinda la habilidad a los Estados de realizar acciones que en otro dominio no pueden realizar, y las características de éste, como el problema de la atribución, la dificultad de determinar la ubicación geográfica de un internauta y la falta de marcos legales que regulen las actividades en el mismo, le permiten realizar actividades que pueden ser mal vistas por la comunidad internacional.

La participación del Estado en ciberamenazas está clasificada en dos tipos, la explotación, que es el aprovechamiento de vulnerabilidades para obtener acceso a redes específicas o extraer información sensible, y la disrupción, enfocada principalmente en crear daños y perjudicar a otros actores. Ambos tipos de ciberamenazas son utilizados continuamente por actores en el Sistema Internacional, y deben ser comprendidos para entender el impacto de este tipo de ciberataques (Applegate 2015).

La participación del Estado en el ciberespacio no es nueva, y su incursión en las ciberamenazas tampoco, por lo que a continuación, se explicará, de manera más detallada, los dos tipos de actividades realizadas por el Estado para perseguir sus intereses, ya que se encuentran relacionadas al caso de NotPetya.

1.3.3.1. Explotación

Las actividades de explotación están enfocadas en el uso de la tecnología para obtener acceso a redes privadas, y se concentra en obtener información confidencial y aprovecharse de diferentes maneras de los datos recabados. Este tipo de ciberataques son invasivos, puesto que las herramientas utilizadas se mantienen por periodos prolongados dentro de los equipos afectados sin ser detectadas, y su nombre proviene de la palabra en inglés *"exploitation"* que literalmente significa "explotación" en el sentido de "aprovechamiento" o de "obtención de ventajas" (Applegate 2015).

Las ciberamenazas que abarcan las actividades de explotación no son tan variadas, pero para el Estado, la actividad de explotación más común e importante es la del ciberespionaje, de la cual se hablará a continuación (Applegate 2015).

1.3.3.1.1. Ciberespionaje

El ciberespionaje es una de las actividades más comunes en el ciberespacio, es llevado a cabo por actores estatales, al no ser sancionada a nivel internacional ni ser considerada un acto de guerra; y por actores no estatales, que reciben grandes ventajas estratégicas y comerciales. El ciberespionaje es la intrusión a las redes y sistemas rivales con el propósito de extraer información sensible, privada o protegida. En esencia, es conseguir acceso a información de un actor, sin que éste lo sepa, para utilizarla en beneficio propio, como el diseño de estrategias y la toma de decisiones (Rid 2012).

Debido a la baja barrera de acceso y el rápido desarrollo de nuevas tecnologías, la cantidad de actores involucrados en actividades de ciberespionaje es cada vez mayor. Anteriormente, sólo algunos individuos expertos en las ciencias de la computación eran los que intentaban penetrar las redes de un gobierno específico para vender su información al gobierno de otra nación, usualmente sólo motivados por las ganancias económicas que obtendrían. Pero en la actualidad, este tipo de actividades han evolucionado hasta convertirse en sofisticadas y complejas campañas, llevadas a cabo por equipos especializados que realizan ciberataques, incluso a escala industrial (Applegate 2015).

El nivel de conocimiento necesario para llevar a cabo ciberespionaje es bastante elevado, y se requiere de *software* muy sofisticado para evitar ser detectado al realizar la operación, sin embargo, los requisitos que debe cumplir la infraestructura necesaria para llevarlos a cabo no son tantos como aquellos requeridos para realizar ciberataques de disrupción. Esto es debido a que el ciberespionaje no es utilizado comúnmente para concretar fines específicos, sino que se utiliza como un instrumento para definir planes a futuro y tomar decisiones con base en la información recabada (Rid 2012).

El impacto del ciberespionaje es variado, y difícil de determinar, principalmente debido a que los actores que han sufrido de él, no comparten que información les fue robada, por lo que sólo se pueden realizar estimaciones de los daños ocasionados. Los actores no estatales, principalmente las grandes empresas, llevan a cabo espionaje corporativo para obtener ventajas estratégicas al diseñar productos y adelantarse a sus competidores. El sector privado posee la mayor cantidad de víctimas de este tipo de crimen y por lo tanto es el sector que se esfuerza más en contrarrestar este tipo de actividades. Anualmente, este tipo de actores llega a tener pérdidas millonarias por el robo de propiedad intelectual, pero el ciberespionaje de este tipo no parece disminuir (Gendron 2013).

Por otro lado, los actores estatales, más allá de valor monetario que perderían, se preocupan más por los secretos gubernamentales que sus rivales podrían obtener, particularmente por la información militar, diplomática o económica que podrían perder y que posteriormente dañaría sus capacidades de competencia y negociación ante la comunidad internacional. No obstante, el ciberespionaje es realizado activamente por diversos Estados y se mantiene como una actividad importante en divisiones del ejército de muchos países (Applegate 2015).

Un ejemplo del gran alcance que puede tener una campaña de ciberespionaje realizada por un actor estatal es el caso de "GhostNet" una operación de ciberespionaje internacional descubierta y nombrada en 2009 por un equipo de expertos de la universidad de Toronto. El equipo liderado por Ron Deibert determinó que el posible origen de la campaña era de China y que aproximadamente 1,295 computadoras de oficinas gubernamentales, embajadas, organizaciones internacionales, medios de comunicación y organismos no gubernamentales en 104 países habían sido infectadas (Rid 2012).

El programa malicioso tenía la capacidad de tomar el control total de los equipos infectados, además de buscar y recolectar documentos específicos y registrar el movimiento del mouse y teclas para el robo de contraseñas. Incluso, en algunos casos, lograba activar las cámaras y micrófonos

de los dispositivos sin el consentimiento ni el conocimiento del usuario afectado, logrando grabar y exfiltrar la información (Rid 2012).

Sin embargo, el descubrimiento del programa malicioso no fue suficiente para que sus creadores reconocieran sus acciones, e incluso, los países afectados negaron haber perdido información valiosa y no revelaron los datos perdidos. Así como en todos los aspectos de la ciberseguridad, el problema de la atribución también es destacado en el ciberespionaje, puesto que sólo se puede señalar a los posibles culpables sin realmente lograr una aceptación de culpabilidad. Además, la naturaleza secreta de la información obtenida provoca que la cooperación entre países se dificulte, puesto que, revelar la información perdida, puede provocar la pérdida de ventajas estratégicas que esa información podría brindar (Rid 2012).

A pesar de la dificultad para determinar precisamente el origen de ciberataques, existen múltiples métodos que pueden dar indicios de manera general la zona geográfica de donde surgieron, de esta forma, los gobiernos de los diferentes países señalan a los posibles culpables de generar este tipo de acciones. Asimismo, debido a sus capacidades militares y tecnológicas, además de sus intereses nacionales y sus interacciones con la comunidad internacional, se han detectado algunos Estados que llevan o han llevado a cabo campañas de ciberespionaje destacadas para perseguir sus objetivos, como lo son Estados Unidos, China, Rusia, Corea del Norte e Israel (N. Lee 2015).

La importancia del ciberespionaje recae en la facilidad que tienen los Estados de obtener la información que desean y que pueden llevar a cabo actividades de inteligencia sin la necesidad de desplegar elementos en otros territorios. El valor de la información recabada después de una operación de este tipo, no recae en la cantidad ni en el tipo de datos obtenidos, sino en lo que se realiza posteriormente con ella.

Un Estado puede definir la estrategia a seguir con otro si sabe de ante mano cuales son las capacidades de negociación que su contraparte tiene. Si la información recabada es suficiente, puede determinar las fortalezas, debilidades e intereses de un actor determinado. O incluso, si obtiene información militar, puede preparar un ataque preventivo o aumentar sus fuerzas para disuadir a su rival de atacarlo.

El ciberespionaje le brinda a un actor específico las capacidades de transformar sus acciones tomando en cuenta las ventajas o desventajas que posee con respecto a los demás, también permitiéndole modificar la manera de actuar de otros con la información recabada. De esta forma, podemos decir que el ciberespionaje incrementa las capacidades de los actores internacionales y, por lo tanto, es una fuente de poder muy destacada en la actualidad.

Posteriormente se ejemplificarán otras campañas de ciberespionaje que han trascendido en el escenario internacional y se expondrán sus consecuencias. A continuación, se abordará un tipo de ciberataque que provoca mayor caos a quien lo sufre, la disrupción.

1.3.3.2. Disrupción

Las ciberamenazas de disrupción son aquellas enfocadas en "denegar, dañar, interrumpir, o destruir los recursos informáticos y sus arquitecturas subyacentes, u otras tecnologías conectadas", principalmente para llevar actos relacionados con conflicto a través del ciberespacio (Applegate 2015, 24).

A diferencia de las ciberamenazas de explotación, la importancia de las de disrupción no recae tanto en su valor estratégico a futuro, sino en su impacto inmediato en las redes de las víctimas. Existen diversos efectos de los ataques de disrupción que pueden provocar daños importantes en los equipos afectados (Gendron 2013):

1. *Fallas por causa común*: Son efectos producidos en diversos equipos localizados dentro de una misma instalación, ocasionados por el mismo ciberataque. Por ejemplo, que todos los dispositivos en una sola estación eléctrica se vean afectados y dejen de funcionar (Gendron 2013).
2. *Fallas en cascada*: Ocurren cuando un ciberataque afecta a los sistemas de control de una instalación en específico, lo que lleva que la disrupción se expanda a una segunda o tercera instalación que dependen de la primera. Por ejemplo, la disrupción del sistema eléctrico de un país determinado, puede llevar a la falla del sistema de transporte y subsecuentemente puede generar la disrupción de la cadena de suministro nacional (Gendron 2013).
3. *Fallas en escalada*: Este tipo de efectos ocurren cuando la disrupción en una infraestructura determinada ocasiona daños severos que imposibilitan el restablecimiento de otras infraestructuras dañadas por otro tipo de ciberataques, o por las consecuencias ocasionadas por el mismo. Por ejemplo, la disrupción de los sistemas de comunicación de un país, puede llevar a la disrupción de los servicios de emergencia, que no pueden ser restablecidos hasta que los primeros logren ser reparados (Gendron 2013).

Como podemos observar, los efectos ocasionados por ciberamenazas de disrupción son importantes y pueden llegar a inhabilitar redes enteras de una infraestructura esencial de un territorio determinado, por lo que su peligro es elevado debido a los posibles daños que pueden provocar. En los últimos años han ocurrido diversos ciberataques de este tipo y sus efectos a nivel internacional han sido relevantes para los estudios de ciberseguridad.

Han impactado diversos sectores y han provocado daños importantes. Aquellos que han ocasionado disrupciones en infraestructura esencial, han generado caos y desorden social. Los

dirigidos a instituciones financieras, han provocado pérdidas económicas multimillonarias. Y aquellos ciberataques enfocados en sectores de seguridad, como el ejército, han provocado la revelación de secretos militares (N. Lee 2015).

Debido a que el objetivo principal de la disrupción es ocasionar daños en la víctima, existe una gran variedad de métodos para lograrlo, pero sin duda alguna, los ciberataques de sabotaje son de las maneras preferidas por los actores estatales para alcanzar sus objetivos. Debido a su relevancia en el caso estudiado, a continuación, se profundizará en el sabotaje.

1.3.3.2.1 Sabotaje

El sabotaje a través del ciberespacio es una de las técnicas comunes utilizadas por los Estados. Usualmente se lleva a cabo con la creación de programas maliciosos sofisticados que tienen el propósito de deteriorar los sistemas de un país específico, usualmente con la intención de crear una interrupción de los equipos afectados o generar daños significativos que alteren el correcto funcionamiento de los mismos (Sailio, Latvala, y Szanto 2020).

También podemos interpretar al sabotaje como un "intento deliberado de debilitar o destruir un sistema económico o militar", principalmente cuando existe crisis o algún conflicto entre Estados particulares. Es importante distinguir que un ciberataque de sabotaje no necesariamente genera directamente daños físicos considerables o provoca una escalada de violencia, pero debido al fuerte impacto que puede ocasionar en infraestructura esencial, lo puede llegar a desencadenar (Rid 2012).

El objetivo primordial del sabotaje es afectar a un sistema técnico para que no realice sus actividades normales o no pueda ser utilizado por la víctima (Rid 2012). Algunos Estados incluso se enfocan en la destrucción a larga escala de infraestructura esencial, cuya reparación usualmente

necesita de grandes cantidades de dinero y personal, recursos en los que en ocasiones no puede contar un gobierno de forma inmediata (Kamiński 2020).

Similar a lo sucedido con el ciberespionaje, el sabotaje tiene una naturaleza táctica, lo que significa que es una parte de una estrategia mayor aplicada en la búsqueda de intereses nacionales. Por lo tanto, el sabotaje puede no generar impactos a gran escala en los objetivos a quien se le dirige, pero sus consecuencias pueden facilitar la realización de otro tipo de operaciones (Rid 2012).

Por sí mismo, el sabotaje no es considerado un acto de guerra, puesto que no se considera como una agresión directa a un país, ni ha generado una escalada de violencia inmediata que haya llevado a la pérdida de vidas. Incluso, el sabotaje puede ser utilizado como un método para evitar que un conflicto detone, puesto que sus características facilitan que un Estado pueda utilizarlo para reducir las capacidades de otro, sin que éste se dé cuenta, orillándolo a optar por otro tipo de medidas (Rid 2012).

Como se mencionaba anteriormente, las operaciones a través del ciberespacio no son usualmente el objetivo final de un Estado, sino que funcionan como una herramienta que facilita el alcanzar otros objetivos. Lo mismo puede decirse del Sabotaje, que es un instrumento de apoyo para realizar otras actividades y perseguir intereses específicos (Rid 2012).

Los Estados con mayores capacidades y recursos son los que usualmente llevan a cabo este tipo de operaciones, que requieren de habilidades muy desarrolladas y el uso de una variedad de técnicas y recursos de inteligencia. Por lo que, aquellos Estados con mayor cantidad de recursos económicos y una rama militar y de inteligencia bien desarrollada, son los que usualmente llevan a cabo este tipo de operaciones. De esta forma, podemos destacar a países como Estados Unidos, Israel y Rusia que han llevado a cabo ciberataques de este tipo (Kamiński 2020).

Sin duda alguna, al hablar de sabotaje y de ciberseguridad, se tiene que abordar el caso de Stuxnet y la operación "*Olympic Games"* llevada a cabo por Estados Unidos e Israel. Este evento es considerado como uno de los más importantes de la ciberseguridad actual al haber sido el primer ciberataque diseñado para neutralizar componentes muy específicos de una planta nuclear. Este es uno de los ejemplos más claros de como el sabotaje puede facilitar que los Estados persigan sus intereses, pero se profundizará sobre el tema en párrafos posteriores (Kamiński 2020).

El sabotaje es una herramienta de suma eficacia para perseguir intereses particulares, los efectos radicales inmediatos que puede tener en los dispositivos de sus víctimas, sumado al factor sorpresa que este tipo de ataques suele tener, provoca que la respuesta a los mismos no sea inmediata y que los esfuerzos se enfoquen en reestablecer el funcionamiento de los equipos afectados lo más rápido posible, disponiendo de recursos adicionales para resolver la problemática.

Mientras la víctima enfoca sus esfuerzos en detener el ataque y regresar a una completa funcionalidad, desvía su atención de otras áreas, quedando expuesto a recibir otro tipo de ataques, ya sean cibernéticos o militares, por parte de sus rivales. El sabotaje resulta entonces una herramienta estratégica muy importante que puede llegar a afectar y realmente dañar las capacidades de un actor.

De esta manera, se puede decir que el sabotaje es otra fuente de poder a través del ciberespacio muy importante, puesto que transforma a corto plazo la forma de actuar de un actor específico y modifica las actividades que puede realizar.

A continuación, se detallará brevemente algunos ciberataques destacados que han ocurrido a lo largo de los años con el objetivo de ejemplificar de una manera más clara los tipos de ciberataques y el impacto que pueden tener en la comunidad internacional.

Capítulo 2. La creación de NotPetya y su difusión en Ucrania y el mundo.

En los últimos años, el número de incidentes de ciberseguridad ha aumentado considerablemente, y los sectores de los que provienen sus víctimas han sido cada vez más diversos. Se ha convertido en un importante problema de seguridad nacional, puesto que ninguna computadora se encuentra totalmente a salvo de ser infectada de algún programa malicioso, ya que éstos, no sólo poseen un mayor grado de complejidad, sino que pueden realizar sus actividades sin ser detectados, por lo que pueden ocasionar daños económicos, materiales, sociales y políticos muy importantes.

NotPetya es un ejemplo claro de cómo ha evolucionado el panorama de la ciberseguridad, tanto para el mundo de la computación, como para las Relaciones Internacionales, puesto que en cuestión de minutos se convirtió en el ciberataque con el mayor daño económico en la historia, incluso superando a WannaCry, incidente que había ocurrido tan sólo un mes antes y cuyo impacto generó pérdidas económicas importantes, que Kaspersky estima en $4 mil millones de dólares alrededor del mundo (Kaspersky Lab 2021e).

El diseño técnico del programa malicioso fue tan avanzado, que tenía la capacidad de infectar sistemas enteros en cuestión de segundos y de propagarse a otros sistemas, incluso en otros países, rápidamente, lo que desencadenó una serie de efectos indeseables en computadoras alrededor del mundo. Estas características fueron posibles debido a las herramientas que NotPetya poseía y los *exploits*[16] de los que se aprovechaba, puesto que, tras los análisis forenses, se logró determinar que sus creadores, no sólo utilizaron fragmentos de programas maliciosos destacados

[16] *Exploit* es una palabra derivada del inglés "*exploitation*" que significa explotar o aprovechar. Hace referencia a herramientas informáticas o software que es utilizado para aprovecharse de vulnerabilidades de seguridad de un equipo, programa o sistema determinado.

de ciberataques pasados, sino que los integraron, adaptaron y mejoraron, de tal manera que pudieran complementarse para lograr penetrar con facilidad una gran variedad de sistemas.

Debido al alto nivel de sofisticación y el tiempo que se requirió para crearlo, se cree que existe una alta probabilidad de que el autor de NotPetya sea un actor estatal, o un actor privado patrocinado por un Estado, ya que se necesitan de grandes cantidades de recursos económicos, personal especializado y una infraestructura avanzada y bien establecida para desarrollar un ciberataque de tal magnitud.

Además, se debe de tomar en cuenta que, a diferencia de otros ciberataques de tipo ransomware que habían sucedido con anterioridad, como WannaCry y CryptoLocker, NotPetya fue un ciberataque dirigido a un objetivo muy específico. Usualmente, los ciberataques de tipo ransomware son realizados por cibercriminales en la búsqueda de obtener la mayor cantidad de dinero posible, por lo que pretenden esparcir sus programas maliciosos a la mayor cantidad de víctimas posible, sin importar su ubicación geográfica. NotPetya no cumple esta característica, ya que fue un evento sumamente enfocado en afectar los sistemas localizados dentro del territorio de Ucrania y se cree que nunca tuvo como propósito la obtención de dinero.

Incluso, desde los inicios del ciberataque, se puede notar como el objetivo siempre fue infectar la mayor cantidad de computadoras ucranianas, ya que, el software que desencadenó las infecciones es usado por una gran cantidad de personas dentro del país. Además, la fecha elegida para iniciar el ciberataque, y la gran cantidad de víctimas en Ucrania, abarcando de oficinas gubernamentales, a grandes empresas, da indicios que el programa malicioso fue creado por un actor estatal con grandes intereses geopolíticos en la región.

Sin embargo, NotPetya no fue el único ciberataque dirigido que ha sufrido Ucrania, puesto que el país tiene una historia importante defendiéndose de ciberataques a su infraestructura esencial, destacando el caso de *Industroyer*, que provocó interrupciones a los sistemas de

distribución de energía eléctrica en 2016 y que desató una serie de apagones en el país. Por estas razones, algunos expertos han considerado a Ucrania como un "laboratorio" de ciberataques, siendo víctima de programas maliciosos innovadores, creados por algún Estado interesado en el territorio.

A pesar de que el ataque fue dirigido a Ucrania, la interconexión del mundo provocó que se detectaran infecciones de NotPetya en múltiples países, y que computadoras que no mantenían una conexión directa con equipos ucranianos, también sufrieran de los efectos del ransomware. Grandes empresas internacionales, como FedEx, Merck o la gigante naviera Maersk, destacan como los actores privados más afectados y nos demuestran como en el ciberespacio, los límites son muy fáciles de cruzar.

En este capítulo se explicarán diversos aspectos importantes de la creación, lanzamiento y difusión de NotPetya en Ucrania y el mundo. Se comenzará describiendo algunos eventos anteriores a NotPetya que se encuentran relacionados con el incidente, ya sea por las herramientas tecnológicas utilizadas, o por su relación directa con Ucrania. Posteriormente, se explicarán algunas herramientas tecnológicas implementadas en el programa malicioso que le dotaron de las características que poseía, así como las vulnerabilidades de las que se aprovechaba para cumplir sus objetivos. Después, se expondrá la manera en la que los creadores del programa malicioso lograron lanzarlo y los efectos que produjo en Ucrania, así como las primeras reacciones. Finalmente, el capítulo concluirá exponiendo la manera en que el programa malicioso alcanzó a víctimas internacionales y los efectos que produjo en otros países.

A continuación, se comenzará explicando algunos sucesos anteriores a NotPetya que son relevantes para el estudio del ciberataque y para la comprensión de las diferentes teorías sobre la identidad del autor del programa malicioso.

2.1. Ciberataques a través de la historia

Desde la normalización del uso de dispositivos digitales y la facilidad de acceso al internet, los ciberataques han incrementado en cantidad y frecuencia. Es normal encontrarse con algún titular de noticia que haga referencia a una intrusión a redes o a un hackeo a una computadora de algún mandatario. Pero los ciberataques tienen una larga historia, y su evolución a través de los años nos demuestra como su peligro se ha incrementado y que es inminente que los incidentes de gran impacto aumenten en frecuencia y cantidad de daños.

Dentro de las Relaciones Internacionales podemos destacar algunos ejemplos de ciberataques que se han originado, ya sea para dañar a actores específicos, o como una parte complementaria de operaciones militares de mayor alcance. Y la variedad de actores, estatales y no estatales, que han participado en ellos, nos muestra como en la actualidad existen las herramientas suficientes para que cualquier actor de la comunidad internacional participe en la ellos.

Los incidentes que se explican a continuación fueron seleccionados por el impacto que generaron a nivel internacional al haber ocasionado suficientes consecuencias que permitieron cambios en la dinámica entre actores internacionales. Asimismo, los programas maliciosos que fueron utilizados para llevarlos a cabo presentaron avances tecnológicos significativos, por lo que estos incidentes también significaron un cambio importante en el aspecto computacional.

Los siguientes casos serán explicados en orden cronológico, y buscan resaltar la manera en que los programas maliciosos fueron evolucionando con el paso del tiempo, hasta llegar a poseer altos niveles de sofisticación que les dotan de características peligrosas. Se puede notar que en los casos más recientes las herramientas utilizadas permitieron a sus creadores no sólo alcanzar sus

objetivos rápidamente, sino también de una manera "invisible", sin ser descubiertos o notados hasta ser demasiado tarde.

Esta cronología también funciona como apoyo para comprender los niveles de complejidad que alcanzó NotPetya debido al rápido progreso tecnológico de los últimos años y para ejemplificar que han existido otros casos en los que el uso del ciberespacio ha ocasionado impacto en las relaciones internacionales.

A continuación, se describirán brevemente algunos de los eventos ocurridos en los últimos años.

2.1.1. Gusano Morris

El 2 de noviembre de 1988, Robert Tappan Morris, estudiante de ciencias de la computación en la Universidad Cornell, lanzaba a la red el primer programa malicioso de alcance global que infamemente llevaría su nombre. Ese día, las computadoras que contaban con el sistema operativo Unix alrededor del mundo, comenzaron a alentarse y a perder funciones clave hasta detenerse por completo. Este fenómeno intrigó a los administradores de sistemas que tardaron horas en determinar el origen de las fallas y días en restaurar el funcionamiento adecuado de los equipos infectados (Orman 2003).

Morris había ocasionado el primer incidente de larga escala en la historia de la ciberseguridad, al crear un gusano informático de rápida reproducción que lograba instalarse en las computadoras conectadas a la red sin ser detectado y que se multiplicaba continuamente hasta saturar la memoria de los equipos infectados y dejarlos inutilizables. Con la intención de que su identidad no fuera descubierta, Morris lanzó el programa desde una computadora del Instituto Tecnológico de Massachusetts (MIT por sus siglas en inglés), intentando encubrir que realmente

estudiaba en Cornell, pero el gusano era tan infeccioso que rápidamente salió de la red local del MIT y se propagó a otras instituciones educativas en Estados Unidos y otros países (Orman 2003).

Los expertos no estaban preparados para combatir un incidente de este tipo, y algunos consideraban que, en ese entonces, era imposible diseñar un programa con esas capacidades. El programa era tan novedoso, que contaba con ciertas fallas que no habían sido identificadas por el mismo Morris, que provocaban que fuera muy agresivo y se multiplicara a un ritmo acelerado a través de la red. Algunos estudios indican que el gusano llegó a infectar al 10% de todas las computadoras conectadas en ese momento a ARPANET, estimadas en 60,000, la mayoría localizadas en Estados Unidos (Furnell y Spafford 2019).

Después del descubrimiento del virus, la Universidad de Cornell conformó una comisión para analizar el incidente y determinar las consecuencias que debía enfrentar Morris, acordando que el estudiante había trabajado solo y que el programa era producto de “acciones juveniles" que ignoraban los efectos que podía desencadenar. Detectaron que la única función que el programa poseía era la de replicarse a sí mismo, saturando por completo la memora de los dispositivos infectados, pero que en ningún momento modificaba, destruía o exfiltraba la información personal o los archivos de ningún usuario, por lo que su peligro radicaba en las afectaciones al funcionamiento de las computadoras, y no en la pérdida de información (Eisenberg et al. 1989).

También concluyeron que el gusano contaba con un nivel elevado de sofisticación, y que Morris probablemente había dedicado mucho tiempo en su diseño para que el gusano no fuera descubierto y que su identidad permaneciera secreta, objetivo que no logró alcanzar debido a errores en el programa, y, adicionalmente, se crearon daños en todo el sistema que Morris posiblemente no deseaba (Eisenberg et al. 1989).

La motivación que Morris tenía al crear este programa malicioso nunca ha sido revelada por el ahora profesor del MIT, pero debido a las características del programa y la falta de

intenciones destructivas, muchos expertos concuerdan que su creación fue con intenciones exploratorias. Una posibilidad es que haya deseado poner a prueba sus capacidades tecnológicas, creando un programa con características que no existían hasta ese momento, o que Morris buscaba demostrar las fallas de seguridad existentes en los sistemas operativos Unix, y la red en general, para crear consciencia de los riesgos que implicaba no darle una mayor importancia a protocolos de privacidad y protección en las computadoras personales (Furnell y Spafford 2019).

Al ser el primer incidente a través del ciberespacio en obtener la atención de los medios de comunicación, el Gusano Morris ocasionó cambios importantes en la informática y la manera en que los protocolos de seguridad eran considerados por los expertos. Si bien no se puede precisar si la intención de Morris fue exponer fallas en los sistemas de seguridad de los equipos computacionales, sin duda alguna fue una de las consecuencias más importantes de su gusano, puesto que los expertos comenzaron a prestarle mayor atención al diseño de protocolos de seguridad, e incluso, impulsó el establecimiento del primer Equipo de Respuesta a Incidentes de Seguridad en Cómputo (CERT por sus siglas en inglés) y la asignación de recursos económicos para la respuesta rápida de este tipo de eventos (Furnell y Spafford 2019; Eken 2013).

Morris se convirtió en la primera persona en enfrentar cargos por la Ley de Abuso y Fraude Informático de 1986 en Estados Unidos, después de que el Tribunal del Distrito Norte de Nueva York lo sentenciara a 3 años de libertad condicional, 400 horas de servicio comunitario y una multa de $10,050 USD por sus acciones (Daly 1993).

El Gusano Morris fue el primer ciberataque que cruzó fronteras y que generó consecuencias informáticas, legales e internacionales importantes. A pesar de que no fue diseñado específicamente para ocasionar daños, pudo generar afectaciones muy importantes a nivel global y comenzó un debate sobre la importancia de la seguridad en la computación.

2.1.2. Campañas chinas de ciberespionaje.

Como se mencionó en la sección de ciberamenazas estatales, el ciberespionaje es una de las técnicas utilizadas con mayor frecuencia por actores estatales y no estatales para alcanzar sus objetivos. Usualmente se llevan a cabo por actores que poseen una gran cantidad de recursos económicos, ya que la duración de este tipo de operaciones puede llegar a extenderse por largos periodos de tiempo.

A lo largo de la historia, diversas compañías, organizaciones e incluso gobiernos han admitido haber sido víctimas de ciberespionaje. China ha sido uno de los actores internacionales que más se ha involucrado en este tipo de actividades y su gobierno ha sido acusado a lo largo de varios años de llevar a cabo campañas de ciberespionaje con unidades especializadas de su ejército dirigidas a múltiples objetivos, que van desde empresas multinacionales como Apple y Google, hasta ramas del ejército de países como Estados Unidos y Rusia.

A continuación, se explican brevemente alguna de ellas para ejemplificar los diversos intereses que se pueden perseguir con el uso de ciberespionaje, la variedad de actores que pueden ser objetivo de este tipo de ciberataques, y la manera en que los programas maliciosos han evolucionado a través de los años hasta obtener altos niveles de complejidad:

2.1.2.1. Titan Rain

Fue una serie de ciberataques revelados por primera vez en 2005, a través de los cuales, se sospecha que el Ejército Popular de Liberación de China se infiltró en computadoras del Departamento de Defensa de los Estados Unidos y del gobierno británico (Segal 2013).

Se cree que con esta campaña de ciberespionaje, China logró acceder a información confidencial de diversas instituciones estadunidense, incluyendo el Comando de Ingeniería de Sistemas de Información del Ejército, la Agencia de Sistemas de Información de Defensa, los

Centros de Sistemas Oceánicos Navales, la Administración Nacional de Aeronáutica y el Espacio (NASA por sus siglas en inglés) e instalaciones de Defensa Estratégica y Espacial del Ejército. También lograron infiltrarse en equipos de Lockheed Martin[17], la base militar de Redstone Arsenal y el Ministerio de Relaciones Exteriores del Reino Unido. Según funcionarios del Departamento de Defensa de Estados Unidos, las infiltraciones exitosas a computadoras obtuvieron poca o nula información confidencial por lo que no existió riesgo de haber comprometido secretos relevantes del gobierno (Segal 2013).

A pesar de que la intrusión fue detectada en 2005, el gobierno estadunidense afirma que la operación podría haber empezado desde 2003, y funcionarios del gobierno británico han señalado que los últimos casos detectados de esta campaña fueron en 2007, indicando que la operación tuvo una duración de al menos cuatro años. Si bien no existieron pérdidas económicas con esta operación de ciberespionaje, existió información perdida por las víctimas de la campaña, y debido a la naturaleza confidencial de la misma, no se puede saber con precisión el tipo de datos exfiltrados, pero se puede asumir que fueron de tipo militar, diplomático y de gobierno, por las instituciones afectadas (Council on Foreign Relations 2021e).

Si bien las agencias de inteligencia de los países afectados señalaron a China como el responsable de la campaña, el gobierno chino por su parte negó todas las acusaciones y no existieron consecuencias diplomáticas relevantes tras el descubrimiento del caso. Algunos líderes de Estado solicitaron al mandatario chino detener este tipo de operaciones e instruyeron a sus respectivas agencias de inteligencia reforzar las capacidades de ciberdefensa, pero no existieron medidas coercitivas hacia la nación asiática. Incluso, Shawn Carpenter, quien detectó la intrusión

[17] Compañía estadunidense enfocada en industria aeroespacial, militar y tecnológica.

en primer lugar y rastreó su origen hasta China, fue despedido por quebrar la ley estadunidense que prohíbe el hackeo a computadoras extranjeras (Rogin 2010; Norton-Taylor 2007).

2.1.2.2. *Shady RAT*

Fue una operación de ciberespionaje descubierta por la empresa de seguridad informática McAfee, la cual le asignó el nombre de "Operación *Shady RAT"* por el acrónimo en inglés "*Remote Access Tool"*[18], que describe las herramientas informáticas utilizadas para llevar a cabo el incidente. Se estima que esta operación tuvo una duración aproximada de 4 años, de 2006 a 2010, en los que se infectaron 71 objetivos de distinta índole, como lo son la Asociación de Naciones del Sudeste Asiático (ASEAN) y el Comité Olímpico Internacional (COI), además de empresas de tecnología e información de Taiwán, Corea del Sur y Estados Unidos (Alperovitch 2011).

El objetivo de esta campaña fue obtener información confidencial, bases de datos, archivos de correo electrónico, contratos y configuraciones específicas de redes de los objetivos impactados por el virus, datos que pueden ser utilizados para realizar otro tipo de operaciones en un futuro. Asimismo, debido a las características de los objetivos impactados y la complejidad y sofisticación del software, se determinó que el autor del mismo era probablemente un actor estatal, por la cantidad de recursos necesarios para mantener una campaña de tan larga duración (Alperovitch 2011).

Además, debido a que los equipos afectados pertenecían a empresas localizadas en países con intereses políticos para el gobierno chino, y que los Juegos Olímpicos de Beijing en 2008 estaban próximos a realizarse, diversos expertos señalaron al gobierno de China como los más probables responsables de haber creado a *Shady RAT* (Segal 2013).

[18] *RAT* es un acrónimo en inglés que significa *Remote Access Tool* o Herramienta de Acceso Remoto. Es un software que le permite a un usuario acceder o controlar de manera remota otro equipo (Alperovitch 2011).

Debido a que la autoría de China no podía comprobarse, no existieron consecuencias de la operación, e incluso, algunos expertos consideran que la operación sigue en marcha en las computadoras de algunas víctimas. No se han reportado pérdidas económicas reales, puesto que se cree que la información obtenida posee únicamente un valor estratégico para toma de decisiones (Segal 2013).

2.1.2.3. *GhostNet*

GhostNet fue un programa de ciberespionaje utilizado para infiltrarse en las computadoras de individuos, organizaciones y gobiernos específicos con el objetivo de obtener información confidencial gubernamental. Se estima que al menos 1,295 computadoras en 103 países fueron infiltradas en un periodo de dos años, enfocándose principalmente en objetivos localizados en el Sudeste Asiático (Council on Foreign Relations 2021c).

El programa malicioso fue descubierto en 2009, tras una investigación de una posible infiltración en los sistemas de la oficina del Dalai Lama en India, y, el gobierno de Canadá, en conjunto con la Universidad de Toronto, rastrearon su origen a China. También se detectaron infecciones en centros de exiliados del Tíbet localizados en India, Bélgica, Reino Unido y Estados Unidos, y en embajadas y oficinas de relaciones exteriores de India, Corea del Sur, Indonesia, Rumania, Taiwán y Alemania (Segal 2013).

Un informe detallado con evidencia forense, explicando la metodología utilizada para respaldar las acusaciones de que China se encontraba detrás de la operación, fue emitido por la Universidad de Toronto, convirtiendo a GhostNet en uno de los primeros casos en los que se exhibe públicamente el análisis detallado del programa malicioso y las técnicas de rastreo, demostrando que los actores privados también poseían las capacidades suficientes para atribuir incidentes de gran importancia en los que participaban actores estatales (Council on Foreign Relations 2021c).

Si bien la Universidad de Toronto afirmó que las computadoras utilizadas para lanzar GhostNet se localizaban en el territorio chino, advirtieron que no podía afirmarse que el gobierno estaba involucrado en el caso, y que el espionaje podría haber sido realizado por individuos autónomos motivados por sus propios intereses. Al respecto, el gobierno chino aseguró que "se opone y prohíbe estrictamente cualquier delito cibernético", negando su participación en el caso. Sin embargo, no se realizaron investigaciones para capturar a los responsables del ciberataque y se desconoce a los autores del mismo (Markoff 2009).

2.1.2.3. *Aurora*

Descubierta en 2010 por Google, la Operación Aurora fue una serie de ciberataques con alto nivel de sofisticación diseñados para realizar espionaje corporativo que resultó en el robo de propiedad intelectual de múltiples empresas. Google rastreó el origen del virus hasta una computadora localizada en Shanghái, pero el gobierno chino niega haber participado en su creación. El virus fue diseñado para aprovecharse de vulnerabilidades del navegador de Microsoft, Internet Explorer, y exfiltró información confidencial de empresas como Yahoo!, Adobe, Symantec, Juniper Networks, Disney, Sony, Johnson & Johnson, General Electric, General Dynamics, King & Spalding y Google (Segal 2013).

Google fue la única compañía en confirmar el haber sido víctima del ciberataque y reveló que las cuentas de Gmail, su servicio de correo electrónico, de diversos activistas de derechos humanos en China habían sido comprometidas. También fue la única víctima en atribuir públicamente a China como el responsable del ataque, algo que otras compañías se negaron a hacer por miedo a afectar sus negocios en el mercado chino (Council on Foreign Relations 2021d).

Este caso llevó a Google a cesar sus operaciones en China, excluyendo Hong Kong, y a notificar a sus usuarios cuando alguna cuenta fuera comprometida, medida que fue implementada

también por otros servicios de correo electrónico. La Operación Aurora ha sido considerada como uno de los incidentes más relevantes en la historia de la ciberseguridad, puesto que muestra la manera en que actores privados pueden hacer uso de ciberespionaje como una herramienta para alcanzar sus objetivos. Si bien no se reportaron pérdidas económicas específicas, se cree que los secretos industriales obtenidos pudieron haber favorecido a empresas chinas en el diseño de nuevos productos para vencer a sus competidores (Council on Foreign Relations 2021d).

2.1.3. Stuxnet y la Operación Olympic Games

No se puede hablar de la historia de los ciberataques y la ciberseguridad sin tocar el tema de Stuxnet, considerado por muchos como el caso más importante y como la "primera ciber arma" utilizada en conflicto. Stuxnet revolucionó el panorama, tanto para la Informática, como para las Relaciones Internacionales, puesto que tuvo repercusiones muy relevantes en ambos campos.

Stuxnet fue descubierto el 17 de junio de 2010 y fue rápidamente catalogado como uno de los virus más peligrosos en el mundo debido al riesgo existente de provocar destrucción física en el mundo real. Se considera que fue creado como parte de una operación conjunta entre Estados Unidos e Israel denominada *Olympic Games*, cuyo propósito era sabotear las instalaciones de enriquecimiento de uranio en la ciudad de Natanz, para crear afectaciones y retrasar el programa de producción de armas nucleares de Irán (Lindsay 2013).

Stuxnet contó con un muy elevado grado de sofisticación y complejidad, pues su diseño se realizó con la intención de infectar exclusivamente a los equipos pertenecientes a la red de la planta nuclear, utilizando diferentes técnicas para que el virus llegara a los sistemas de Natanz, particularmente la infección a través de memorias USB que se conectaban directamente a las computadoras de la planta (Kushner 2013).

Cuando Stuxnet detectaba que se encontraba presente en un equipo de la planta nuclear, automáticamente descargaba una actualización de sí mismo. Posteriormente, tomaba el control de las centrífugas, y las forzaba a girar continuamente sin detenerse hasta provocar una falla en su funcionamiento. Al mismo tiempo, enviaba información falsa a los controles externos para que la avería no fuera detectada hasta que fuera muy tarde y las instalaciones quedaran inutilizables (Kushner 2013).

Stuxnet no detuvo por completo el programa nuclear de Irán, pero modificó los planes que el Estado tenía, ya que retrasó el proyecto por al menos cinco años y detuvo por completo el enriquecimiento de uranio durante un año, mientras el gobierno intentaba restaurar el funcionamiento de las instalaciones (Lindsay 2013).

Si bien ninguno de los actores señalados como responsables del programa malicioso ha aceptado oficialmente su participación en el caso, las características del evento y los sucesos ocurridos indican que seguramente Stuxnet fue creado por actores estatales. Y, si se acepta la teoría de que Estados Unidos e Israel se encontraron detrás del ciberataque, el caso es un ejemplo muy claro de como el ciberespacio puede ocasionar consecuencias en el mundo "real" a partir de lo que ocurren en el mundo "virtual".

Stuxnet cambió la forma en que los expertos en ciencias de la computación percibían los ciberataques y causó que se considerara la posibilidad de que surgieran daños físicos a través de nuevos y más complejos programas maliciosos. Anteriormente, la mayoría de los expertos descartaba la posibilidad de que una ciberguerra pudiera ocurrir y consideraban que existía una baja probabilidad de que se pudieran perder vidas a través de ciberataques. Stuxnet transformó ese panorama, y ahora existe una mayor atención a las vulnerabilidades presentes en infraestructura esencial que pueden ser aprovechadas para desencadenar consecuencias severas en países enteros. Incluso, algunos teóricos señalan la posibilidad de que exista un "Ciber-Pearl Harbor", un

ciberataque de gran magnitud dirigido a Estados Unidos, o cualquier potencia con las capacidades necesarias, que genere suficientes daños para que este país entre en conflicto y que los ciberataques comiencen a ser más dañinos.

En el campo de las Relaciones Internacionales, Stuxnet también fue un evento que transformó la visión de los teóricos, puesto que demostró que el ciberespacio era ya una nueva área en la que podían interactuar los Estados y todos los actores internacionales que tenían presencia en él. También se puede observar la manera en que los actores estatales han generado nuevas capacidades que les permiten realizar actividades que anteriormente no podían llevar a cabo, y que estas capacidades se ven traducidas en nuevas expresiones de poder que modifican la manera de actuar de otros actores.

2.1.4. Duqu y Duqu 2.0

Una de las características más relevantes en la informática, es que los programas se encuentran en constante actualización y evolución, por lo que continuamente se lanzan versiones de programas con características novedosas que les dotan de funciones innovadoras. Esto sucede también con los programas maliciosos, provocando que uno de los retos más importantes para la ciberseguridad sea el mantener en constante actualización los equipos que son potenciales víctimas de ciberataques.

Este fenómeno se puede observar en los casos de Duqu, y su versión posterior, Duqu 2.0, los cuales son versiones renovadas y con nuevas características de Stuxnet. Duqu es un programa malicioso detectado por primera vez en septiembre de 2011, debido a una investigación de un posible incidente de seguridad en el departamento de Tecnologías de la Información de una empresa europea. Su nombre se origina debido a que los archivos utilizados para llevar a cabo el ciberataque poseían la terminación ".DQ" (Bencsáth et al. 2012).

Tras el análisis forense de las computadoras infectadas y observar el comportamiento del programa malicioso, se notaron múltiples similitudes con Stuxnet, particularmente que ambos poseían una estructura modular, que se podían configurar de manera remota y que estaba diseñado para infiltrarse en equipo industrial. Sin embargo, Duqu poseía una diferencia muy importante: No estaba diseñado para sabotear, sino para robar información confidencial (Bencsáth et al. 2012).

Se determinó que Duqu probablemente había sido diseñado y lanzado por el mismo equipo que creó Stuxnet, considerando al Estado de Israel como el principal sospechoso. Las víctimas del programa malicioso se encontraron en diversos países, pero principalmente en aquellos en los que Israel tiene intereses geopolíticos particulares, como Irán y Sudán, y la información exfiltrada de los equipos fue principalmente de instituciones militares y de gobierno, lo que propicia a sospechar de un actor estatal (Council on Foreign Relations 2021b; Gibbs 2015).

Duqu fue una versión mejorada y readaptada de Stuxnet para cumplir nuevos intereses nacionales. Sin embargo, no fue su única versión, pues unos años después surgiría Duqu 2.0, un programa malicioso detectado por primera vez en 2015 por Kaspersky Lab, ya que se intentó realizar una intrusión a sus sistemas de seguridad informática con este virus. Así como el primer Duqu, Duqu 2.0 tenía características muy similares a Stuxnet, pero fue modificado para no ser detectado por un periodo de tiempo muy extenso y para exfiltrar información confidencial particular (Bencsáth et al. 2011).

Se creía que, tras el primer Duqu, el grupo detrás del programa había detenido sus operaciones en 2012, pero después de la detección por Kaspersky, se realizó una investigación detallada del programa malicioso y se descubrió que poseían el mismo origen. Además de Kaspersky Lab, se detectaron infecciones de Duqu 2.0 en computadoras localizadas en diferentes países del Sudeste Asiático. Sin embargo, las intrusiones que resaltaron en mayor medida fueron las detectadas entre 2014 y 2015, particularmente en computadoras localizadas dentro de las

instalaciones utilizadas para reuniones del grupo P5+1[19] sobre las negociaciones del tratado nuclear de Irán. También se detectaron intrusiones en computadoras relacionadas al setenta aniversario de la liberación de Auschwitz-Birkenau, por lo que Kaspersky afirmó que el programa malicioso fue diseñado con objetivos geopolíticos muy claros (Kaspersky Lab 2015a, 2015b).

Duqu 2.0 infectó los sistemas de al menos tres hoteles en los que se llevaron a cabo reuniones del P5+1 con Irán sobre el tratado nuclear, y podía exfiltrar información confidencial a través de diferentes métodos. El virus, logró obtener acceso a los canales de video de los circuitos cerrados de las cámaras de seguridad de los hoteles, intervino los teléfonos celulares de los funcionarios participantes a través de las redes Wifi y controló micrófonos, cámaras, elevadores y sistemas de alarma de los hoteles. El programa malicioso también fue detectado en las recepciones de los hoteles, por lo que la información de las habitaciones en donde se hospedaban los delegados fue obtenida con facilidad. Duqu 2.0 podía controlar por completo lo que sucedía en los hoteles y tenía acceso total a las conversaciones y procesos de negociación que se llevaba a cabo en ellos (Entous y Yadron 2015).

Aunque Kaspersky no declaró explícitamente quién podría estar detrás de Duqu 2.0, sí consideró que habían sido los mismos creadores del primer Duqu y de Stuxnet, y tomó en cuenta que diversos funcionarios del gobierno de Estados Unidos habían sido informados por agentes de contra inteligencia que sus conversaciones podrían ser escuchadas por el gobierno israelí. Asimismo, en marzo de 2015, funcionarios del gobierno americano informaron que habían recibido información de que Israel planeaba realizar una operación de espionaje, esto tras haber colaborado en establecer una línea de comunicación secreta con Teherán en 2012 (Gibbs 2015).

[19] Es un grupo conformado por los cinco miembros permanentes del Consejo de Seguridad de la Organización de Naciones Unidas (Estados Unidos, China, Rusia, Reino Unido y Francia) y Alemania. Se integró el grupo para llevar a cabo negociaciones diplomáticas con Irán acerca de su programa nuclear y para llegar a un acuerdo.

Duqu 2.0 se diferencia de otras campañas de ciberespionaje en su duración, puesto que, en lugar de haber sido una operación de varios años, se concentró en obtener información confidencial de lugares y momentos muy específicos gracias a su alto nivel de sofisticación. Este caso ejemplifica el uso de ciberespionaje como una herramienta de gran valor en la actualidad, puesto que no sólo recabó mucha información de reuniones secretas, sino que le facilitó al Estado de Israel diseñar sus estrategias futuras con respecto a una de las potencias regionales principales, Irán.

A continuación, se presentará en una tabla los casos mencionados anteriormente para visualizar de una mejor manera las características de cada uno de ellos:

Tabla 2.

Evolución de los incidentes de ciberseguridad de impacto internacional.

Nombre	Año	Víctimas	Autor	Propósito	Consecuencias
Gusano Morris	1988	Red global de ARPANET	Robert Tappan Morris	Exploratorio	Creación del primer Equipo de Respuesta a Emergencias Informáticas. Primer juicio por la Ley de Abuso y Fraude Informático de 1986
Tiran Rain	2005	Lockheed Martin, Departamentos Gubernamentales de EUA, Ministerio de Relaciones Exteriores de Reino Unido	Probablemente China	Espionaje	Despido de quien rastreó la campaña. Solicitudes a China por parte de diversos mandatarios de detener las actividades.
ShadyRAT	2006	ASEAN, COI y empresas de tecnología	Probablemente China	Espionaje	Escándalo internacional sin repercusiones políticas o económicas relevantes.
GhostNet	2009	Oficinas del Dalai Lama y centro de exiliados del Tíbet en Asia y Europa.	Probablemente China	Espionaje	El caso fue condenado por el gobierno chino, pero no se realizaron investigaciones para determinar el origen del ciberataque.
Aurora	2010	Google, Microsoft, Yahoo!, Adobe, Symantec, Johnson & Johnson, Disney, Sony, entre otras empresas.	Probablemente China	Espionaje	Exfiltración de secretos empresariales y diseños de productos para favorecer empresas chinas en el mercado. Se comprometieron cuentas de correo electrónico de activistas. Google cesó su actividad en China.
Stuxnet	2010	Instalaciones de enriquecimiento de uranio de Natanz, Irán.	Probablemente Estados Unidos e	Sabotaje	Daños a las centrífugas de enriquecimiento de uranio, retrasando el programa nuclear de Irán.
Duqu	2011	Equipos industriales principalmente en Irán y Sudán.	Probablemente Israel	Espionaje	Exfiltración de información militar confidencial
Duqu 2.0	2015	Hoteles en donde se realizaron las reuniones del P5+1 con Irán.	Probablemente Israel	Espionaje	Exfiltración de información diplomática confidencial.

Los programas maliciosos utilizados en incidentes de ciberseguridad internacional han evolucionado hasta ser sumamente complejos. Con el paso del tiempo, surge nueva tecnología, que les brinda nuevas funciones, y a su vez, mayores niveles de sofisticación, aumentando la preocupación de las consecuencias que puedan ocasionar. *Tabla de elaboración propia.*

2.2. Antecedentes de NotPetya

Antes de explicar el lanzamiento de NotPetya y su rápida infección en computadoras ucranianas, es necesario exponer algunos eventos anteriores que influenciaron el desarrollo del programa malicioso. A continuación, se expondrán de manera cronológica esta serie de eventos para comprender de mejor manera el desarrollo y lanzamiento de NotPetya.

2.2.1. BlackEnergy

En diciembre de 2015, diversas estaciones eléctricas localizadas al oeste de Ucrania sufrieron un ciberataque que provocó un corte de energía a más de 230,000 habitantes de la región por hasta seis horas. Diversos centros de comando de Prikarpattiaoblenergo, la compañía de electricidad, fueron atacados simultáneamente hasta que los autores del ciberataque obtuvieron acceso a la red de la región de Ivano-Frankovsk para desactivarla y ocasionar los apagones (Council on Foreign Relations 2021a).

Además, durante el incidente, las líneas telefónicas de atención al cliente de Prikarpattiaoblenergo fueron saturadas intencionalmente por los autores del ciberataque con miles de llamadas con la intención de evitar que los clientes reportaran las fallas y el ciberataque se prolongara el mayor tiempo posible (Council on Foreign Relations 2021a).

Este incidente se llevó a cabo con el uso de un programa malicioso denominado *BlackEnergy*[20], el cual es un troyano utilizado con diferentes objetivos, desde el lanzamiento de ataques DDoS y ciberespionaje, hasta operaciones de sabotaje, como en este caso. La distribución de este programa malicioso comenzó, en un inicio, con el envío masivo de correos electrónicos que

[20] *BlackEnergy* podría ser traducido al español literalmente como “EnergíaNegra”

poseían documentos de Excel diseñados para ocasionar la infección de manera disimulada (Kaspersky Lab 2021a).

La gran mayoría de infecciones fueron detectadas en Ucrania, dirigidas específicamente a equipos industriales pertenecientes a los sectores de energía, gobierno y medios de comunicación. Los apagones de 2015 fueron la culminación de una serie de ciberataques dirigidos a los sistemas de distribución eléctrica, que Ucrania había sufrido a lo largo del año. Los efectos ocasionados hicieron que BlackEnergy se convirtiera en el primer caso en el que un programa malicioso desactivaba la red eléctrica de un país con éxito, convirtiéndose en un parteaguas de incidentes posteriores (Council on Foreign Relations 2021a; Kaspersky Lab 2021a).

Debido a que el ciberataque fue dirigido específicamente a Ucrania y a su infraestructura esencial, se ha asumido que existe un actor estatal detrás de él, la mayoría de expertos señalando a Rusia como el probable responsable debido a la escalada de tensiones entre ambos países desde el conflicto iniciado por la anexión de Crimea en 2014. Se considera que el creador de este, y de varios ciberataques de los que ha sufrido Ucrania en los últimos años, es un grupo denominado "*Sandworm",* un grupo de hackers que se cree pertenecen a las fuerzas especiales de inteligencia de Rusia (Council on Foreign Relations 2021a; Greenberg 2019).

La respuesta al ciberataque fue inmediata, y los miembros del CERT de Ucrania trabajaron rápidamente en colaboración con la empresa de energía eléctrica para restaurar los servicios. La empresa afirmó que revisaría sus protocolos de seguridad y los reforzaría para evitar una nueva intrusión. El gobierno de Ucrania denunció el ataque y señaló a Rusia como el principal sospechoso, mientras que el gobierno estadunidense apoyó esta postura (Polityuk 2016; Council on Foreign Relations 2021a).

Este incidente destaca, porque demuestra la sofisticación que han alcanzado los programas maliciosos al haber sido el primer caso de sabotaje de una red eléctrica con éxito. Si bien la

compañía eléctrica y el gobierno aseguraron que trabajarían para evitar casos posteriores, éste no fue el único incidente y Ucrania sufrió un segundo ciberataque que desencadenaría en apagones un año después, del cual se hablará posteriormente.

2.2.2. Petya

Para poder explicar los sucesos de NotPetya, es necesario exponer lo que ocurrió con Petya, la versión "original" del programa malicioso. Petya es una familia de *ransomware* diseñados para la encriptación de archivos descubierta por primera vez a principios de 2016. Este tipo de programas maliciosos fueron diseñados para infectar específicamente a los equipos que cuentan con el sistema operativo Microsoft Windows (Mohammad 2020).

Petya encriptaba la Tabla Maestra de Archivos[21] del disco duro de la computadora infectada, lo que significaba que no modificaba los archivos dentro de una computadora, sólo provocaba que el equipo fuera incapaz de encontrarlos, y, por lo tanto, también de mostrarlos. El *ransomware* poseía diversas fallas, por lo que fue fácil de contrarrestar y no fue difundido a tan gran escala como su versión más sofisticada (Mansfield-Devine 2016).

Las víctimas principales del programa malicioso fueron las computadoras de los departamentos de recursos humanos de múltiples empresas, localizadas principalmente en Alemania. Las víctimas recibían un correo electrónico de phishing[22] proveniente de un presunto aplicante a un puesto laboral. El correo no presentaba ninguna señal de que fuera falso, puesto que poseía una excelente redacción y, a simple vista, parecía ser una solicitud normal. Sin embargo, el supuesto aspirante no enviaba los archivos necesarios para la aplicación de trabajo como

[21] La Tabla Maestra de Archivos es una base de datos en la que se almacena la información de cada uno de los archivos de un directorio (IDERA Inc 2021).

[22] Es un término conformado por un juego de palabras en inglés, en el que intencionalmente se deletrea erróneamente la palabra "*fishing*", que en español es pescar. Es un tipo de cibercrimen cuyo propósito es el robo de información confidencial de una computadora a través de técnicas de ingeniería social, por ejemplo, la suplantación de identidad (Kaspersky Lab 2021c).

documento adjunto al correo, sino que incluía una liga a una carpeta del sitio web dedicado al almacenamiento de archivos en la nube, Dropbox, titulada “Solicitud de Empleo”, la cual era descargada por el personal de recursos humanos sin sospechar que al hacerlo, Petya automáticamente comenzaba a tomar control del equipo (Bilić 2016).

Después de enterarse del método de infección, Dropbox detectó y eliminó todos los archivos infectados con Petya para detener la propagación del virus, y el usuario de GitHub[23], leostone, compartió una herramienta gratuita que generaba claves que podían ser utilizadas para desencriptar los archivos que habían sido dañados por Petya para la recuperación de los equipos fuera rápida (Bilić 2016).

Se cree que Petya fue creado originalmente por un hacker, o grupo de hackers, autodenominados *Janus Cybercrime Solutions*, quienes utilizaron su programa con intenciones de obtener ganancias económicas. Una característica que llama la atención es, que tanto el nombre del autor, como el de los programas maliciosos que ha creado, incluyendo Petya, hacen referencias a la película de 1996 de la saga de James Bond, *GoldenEye*[24]. Se desconoce la o las identidades de *Janus Cybercrime Solutions*, y, debido a que sus víctimas pertenecen al sector privado y no poseen tanto poder ni recursos económicos, no se han realizado los esfuerzos necesarios para determinar su identidad o localización (Malwarebytes Labs 2017).

2.2.3. Industroyer/Crashoverride

El 17 de diciembre de 2016, la planta eléctrica de Ukrenergo localizada cerca de Kiev reportó diversas fallas que dejaron sin electricidad a la capital ucraniana por al menos una hora. A

[23] GitHub es un sitio de internet dirigido a desarrolladores para compartir herramientas y software.

[24] "Janus" hace referencia a un sindicato que juega el papel antagónico en la película. "Petya" es el nombre de una de las armas, importante para la trama. Inclusive, el programa malicioso Petya tuvo un nombre alternativo, "GoldenEye", haciendo referencia directa a la película.

pesar de que la energía eléctrica se restauró rápidamente y no surgieron problemas de gravedad, las autoridades locales confirmaron que el incidente había sido ocasionado por un ciberataque. Ese mismo día, investigadores de seguridad informática detectaron y analizaron un nuevo programa malicioso, el cual se cree fue el causante de los cortes de suministro eléctrico en la capital ucraniana. Tras diversos estudios, se determinó que era un programa sumamente sofisticado, y se catalogó rápidamente como la mayor amenaza existente hacia Sistemas de Control Industrial desde el lanzamiento de Stuxnet, seis años atrás (ESET 2017).

Dos compañías de seguridad informática fueron las principales instituciones que participaron en el análisis del programa malicioso. Ambas compañías emitieron reportes independientes mostrando el resultado de sus investigaciones y asignándole nombres distintos al mismo programa malicioso. ESET, la empresa eslovaca establecida en Bratislava, le asignó el nombre *Win32/Industroyer*, aunque comúnmente se utiliza simplemente el nombre *Industroyer* para identificarlo (ESET 2017). Por otro lado, Dragos Inc., la empresa estadunidense, nombró al programa malicioso *Crashoverride* haciendo referencia al efecto que producía en los equipos infectados. A pesar de poseer dos nombres distintos, ambos describen al mismo programa malicioso causante de los apagones en Ucrania (Slowik 2019). Para fines prácticos y evitar confusiones, se utilizará el nombre *Industroyer* a lo largo de esta investigación para hacer referencia a este programa malicioso.

Tras el análisis de las compañías de seguridad informática, se descubrió que Industroyer era un programa malicioso diseñado para generar disrupción en procesos industriales y equipo físico mediante la infección de Sistemas de Control Industrial, que no necesariamente pertenecían a alguna marca, modelo o configuración en específico. Esta característica le permitía ser adaptado y reconfigurado para afectar cualquier tipo de infraestructura localizada en Europa, Medio Oriente, Asia e incluso Norteamérica, por lo que se creyó que el programa había sido diseñado para ser

reutilizado y relanzado en diversas ubicaciones, de acuerdo al objetivo que se buscara alcanzar (Bindra 2017).

El peligro de Industroyer radica en las herramientas avanzadas con las que cuenta, puesto que permiten a sus creadores tomar el control de los interruptores de subestaciones eléctricas directamente. Para lograr su objetivo, el programa utilizaba protocolos de comunicación industrial utilizados comúnmente alrededor del mundo en instalaciones de infraestructura esencial diversa, que van desde redes de suministro de energía eléctrica, gas y agua, hasta sistemas de control de transporte, otorgándole la habilidad de controlar o desactivar cualquiera de este tipo de instalaciones (Cherepanov 2017).

Si bien los efectos provocados por este incidente fueron menores que los ocasionados un año antes por BlackEnergy, se considera a Industroyer como una mayor amenaza por su sofisticación y por su amplia posibilidad de personalización y adaptabilidad. Como consecuencia principal de haber sido impactados por un ciberataque de tal magnitud, Ukrenergo desarrolló una reforma enfocada en la renovación y reestructuración de su infraestructura y seguridad informática. También creó un CERT propio para actuar con mayor rapidez en caso de ser impactados nuevamente por un ciberataque (Haji 2021).

Tras el análisis del programa malicioso y debido a sus similitudes con los sucesos ocurridos un año antes, tanto Dragos Inc., como ESET, atribuyen el incidente a *Sandworm*, o a un equipo estrechamente relacionado con ellos. En esta ocasión no hubo una declaración oficial del gobierno ucraniano señalando a Rusia, sino que fueron las compañías de seguridad informática y la misma Ukrenergo que reconocieron la probable participación rusa en el incidente (Haji 2021; Greenberg 2019).

2.2.4. The Shadow Brokers

Para comprender completamente el lanzamiento de NotPetya, es necesario entender la manera en que uno de los *exploits* utilizados para su creación, EternalBlue, surgió, ya que, a diferencia de otros programas maliciosos cuya procedencia es desconocida o debatible, en este caso se pudo confirmar que EternalBlue fue obtenido debido a brechas en la seguridad de uno de los departamentos de inteligencia con mayor actividad: La Agencia Nacional de Seguridad de los Estados Unidos (NSA por sus siglas en inglés).

Para poder relatar la manera en que la exfiltración de la información ocurrió es necesario, en primer lugar, explicar quiénes son *The Shadow Brokers* y cuáles son sus actividades. *The Shadow Brokers*[25] (TSB) son un grupo de *hackers* conocidos popularmente por obtener exploits de *software*, detectar vulnerabilidades en programas de uso común y exfiltrar información sensible de la NSA para posteriormente divulgar toda la información en línea a cambio de un pago. Las herramientas compartidas por TSB han sido incorporadas en incidentes de ransomware relevantes, resaltando WannaCry y NotPetya, por lo que representan una importante amenaza para la ciberseguridad (Seung, Kwanwoo, y Shin 2018).

Se desconoce la fecha en que TSB inició sus operaciones, pero comenzó a llamar la atención de los expertos en 2016, tras una serie de tweets publicados a través de la cuenta con nombre de usuario "@shadowbrokerss". En uno de ellos aparecía una liga que llevaba al sitio web Pastebin, una página comúnmente utilizada para publicar anónimamente herramientas de hackeo, en donde se pudo encontrar un mensaje, en un inglés deficiente, dirigido a los "patrocinadores gubernamentales de la ciberguerra", preguntándoles el precio que pagarían por "ciberarmas de los enemigos" (Greenberg 2019, 168).

[25] *The Shadow Brokers* puede ser traducido al español como "Los Corredores de Sombras".

El grupo afirmaba que habían logrado infiltrarse en la NSA y hackear a Equation Group[26], por lo que habían obtenido una serie de archivos confidenciales y herramientas altamente sofisticadas que venderían al mejor postor. Señalaron que toda persona que deseara obtener acceso a los archivos debía enviar sumas importantes de dinero en Bitcoin, las cuales no serían devueltas, y que sólo la transferencia mayor sería la que podría recibir las herramientas. También agregaron que, si la recolección de fondos superaba el millón de Bitcoins, los archivos serían compartidos al público de forma gratuita, para que todo el mundo pudiera utilizar las herramientas en la creación de nuevos programas maliciosos (Greenberg 2019).

La lista de archivos publicada por TSB fue analizada por expertos y afirmaron, particularmente algunos ex trabajadores de la NSA, que eran herramientas reales, muy sofisticadas y peligrosas, por lo que su difusión al público general era un riesgo muy grande para la ciberseguridad internacional. Algunas tenían las capacidades de monitorear y modificar el flujo del tráfico dentro de las ciudades, y otras podían tomar el control de equipos industriales de Cisco[27], una de las empresas dedicadas a la venta y mantenimiento de equipos computacionales y dispositivos digitales más grande del mundo (Greenberg 2019).

TSB no obtuvo el millón de Bitcoins que deseaba, y 24 horas después de su publicación obtuvieron tan sólo $937.15 USD. Sin embargo, expertos creen que la recolección de dinero fue una estrategia para dar falsas señales de que eran un grupo cibercriminal y encubrir que realmente eran un grupo patrocinado por un Estado con el objetivo específico de atacar a la NSA. Sus estrategias para compartir las herramientas que obtenían, se fueron transformando con el paso del

[26] Equation Group es un nombre asignado por la compañía de seguridad informática, Kaspersky Lab, al grupo estadunidense que participó en la creación de Stuxnet.

[27] Al enterarse de la situación, Cisco alertó a sus clientes e inmediatamente comenzó el cambio de dispositivos que podían ser afectados por alguna de las herramientas divulgadas por TSB, puesto que estaban conscientes que eran fallas muy difíciles de reparar y en caso de un ciberataque, se podía perder el control total de los equipos (Greenberg 2019).

tiempo, intentando crear un sistema de suscripción mensual o incluso vender herramientas específicas bajo demanda, pero a finales de 2016, su actividad se redujo considerablemente y por meses no dieron señales de actividad alguna, haciéndole creer a los expertos que el grupo había desaparecido (Greenberg 2019).

En abril de 2017, después de 4 meses sin actividad, TSB apareció nuevamente y publicaron una contraseña de 32 caracteres que podía ser utilizada para desbloquear su primera publicación, realizada un año antes. Al desencriptar los archivos se encontró una colección de herramientas para poder aprovecharse de vulnerabilidades de dispositivos que funcionaban con los sistemas de Linux, Unix y Solaris (Greenberg 2019).

Una semana después, el 14 de abril, volvieron a aparecer compartiendo una nueva serie de herramientas, incluyendo aquella llamada por la NSA "EternalBlue". Esto causó conmoción en expertos de ciberseguridad que reconocieron la herramienta y comprendían su funcionamiento, ya que podía ser utilizada para aprovecharse de una vulnerabilidad de día cero existente en todas las versiones anteriores a Windows 8, por lo que se podían crear programas maliciosos altamente sofisticados y difíciles de contrarrestar (Greenberg 2019).

Así como los expertos lo sospechaban, EternalBlue fue utilizado para crear WannaCry y NotPetya, pero debido a un artículo publicado en *The Washington Post*, se descubrió que EternalBlue no era una vulnerabilidad de día cero totalmente, ya que la NSA alertó a Microsoft de su existencia de manera secreta, y reconoció que la había detectado tiempo atrás pero que no quería divulgar la información para poder ser utilizada en favor de Estados Unidos. Tras la alerta, un mes antes de WannaCry, Microsoft lanzó parches de actualización de emergencia a los equipos que contaban con esa vulnerabilidad, pero debido a que la mayoría de usuarios no descargó el parche, los equipos se mantuvieron expuestos (Greenberg 2019).

Desde la publicación de EternalBlue, TSB no ha vuelto a compartir herramientas, pero no se descarta que el grupo continúe trabajando. Algunos expertos señalan a Rusia como el Estado que patrocina al grupo de hackers con el objetivo de perseguir sus intereses, mientras que otros argumentan que se trata de uno, o varios empleados, de la NSA que publican contenido de la agencia por venganza, inconformidad o ganancia económica. Si bien ninguna teoría se ha logrado confirmar, no se puede negar que TSB sigue siendo un grupo que representa un serio peligro a la integridad de los sistemas computacionales mundiales.

2.2.5. WannaCry

WannaCry es el nombre de un programa malicioso de tipo ransomware, que bloquea los archivos dentro de una computadora y niega el acceso a sus usuarios, forzándolos a pagar una cantidad de dinero a cambio de la llave digital que desbloquea sus equipos. Fue lanzado el 12 de mayo de 2017 y, en su momento, era considerado el peor ciberataque de la historia por los severos daños económicos que provocó (Mohurle y Patil 2017).

WannaCry se propagó a una gran velocidad y llego a infectar más de 200,000 computadoras en 150 países alrededor del mundo, por lo que es considerado uno de los ciberataques de mayor magnitud de la historia. Sus víctimas principales fueron personas que poseían equipos con alguna versión desactualizada de Microsoft Windows, debido a que no contaba con los parches adecuados para corregir una serie de severas vulnerabilidades que exponían gravemente la seguridad de los archivos de los usuarios (Ehrenfeld 2017).

Las víctimas no podían visualizar sus archivos, puesto que WannaCry los ocultaba a través de complejas técnicas de encriptación, ocasionando que los equipos quedaran inutilizables. Los usuarios sólo tenían acceso a dos archivos, el primero contenía las instrucciones que debían ser

seguidas para recuperar el control del dispositivo, junto con la leyenda "*Wanna Cry?*"[28]; y el segundo, la herramienta de desencriptación, que sólo podía ser activada con una clave específica, obtenida únicamente tras haber realizado el pago del rescate (Mohurle y Patil 2017).

WannaCry fue diseñado con diferentes exploits, que le permitían acceder y encriptar rápidamente la información de sus víctimas. Se debe destacar el caso de "EternalBlue"[29], debido a lo mencionado anteriormente, la NSA decidió ocultar la información a Microsoft para utilizarla en favor de Estados Unidos. Este exploit resalta también porque fue utilizado para la creación de NotPetya, e incluso algunas teorías señalan que WannaCry fue una prueba para observar lo que EternalBlue podía provocar, incentivando a los creadores del programa malicioso a utilizarlo en el diseño de NotPetya (D. Lee 2019).

Como se ha mencionado anteriormente, WannaCry generó daños económicos destacados, ya que impactó a una gran cantidad de computadoras alrededor del mundo, afectando directamente el correcto funcionamiento de equipos esenciales en las actividades de diversas instituciones. A continuación, se describen algunos efectos provocados en las víctimas principales de WannaCry:

El Servicio Nacional de Salud del Reino Unido (NHS por sus siglas en inglés) fue uno de los más afectados por WannaCry, pues se esparció a los dispositivos de clínicas y hospitales en todo el Reino Unido. Provocó que computadoras, escáneres de resonancia magnética, refrigeradores de almacenamiento de sangre y equipo de quirófanos dejaran de funcionar correctamente. En algunas regiones, sólo funcionaron las salas de urgencia y se detuvieron operaciones en otros tipos de servicio. El NHS tardó días en restablecer operaciones normales y

[28] "*Wanna Cry?"* significa literalmente "¿Quieres llorar?" en español. La frase hacía burla a sus víctimas señalándolas de querer llorar por haber perdido sus documentos. También fue la razón por la que se asignó el nombre a este programa.

[29] Exploit descubierto por la NSA para aprovecharse de vulnerabilidades de Microsoft. En español significaría literalmente "AzulEterno". Se ha descubierto su uso en múltiples ciberataques.

meses en recuperar la información perdida de sus pacientes, y en algunos casos, los expedientes no pudieron ser recuperados y los perfiles tuvieron que ser reconstruidos por completo (Ehrenfeld 2017).

En India, los departamentos de policía fueron los más afectados, principalmente los localizados en el estado de Andhra Pradesh. Se estima que 18 sistemas fueron deshabilitados por WannaCry. El gobierno indio aseguró que no se perdió información confidencial y que las afectaciones fueron principalmente operacionales (BBC News 2017b).

Empresas privadas multinacionales también se vieron impactadas por el programa malicioso, como Nissan y Renault, que detuvieron sus operaciones en fábricas localizadas en Reino Unido, Francia, Eslovenia, Rumania e India. Ambas compañías reportaron daños económicos significativos, pero lograron la restauración inmediata de los equipos infectados por WannaCry (Frost y Tajitsu 2017).

En China, miles de casos fueron detectados, tanto en el sector público, como en el privado. La Corporación Nacional de Petróleo de China (CNPC) tuvo que detener sus actividades, puesto que el sistema para procesar pagos con tarjeta fue afectado por WannaCry, generando una saturación en estaciones de servicio y embotellamientos por las largas filas de automóviles que esperaban solucionar sus problemas de cobro. En universidades públicas, las computadoras de los estudiantes fueron las más afectadas, y, debido a que el ciberataque sucedió durante un periodo de evaluaciones, un gran número de estudiantes pagó el rescate de sus documentos. Se estima que 30,000 instituciones y compañías en china, así como agencias gubernamentales y hospitales fueron las afectadas por el ransomware (BBC News 2017b).

Como se puede observar en los párrafos anteriores, las víctimas del ransomware provenían de una gran diversidad de sectores y se localizaban en diferentes países alrededor del mundo. También se pueden destacar los casos de la empresa española de telecomunicaciones, Telefónica,

que sufrió afectaciones en sus servicios por WannaCry, así como el banco ruso Sberbank, y la compañía alemana de trenes Deutsche Bahn, que tuvieron que modificar sus actividades por el ransomware (Greenberg 2019).

A pesar de la complejidad de WannaCry y el uso de diversos programas sofisticados para encriptar información, la solución al ciberataque fue más sencilla de lo que se esperaba. Marcus Hutchins, investigador de seguridad informática británico, logró determinar que antes de encriptar los documentos de sus víctimas, WannaCry intentaba comunicarse con un sitio de internet específico[30]. Si el programa malicioso no lograba conectarse con el sitio, comenzaba la encriptación de los documentos. Esto significaba que era una medida que utilizaba el programa para detectar si se encontraba en una computadora real, o una virtual[31]. Si WannaCry lograba conectarse a internet, la encriptación no sucedía, por lo que, tras darse cuenta que el sitio no le pertenecía a nadie, Hutchins lo compró por $10.69 USD (Greenberg 2019).

Tras haber adquirido la página web, Hutchins comenzó a notar los miles de conexiones que comenzaron a surgir de diversas partes del mundo, cada una de un equipo infectado, indicando que el ciberataque había sido de una gran magnitud. Sus intenciones originales eran encontrar el "centro de comando" de los creadores de WannaCry para estudiar con mayor profundidad su funcionamiento, pero accidentalmente encontró su *killswitch*[32] (Greenberg 2019).

[30] El sitio web estaba conformado por una serie de letras que no parecen estar relacionadas ni ordenadas de alguna manera: iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com (Greenberg 2019).

[31] Una Computadora Virtual, Máquina Virtual (MV) o *Virtual Machine* (VM) es un programa computacional que emula el funcionamiento de una computadora física. Se podría describir como "tener una computadora, dentro de una computadora". Debido a que usualmente se encuentran aisladas del sistema, son utilizadas comúnmente por los trabajadores de la seguridad informática para poner a prueba programas maliciosos sin infectar una computadora real (Intel Corporation 2021).

[32] Un *killswitch* es un término utilizado comúnmente como "interruptor de emergencia". En este caso se refiere a que se encontró una acción que interrumpió súbitamente el funcionamiento del programa malicioso.

No se conocen las motivaciones, los objetivos, ni la identidad[33] de los creadores de WannaCry. Las dos teorías principales señalan que buscaban obtener la mayor cantidad de recursos económicos o generar daños y caos en escala mundial. Pero, el hecho de que haya tenido un error estratégico tan grave como la existencia de un *killswitch* y la falta de un sistema para entregar las llaves de desbloqueo de los archivos encriptados, dan indicios de que el ransomware fue liberado antes de lo deseado (Greenberg 2019).

WannaCry y NotPetya poseen tales similitudes, que ha provocado que algunos expertos consideren la posibilidad de que ambos programas maliciosos hayan sido creado por el mismo equipo. Incluso, debido a la proximidad de las fechas en que sucedieron ambos eventos, y que los efectos ocasionados fueron similares, se cree que WannaCry pudo haber sido un ensayo para la liberación de NotPetya posteriormente.

WannaCry tuvo consecuencias económicas de gran magnitud, y en su momento, fue el ciberataque de mayor impacto económico de la historia. Se estima que para el Reino Unido tuvo una pérdida de £22,000,000 de libras esterlinas, mientras que, a nivel mundial, se estima una pérdida de $4,000,000,000 USD por el alto a la producción, la restauración de equipos y el pago de costos en diferentes empresas multinacionales. No hubo verdaderas consecuencias para los autores del ciberataque, puesto que no se logró determinar con exactitud su identidad, mientras diversos expertos afirman que el responsable del ataque fue *Sandworm* , otros expertos apuntan a Corea del Norte (Greenberg 2019; Kaspersky Lab 2021e).

[33] El gobierno de Donald Trump, a través de la Casa Blanca, emitió un comunicado en diciembre de 2017 señalando a Corea del Norte como los autores de WannaCry y relacionando el evento a los hackeos a Sony. Sin embargo, muchos expertos cuestionan esta teoría, puesto que se cree que las ciberamenazas creadas por el gobierno norcoreano suelen tener motivaciones ideológicas y políticas, además de ser dirigidas a objetivos muy específicos, características que no son detectadas en este incidente (Greenberg 2019).

A continuación, se presentan en una tabla los eventos mencionados anteriormente con el objetivo de sintetizar y visualizar de una mejor manera lo sucedido:

Tabla 3.

Antecedentes de NotPetya.

Nombre	**Año**	**Víctimas**	**Autor**	**Propósito**	**Consecuencias**
BlackEnergy	2015	Compañía eléctrica Prikarpattiaoblenergo	Probablemente Rusia/Sandworm	Sabotaje	Apagones de electricidad al oeste de Ucrania de hasta 6 horas
Petya	2016	Computadoras de recursos humanos, principalmente en Alemania	Janus Cybercrime Solutions	Cibercrimen	Equipos e información "secuestrados". Pago del rescate a los autores.
Industroyer/ CrashOverride	2016	Compañía eléctrica Ukrenergo	Probablemente Rusia/Sandworm	Sabotaje	Apagones de electricidad en Kiev de aproximadamente 1 hora
The Shadow Brokers	2017	Agencia Nacional de Seguridad de los Estados Unidos	The Shadow Brokers	Espionaje	Exfiltración y divulgación al público de herramientas de hackeo altamente sofisticadas detectadas por la NSA
WannaCry	2017	Infecciones a nivel global de equipos con versiones desactualizadas de Microsoft Windows	Desconocido	Cibercrimen	Pérdida de 4 mil millones de dólares a nivel mundial. Encriptación de archivos esenciales. "Ensayo" del uso de EternalBlue en un programa malicioso

Antes del lanzamiento de NotPetya, ocurrieron una serie de eventos, cuyas consecuencias contribuyeron directa o indirectamente a su diseño. *Tabla de elaboración propia.*

2.3. Diseño técnico de NotPetya

Antes de explicar la propagación de NotPetya alrededor del mundo, es necesario detallar las diferentes herramientas con las que contaba este programa malicioso, ya que poseía un nivel de sofisticación técnica muy elevado que le permitió desencadenar los efectos deseados. A continuación, se explicarán las características técnicas más importantes de NotPetya.

2.3.1. EternalBlue

Como se mencionó en la sección anterior, EternalBlue fue uno de los exploits principales obtenidos de la NSA y compartidos en la red por TSB. Este exploit estaba diseñado para aprovecharse de una vulnerabilidad específica presente en todas las versiones desactualizadas de Windows 8, ya que estos equipos contaban con una función antigua que poseía una falla muy importante, el Server Message Block (SMB)[34]. El SMB es un tipo de protocolo que permitía la comunicación entre dispositivos conectados a una misma red, y facilitaba el compartir información, archivos y el acceso a impresoras directamente. Esta característica contenía errores de seguridad críticos que permitían que cualquier persona pudiera enviar mensajes SMB a una computadora de una manera específica para ejecutar código en ella a distancia (Greenberg 2019).

EternalBlue se aprovechaba de principalmente tres vulnerabilidades del SMB que producían un desbordamiento de búfer, ocasionando que la computadora no detectara que la información recibida poseía una carga útil para generar efectos no deseados. Los atacantes utilizaban esta brecha en la seguridad para lanzar ejecuciones remotas de código en las computadoras afectadas y modificar el comportamiento estas. En el caso de NotPetya, EternalBlue fue utilizado para, en primer lugar, infectar los equipos que no contaban con las actualizaciones de Windows adecuadas, y en segundo lugar, instalar otra herramienta sofisticada para proseguir el ataque: *DoublePulsar* (Kulkarni et al. 2018; Greenberg 2019).

Para WannaCry y NotPetya, EternalBlue funcionó como la "llave" que les otorgó acceso a los equipos con versiones antiguas de Windows 8, y les facilitó propagarse rápidamente, ya que una gran parte de las víctimas no actualizaba sus equipos por miedo a perder información, funciones o que los programas de sus computadoras dejaran de ser compatibles con las nuevas

[34] *Server Message Block* (SMB) es un protocolo para el intercambio de archivos dentro de una misma red, que permite que las aplicaciones de una computadora lean y escriban archivos (Microsoft 2016).

versiones del sistema operativo. Además, debido a que Microsoft se enteró del exploit unos días antes, lanzó una actualización de emergencia, pero debido a que una gran parte de los usuarios decidió no descargar esta actualización, el número de potenciales víctimas no se redujo de manera significativa.

2.3.2. DoublePulsar

Después de haberse infiltrado en una computadora, *EternalBlue* se conectaba a internet y comenzaba la instalación de otro exploit llamado *DoublePulsar*, también diseñado por la NSA y publicado por TSB. *DoublePulsar* funcionaba como *backdoor* para que los atacantes pudieran instalar código malicioso sin que el usuario se enterara o tuviera que interactuar con la computadora de manera alguna (Saldana 2018).

DoublePulsar también se aprovechaba de vulnerabilidades en SMB, pero afectaba específicamente a los sistemas operativos de Windows XP, 2003, Vista, 7, 8 y 2008 R2. También fue corregido con el parche de actualización lanzado por Microsoft que corregía *EternalBlue*, ya que ambos exploits funcionaban en conjunto, pero la cantidad de equipos infectados con ambos exploits fue muy elevada (Kulkarni et al. 2018).

Los investigadores de seguridad informática no sabían cómo determinar el número de equipos infectados con ambos exploits, hasta que comenzaron a escanear el internet y se dieron cuenta que aquellas computadoras que habían sido vulneradas con *DoublePulsar*, respondían de una manera particular si recibían un ping de red[35]. Al descubrir esto, los investigadores comenzaron a lanzar pings de red continuamente para descubrir la cantidad de respuestas obtenidas y, el 14 de

[35] Ping es la abreviación de *Packet Internet Groper*, que en español puede ser interpretado como "Buscador de Paquetes de Internet". Es un tipo de programa que le permite a los usuarios comprobar la existencia de una dirección IP específica. Es una herramienta utilizada comúnmente para el diagnóstico de conexiones de una computadora (Zola 2021).

abril, dos semanas después de la publicación de TSB, lograron determinar que más de 400,000 equipos habían sido infectados, y que el número iba en aumento (Greenberg 2019).

DoublePulsar funcionó como la puerta trasera para los ciberatacantes, que lo utilizaban para monitorear lo que sucedía con el programa malicioso y para continuar implementando las siguientes fases del ciberataque. Era una línea de comunicación entre sus creadores y el programa malicioso, que les facilitó llevar a cabo el ciberataque.

2.3.3. Mimikatz

Mimikatz[36] es un programa creado por el programador francés Benjamin Delpy como forma de protesta en contra de Microsoft por no hacer caso a sus recomendaciones de seguridad. *Mimikatz* se aprovecha de una vulnerabilidad en WDigest, una función de Windows para permitir que usuarios, principalmente pertenecientes a instituciones corporativas o gubernamentales, pudieran iniciar sesión con su usuario y contraseña de manera sencilla. WDigest guardaba los nombres de usuario y contraseñas en la memoria de la computadora para ser llenados automáticamente cuando se le solicitaba, por lo que sólo era necesario ingresarlas una única vez para evitar escribirlas continuamente (Greenberg 2019).

Delpy se dio cuenta que WDigest encriptaba las claves de los usuarios en la memoria de la computadora, por lo que no podían ser leídas de manera sencilla, pero también detectó que la misma computadora reservaba una copia de la clave secreta necesaria para desencriptar la información, por lo que afirmaba era como "guardar un secreto protegido con contraseña en un correo, en el que también compartes la contraseña". Delpy detectó esta característica como una vulnerabilidad grave en el sistema de Windows, por lo que alertó a Microsoft de los posibles riesgos de mantener el

[36] *Mimikatz* es un nombre conformado por el prefijo francés "*mimi*" que significa "lindo" y "*katz"*, que significa "*gatos",* por lo que *Mimikatz* podría traducirse como "gatos lindos" (Greenberg 2019).

funcionamiento de WDigest sin modificar. Sin embargo, Microsoft descartó sus comentarios y afirmó que no era una amenaza seria, y que no se necesitaba lanzar ningún parche de actualización ya que no existía ningún riesgo verdadero de penetrar la seguridad de su sistema (Greenberg 2019, 187).

Al frustrarse con la respuesta de Microsoft, Delpy diseñó *Mimikatz* para demostrar que la vulnerabilidad podía ser aprovechada para extraer las contraseñas del equipo y obtener acceso a toda la información dentro del sistema, buscando incentivar a la empresa informática a lanzar un parche de actualización que corrigiera las potenciales brechas de seguridad (Greenberg 2019).

En mayo de 2011, Delpy lanzó al público *Mimikatz* mencionando que, si Microsoft no quería corregir sus errores, entonces le mostraría al mundo lo que ocurría, con el propósito de fomentar prevención y mayor cuidado de la información sensible. A pesar de que Delpy lanzó *Mimikatz* como software privativo[37] y encriptó la manera en que funcionaba, rápidamente detectó que en foros de *hackers* discutían el funcionamiento de la herramienta que había creado, y que habían equipos dispuestos a aplicar ingeniería inversa para descifrar su funcionamiento, e incluso, aceptó haber sido informado que su programa había sido utilizado para penetrar las redes de oficinas gubernamentales de un gobierno, sin especificar cual (Greenberg 2019).

Mimikatz se convirtió rápidamente en una herramienta utilizada ampliamente por *hackers* para diseñar nuevos programas maliciosos para obtención de contraseñas, y su uso se volvió muy común. En 2013, Microsoft finalmente reconoció las brechas de seguridad existentes y lanzó un parche de actualización para inhabilitar las funciones de WDigest a partir del sistema operativo

[37] Es un tipo de programa el cuál posee restricciones de uso, modificación y copia establecidos por sus creadores. El programa está compuesto de código cerrado para evitar la descompilación o cambios en el código (Kaspersky Lab 2021b).

Windows 8.1, neutralizando las vulnerabilidades que podían ser aprovechadas por *Mimikatz (Greenberg 2019).*

A pesar de que *Mimikatz* dejó de ser efectivo en equipos actualizados con los últimos sistemas operativos de Microsoft Windows, fue detectado en el código de NotPetya y en el de otro *ransomware* que ocurrió posteriormente llamado *BadRabbit*[38]. Esta característica puede sugerir que los creadores de ambos programas maliciosos tenían contemplado infectar equipos que poseían versiones desactualizadas de Windows que contaban aún con WDigest para aprovecharse de la vulnerabilidad.

Mimikatz funcionó como la herramienta para obtener acceso a los usuarios y contraseñas de las víctimas de NotPetya, no sólo para facilitar el proceso de encriptación y restringir el acceso a archivos, sino también para propagarse fácil y rápidamente a través de las redes infectadas.

2.3.4. EternalRomance

EternalRomance es otra de las herramientas de explotación de vulnerabilidades filtradas por TSB y extraídas de la NSA. Este *software* está diseñado para aprovecharse de una vulnerabilidad en el protocolo del *Server Message Block* (SMB) de Windows para poder implementar una ejecución de código remota. Fue detectado tanto en NotPetya, como en BadRabbit (Malwarebytes 2019).

EternalRomance se aprovecha de elementos como el puerto TCP 445[39] y PsExec[40] para ejecutar programas de manera remota, ya que les permiten a los atacantes interactuar y controlar

[38] *BadRabbit* puede ser traducido al español literalmente como "MalConejo". Fue otro programa malicioso de tipo *ransomware* liberado meses después de NotPetya y que, de manera similar, se propagó rápidamente.

[39] El Puerto TCP 445 es utilizado por las versiones más modernas de SMB. Es un tipo de puerto abierto, significando que permite la conexión y aceptación de paquetes a través de la red, por lo que puede recibir información de fuentes externas (Tunggal 2021).

[40] PsExec es un programa que permite la ejecución de procesos en otros sistemas sin la necesidad de instalar programas manualmente. También le permite al usuario dar indicaciones de comando a sistemas de manera remota.(Russinovich 2021).

las aplicaciones y configuraciones dentro de un sistema. Las vulnerabilidades que eran explotadas por EternalRomance fueron detectadas por Microsoft y corregidas a través del mismo parche de actualizaciones de nivel crítico emitido para corregir las vulnerabilidades de EternalBlue (Russinovich 2021; Microsoft 2017).

Podríamos decir que EternalRomance fue una pieza clave para NotPetya, puesto que fue una de las herramientas que les permitió a sus creadores ejecutar código de manera remota y realizar cambios en los dispositivos sin la necesidad de estar cerca de ellos. Podría considerarse como un "control remoto" con el que podían realizar las actividades que deseaban, desde cualquier ubicación geográfica.

2.3.5. Integración de NotPetya

Los exploits y vulnerabilidades expuestas en las secciones anteriores, fueron las principales herramientas que les brindaron el nivel de complejidad y peligrosidad a NotPetya. La adecuada integración de cada uno de sus elementos, permitieron llevar a cabo sus actividades de una manera rápida y efectiva. Si bien, el funcionamiento y características de cada una de sus partes ya fueron expuestos, es adecuado recapitular brevemente la función de cada una de ellas antes de profundizar en la manera en que el programa malicioso fue liberado y esparcido en Ucrania y alrededor del mundo.

NotPetya utilizó principalmente cuatro herramientas para la explotación de vulnerabilidades, presentes principalmente en equipos que funcionaban con una versión desactualizada del sistema operativo de Microsoft, Windows: EternalBlue, DoublePulsar, Mimikatz y EternalRomance; cada uno de ellos cumplía una función importante en el proceso de propagación del programa malicioso y la encriptación de archivos.

EternalBlue, DoublePulsar y EternalRomance fueron herramientas creadas por la NSA para la vigilancia y monitoreo de equipos con el propósito de proteger la seguridad nacional. El gobierno de Estados Unidos estaba consciente de las vulnerabilidades existentes en los sistemas de Windows, pero en lugar de dar aviso a la empresa informática, utilizaron la información para crear estas herramientas para su propio beneficio. Debido a la intrusión de TSB y exfiltración de esta información, fue que las tres herramientas fueron conocidas y utilizadas por el público.

EternalBlue fue la herramienta utilizada para la primera fase del ciberataque, ya que funcionaba para infectar a aquellos equipos que no contaban con los parches de seguridad necesarios para defenderse del programa malicioso, por lo que identificaba a sus víctimas y las infectaba de manera desapercibida, para posteriormente ejecutar código a distancia y de esa manera instalar la segunda herramienta, DoublePulsar.

La labor de DoublePulsar consistió en establecer una puerta trasera en los equipos infectados para mantener una línea de comunicación con sus creadores y ejecutar las instrucciones emitidas por ellos. Esta herramienta fue la "entrada" para que los *hackers* pudieran realizar las acciones deseadas en los equipos y funcionó como la conexión entre los atacantes y sus víctimas.

Gracias a DoublePulsar, se enviaba la información necesaria para instalar y ejecutar Mimikatz, el exploit creado por Benjamin Delpy, el cual encontraba los nombres de usuario y contraseñas guardadas dentro de los equipos infectados. Mimikatz procedía a obtener acceso no autorizado a los equipos conectados dentro de una misma red y procedía a infiltrarse en ellos para posteriormente denegar el acceso a los usuarios y encriptar sus archivos.

Finalmente, EternalRomance fue una herramienta complementaria que les permitía a los atacantes ejecutar código a distancia, por lo que podían realizar los cambios deseados de manera remota.

Cada una de estas piezas de *software* se complementaron de tal manera que la encriptación de archivos fue rápida y precisa. Además, debido a que estaban enfocados en afectar a equipos desactualizados, las infecciones fueron muy fáciles de realizar. Cuando una persona detectaba la infección, ya era demasiado tarde y había perdido el acceso a sus archivos y equipos.

Después de haber conocido los aspectos técnicos de NotPetya, a continuación, se expondrán los eventos principales en el proceso de propagación del programa malicioso y la manera en que sus creadores lanzaron el ciberataque.

2.4. Propagación de NotPetya

El 27 de junio de 2017, NotPetya fue lanzado a la red, infectando a millones de computadoras alrededor del mundo, pero centrándose principalmente en Ucrania. Es un programa malicioso de tipo *ransomware*[41] que encripta la información de las computadoras infectadas que no poseen una versión actualizada de Windows.

El ciberataque ocurrió tan sólo unos días después de WannaCry, por lo que Microsoft había publicado una serie de actualizaciones para sus sistemas operativos con la intención de corregir las vulnerabilidades que fueron aprovechadas por el programa malicioso, y que también fueron utilizadas para la distribución de NotPetya. Sin embargo, no todas las personas habían logrado actualizar sus equipos antes del ciberataque, ya sea porque los equipos cumplían actividades esenciales y no podían ser apagados, por desinformación o por creer que no era necesario hacerlo.

[41] Si bien se ha determinado que NotPetya es un *ransomware* debido a que su actividad principal fue la encriptación de archivos, debido a las características del ciberataque y la falta de un mecanismo para la devolución de los archivos encriptados, muchos expertos han determinado que no es un *ransomware* normal. Se cree que NotPetya utilizó las técnicas de un *ransomware*, no para obtener dinero para el rescate de los equipos, sino para crear disrupción y caos dentro de Ucrania, por lo que también han concluido que un actor estatal se encuentra detrás del incidente (Greenberg 2019).

Debido a la falta de actualizaciones en las computadoras, NotPetya logró infectar equipos pertenecientes al sector público y privado, dentro y fuera de Ucrania, a una gran velocidad. Redes de importantes organizaciones e infraestructura esencial en Ucrania comenzaron a presentar afectaciones en su funcionamiento y diversas actividades tuvieron que ser detenidas.

NotPetya comenzó a ser considerado el mayor ciberataque en la historia de la ciberseguridad por las consecuencias económicas, políticas y sociales que generó, al haber alterado el orden y el funcionamiento normal de la sociedad ucraniana. Se reportaron infecciones en diversas dependencias gubernamentales, empresas y grandes conglomerados multinacionales, por lo que el programa malicioso tuvo un gran alcance.

Si bien, los ciberataques de tipo *ransomware* suelen ser diseñados por cibercriminales en la búsqueda por obtener importantes ganancias económicas, el proceso que se llevó a cabo para su difusión despertó algunas sospechas de que un grupo con intereses importantes en el país eran los verdaderos creadores del programa malicioso. Se descubrió que NotPetya no era un *ransomware* común, y que el programa malicioso no poseía ningún mecanismo para devolver la información encriptada, por lo que se sospecha que fue diseñado con intenciones de crear la mayor cantidad de disrupción posible en el territorio ucraniano, y que, por lo tanto, un actor estatal se encontraba detrás de su creación.

Un primer dato al que se debe prestar atención es la fecha en la que NotPetya fue lanzado. El ciberataque se realizó el 27 de junio de 2017, un día antes del Día de la Constitución en Ucrania, fecha de descanso oficial en la que una gran parte de la población no labora y las oficinas quedan vacías. Este factor provocó que el personal de los departamentos de informática no pudieran reaccionar inmediatamente al ataque o no tuvieran acceso al equipo necesario para comenzar una respuesta, por lo que las infecciones comenzaron a ocurrir sin ninguna oposición (Greenberg 2018).

Ese mismo día por la mañana, el coronel Maksym Shapoval fue asesinado con una bomba escondida en el automóvil que iba conduciendo en Solomyansky, un distrito localizado al oeste de Kiev. Shapoval era el jefe de una unidad de fuerzas especiales perteneciente al ejército ucraniano, y también había participado activamente en misiones al este de Ucrania como parte del conflicto con Rusia. Las autoridades ucranianas afirmaron que era posible que el ejército ruso se encontrara detrás del atentado, en el que también hubo civiles heridos que se encontraban cerca del automóvil al momento de la explosión (Greenberg 2019; Luhn 2017).

Sin embargo, este no fue el único asesinato de un miembro del ejército ucraniano, pues al día siguiente, el 28 de junio de 2017, fue asesinado el coronel Yuriy Vozny, de la misma manera que el coronel Shapoval, con una bomba escondida en el auto que conducía. Este atentado ocurrió en Kostiantynivka, en el Óblast de Donetsk; el coronel Vozny murió inmediatamente y sus tres acompañantes, también miembros del ejército, fueron heridos de gravedad. Así como con el atentado del coronel Shapoval, el gobierno de Ucrania señaló a Rusia como los responsables y consideró que ambos eventos se encontraban relacionados directamente con el ciberataque de NotPetya, pero el gobierno ruso negó las acusaciones (RFE/RL's Ukrainian Service 2017).

Sin embargo, el factor más importante a considerar es que, el ataque fue dirigido específicamente a Ucrania y fue diseñado de tal manera que los objetivos localizados dentro del país fueran las primeras víctimas, y las más afectadas. Así mismo, su propagación a nivel internacional se realizó a través de empresas e instituciones que tenían algún vínculo con Ucrania, por lo que algunos expertos sugieren que el *ransomware* no fue diseñado en ningún momento para obtener dinero, sino para enviar un mensaje político, que Ucrania y cualquiera que hiciera negocios con el país, estaba propenso a recibir un ataque (Levi y Serper 2021b).

Debido a estos factores, los eventos que antecedieron a NotPetya y las tensiones continuas entre ambos países, diversos expertos y autoridades gubernamentales han considerado que

Sandworm también es el equipo detrás de la creación y liberación del programa malicioso, afirmando que es una fase más de las continuas operaciones de ciberespacio realizadas contra Ucrania desde la anexión de Crimea (Greenberg 2019).

Similar a lo que ocurre con una pandemia de un nuevo virus a nivel global, algunos expertos han hecho la comparación con la propagación de virus informáticos y han señalado sus similitudes. Si bien la propagación de NotPetya fue mucho más rápida que la de un virus biológico, los expertos señalan a Ucrania como el "paciente cero" de las infecciones y señalan la intrusión a Linkos Group en primavera de 2017 como una fase inicial y clave para entender la difusión del programa malicioso en el mundo (Levi y Serper 2021a).

Antes de explicar con mayor detalle los efectos provocados por NotPetya en sus víctimas y las consecuencias desencadenadas por el ciberataque, a continuación, se explicarán los primeros momentos que fueron clave en el lanzamiento y distribución del programa malicioso.

2.4.1. Linkos Group y M.E.Doc

Linkos Group es una compañía de *software* ucraniana localizada en Kiev que proporciona diversos servicios informáticos, enfocados principalmente en el desarrollo de programas computacionales financieros, legales y de transferencia de documentos dirigidos a instituciones gubernamentales o privadas que emprenden actividades económicas en o con Ucrania. Uno de sus productos más importantes es el programa M.E.Doc, un programa diseñado para oficinas de gobierno y empresas para el reporte y administración de datos financieros importantes, desde salarios, hasta el pago de impuestos (Linkos Group 2021a, 2021b).

M.E.Doc es una plataforma de contabilidad utilizada ampliamente por las empresas que realizan negocios en Ucrania, y, anteriormente, era la principal opción para el pago de impuestos, por lo que, de una forma, todos los negocios que emprendían actividades económicas en o con

Ucrania, se encontraban conectados indirectamente a través de este programa computacional instalado en sus equipos. Linkos Group se encarga de lanzar actualizaciones continuamente desde sus servidores en las oficinas de Kiev para mantener a las empresas con las versiones más recientes del programa y parchar cualquier vulnerabilidad detectada (Levi y Serper 2021a; Linkos Group 2021b).

En la primera mitad de 2017, los autores de NotPetya lograron infiltrarse en los sistemas de Linkos Group y colocar un *backdoor* en los equipos encargados de lanzar las actualizaciones de M.E.Doc, lo que les permitía no sólo tener acceso y modificar remotamente las computadoras de la empresa ucraniana, sino también llegar a todos los equipos que tuvieran el programa financiero instalado. Esta brecha de seguridad no fue detectada a tiempo por Linkos Group y continuaron realizando sus actividades con normalidad, lanzando las actualizaciones diarias de rutina y procesando la información de miles de computadoras conectadas a través de los servidores de M.E.Doc (Levi y Serper 2021a).

Las actualizaciones continúas realizadas por Linkos Group a través de los servidores infectados también comenzaron a instalar, sin autorización y sin ser descubiertos, un *backdoor* a cada una de las computadoras que tuviera M.E.Doc instalado, y si bien no provocaron ninguna alteración en el funcionamiento de los equipos, fue un paso de preparación para lo que ocurriría después. El 27 de junio de 2017, los creadores de NotPetya utilizaron este acceso no autorizado a las computadoras con M.E.Doc para liberar el *payload* y comenzar el ciberataque. Rápidamente las computadoras infectadas comenzaron no sólo a reiniciarse, encriptando toda la información dentro de ellas, sino también a propagar NotPetya a los equipos conectados en la misma red, y posteriormente, a otras redes (Greenberg 2019).

El sistema de pago de impuestos proveído por M.E.Doc era utilizado por más de 400,000 clientes en toda Ucrania, representando aproximadamente el 90% de las empresas en el país. Los

creadores de NotPetya no necesitaron infectar individualmente cada computadora, y no tuvieron que crear un programa que aparentara ser una versión real de M.E.Doc. Lo único que necesitaron fue infectar la "fuente", los servidores encargados de las actualizaciones de M.E.Doc, de esa manera no sólo lograron propagar el programa malicioso a todas las computadoras conectadas a los servidores, sino también utilizaron un programa real para llevar a cabo sus actividades y no levantar ninguna sospecha (Borys 2017).

Diversos expertos comenzaron a notar que el programa malicioso estaba corrompiendo el funcionamiento de los dispositivos a una gran velocidad, y que se propagaba a redes enteras en cuestión de segundos. Se comenzaron a reportar infecciones en instituciones gubernamentales y empresas privadas, y algunas actividades se detuvieron por la falla en las computadoras. Con el paso de tiempo, notaron que la característica en común de las primeras infecciones era M.E.Doc, por lo que intentaron desconectar sus equipos a las redes, aunque en algunas ocasiones era ya demasiado tarde (Greenberg 2019).

Después de haber detectado que las infecciones comenzaron por el programa financiero, las autoridades ucranianas decidieron obtener los servidores para realizar las investigaciones adecuadas, por lo que emitieron una orden para entrar a las oficinas de Linkos Group y extraerlos. Sin embargo, esto sucedió una semana después del ciberataque, cuando NotPetya ya se había esparcido por el mundo y el aislamiento del origen del programa malicioso ya no contribuía a detener su progreso. A pesar de esto, un equipo de la policía ucraniana entró a Linkos Group y aseguró los servidores para su posterior investigación (Greenberg 2019).

Tras las investigaciones de lo ocurrido, se pudo determinar que Linkos Group había sido infiltrado por un largo periodo de tiempo, y que M.E.Doc no había sido el único programa alterado, sino que también existía un "plan B" en caso de que la infección del programa financiero fuera

detectada y eliminada: Un script VBS[42] que comprobaba si la propagación de NotPetya ocurría de acuerdo a lo planeado y que poseía las capacidades de instalar programas no deseados para llevar a cabo el ciberataque en caso de que el plan original fallara (Greenberg 2019).

También se descubrió que la manera en que se logró infectar Linkos Group fue a través del sistema de gestión de contenido[43] de su página web, el cual es utilizado para modificar la apariencia que el sitio tiene. Los *hackers* configuraron un *web shell*[44] en el servidor para instalar cualquier programa deseado, permitiéndoles no sólo distribuir el programa malicioso a través de la versión alterada de M.E.Doc, sino también crear un canal de comunicación directa con todas las computadoras infectadas, que utilizaron para enviar información específica, instalar programas remotamente y robar información de las maquinas que poseyeran M.E.Doc (Greenberg 2019).

Otro hallazgo importante de las investigaciones fue una serie de archivos que datan de 2015, en el que se encontró otro *web shell* oculto, indicando que Linkos Group había sido infiltrada por al menos dos años antes del ciberataque. No se pudo comprobar si esta penetración estaba directamente relacionada con NotPetya o con alguno otro ciberataque anterior dirigido a Ucrania, pero demuestra que la seguridad que poseía la empresa no era la más avanzada, lo que contribuyó a que fuera elegida como el objetivo principal para desencadenar el ciberataque. Al ser cuestionada de estos hechos, Olesya Linnyk, la fundadora de Linkos Group, aseguró que siempre prestaban atención a la seguridad informática de su empresa, pero que jamás se imaginaban ser el centro de

[42] VBS son las siglas de "*Visual Basic Script".* Es un lenguaje de script de Microsoft utilizado comúnmente para el diseño de sitios web (Kaspersky Lab 2021d).

[43] Son programas utilizados para la creación, administración y modificación de un sitio web. Comúnmente utilizados por personas que no cuentan con conocimientos técnicos especializados para crear un código y construir una página web desde cero (Kinsta Inc. 2020).

[44] Los *Web Shells* son interfaces que le permiten a los usuarios, usualmente creadores de programas maliciosos, ejecutar comandos en servidores para el robo de información y credenciales (Detection and Response Team (DART) y Microsoft 365 Defender Research Team 2021).

un ciberataque de tal magnitud, por lo que no se encontraban preparados para enfrentar un incidente de ese tipo (Greenberg 2019).

Linkos Group se convirtió en el centro de las infecciones de NotPetya, si bien involuntaria e inconscientemente, su programa financiero fue la causa de que ocurrieron consecuencias importantes, no sólo en los equipos computacionales infectados, sino también económica, social y políticamente.

2.4.2. Inicio del ciberataque y propagación internacional

El día en que NotPetya fue liberado, diversos expertos fueron alertados rápidamente para comenzar el análisis del malware e iniciar la respuesta del ciberataque. Uno de ellos fue Oleh Devianko, el cofundador de Information Systems Security Partners (ISSP), una empresa ucraniana enfocada en ciberseguridad, fundada en 2008, dedicada a la detección, respuesta y análisis de ciberincidentes alrededor del mundo (Kosciuszko Institute y CYBERSEC 2019).

Debido al descanso por el Día de la Constitución, Derevianko se encontraba fuera de la oficina, en una región alejada del centro de Kiev, por lo que cuando recibió las llamadas de emergencia de diversas oficinas alrededor de Ucrania, tuvo que detenerse a trabajar remotamente desde su computadora en un restaurante que encontró en el camino. Rápidamente se dio cuenta del gran alcance que el programa malicioso tenía, y comenzó a observar sus efectos inmediatos en la población de la región en que se encontraba. Los sistemas de cobro con tarjeta dejaron de funcionar y los cajeros automáticos se detuvieron, por lo que la gente dependía del dinero físico con el que contaban en ese momento y se comenzó a reportar que los sistemas para el reparto de pensiones y medicamentos también presentaban fallas, por lo que comenzó a existir un miedo en la sociedad de no poder contar con bienes y servicios básicos (Levi y Serper 2021a; Greenberg 2019).

Se comenzó a reportar que los sistemas informáticos de computadoras en todo Ucrania se habían inhabilitado por completo, y que todo tipo de oficinas, desde gubernamentales hasta pequeñas empresas, habían detenido sus actividades por no poder acceder a la información de sus equipos. Derevianko clasificó el incidente como una "ciberinvasión masiva y coordinada" y se puso en contacto con los clientes de ISSP para advertirles de lo sucedido y recomendarles desconectar todos sus equipos de la red, aunque en muchos casos, ya era demasiado tarde. Derevianko consideró inmediatamente que el ciberataque había sido creado por un actor estatal o un actor privado apoyado por el Estado, teniendo a Rusia y *Sandworm* como principales sospechosos (Levi y Serper 2021a; Greenberg 2019).

El gobierno de Ucrania también acusó a Rusia de estar detrás del incidente, considerando que no había otro país que se beneficiara de atacarlos. Este señalamiento fue respaldado por autoridades de la Organización del Tratado del Atlántico Norte (OTAN), quienes consideraron a NotPetya como una estrategia de Rusia para desestabilizar al país. La organización asistió al país en las investigaciones y seguimiento del caso, y mencionaron que este tipo de casos podrían activar la cláusula de defensa mutua por sus severas consecuencias (Borys 2017).

Otro experto que comenzó a trabajar en la respuesta contra NotPetya fue Amit Serper, hacker y vicepresidente de investigación de seguridad para América del Norte en Guardicore, además de haber participado en la división de inteligencia del ejército de Israel. Serper no se encontraba en las oficinas de Cybereason, la empresa de ciberseguridad para la que trabajaba, pero se dispuso a analizar NotPetya desde su casa, con las herramientas que contaba y pidiendo información a la gente a través de redes sociales (Levi y Serper 2021b).

Serper logró aplicar ingeniería inversa y logró descubrir que NotPetya no contaba con ninguna herramienta para desencriptar la información bloqueada una vez que el rescate era pagado, por lo que comenzó a alertar a las víctimas de que evitaran transferir los recursos solicitados.

También descubrió que, como NotPetya estaba diseñado específicamente para equipos con el sistema operativo Windows, poseía una característica en su programación que provocaba la cancelación del proceso de encriptación y evitaba la pérdida de documentos (Levi y Serper 2021b).

Tras los análisis del programa malicioso y gracias a la colaboración de Ido Naor, un investigador de Kaspersky se encontró que si la computadora a la que NotPetya intentaba infectar poseía un archivo con el nombre y terminación "perfc.dat", la encriptación no ocurría y los archivos se quedaban a salvo. A diferencia de otros ciberataques en los que se puede encontrar un *killswitch* para erradicar los efectos de un programa malicioso, Serper había encontrado una especie de "vacuna", ya que si los equipos contaban con el archivo señalado, antes de que ocurriera la infección, no sufrían las consecuencias de NotPetya (Levi y Serper 2021b).

A pesar de los descubrimientos y advertencias emitidas por los expertos en informática, NotPetya continuaba infectando equipos a una gran velocidad, y pronto comenzaron a llegar noticias de que el programa malicioso ya había cruzado la frontera, todo en cuestión de horas. Empresas multinacionales comenzaron a reportar interrupciones en sus servicios y a detener operaciones en diversos países alrededor del mundo.

Debido a la interconexión del mundo el programa malicioso logró propagarse a nivel internacional, infectando primero a una empresa multinacional localizada dentro del territorio ucraniano, en este caso particular siendo Maersk una de las más afectadas, para posteriormente continuar su propagación en las redes de esa empresa, incluyendo las localizadas fuera de Ucrania.

El lanzamiento de NotPetya poseyó un alto nivel de preparación y de planeación, con objetivos y víctimas muy claras, lo que provocó que sea considerado como uno de los programas maliciosos más peligrosos y dañinos del mundo. Los efectos que provocó en Ucrania y en el mundo fueron diversos y tuvieron un importante impacto. En el siguiente capítulo se profundizarán estos elementos y se abordará el impacto internacional que el ciberataque tuvo.

Capítulo 3. Las consecuencias provocadas por NotPetya y sus efectos en Ucrania y el mundo

Como se ha mencionado anteriormente, el poder ejercido por medio del ciberespacio se puede observar de una mejor manera a través de los efectos que son producidos por las acciones de los actores internacionales. Debido a la naturaleza de este espacio, en ocasiones es muy complicado detectar cuando un actor ha realizado alguna acción a través del ciberespacio con el objetivo de influir la conducta de otro, sin embargo, cuando estas consecuencias tienen un impacto significativo en el mundo real, las intenciones pueden ser más claras.

Los casos de ciberataques expuestos anteriormente han ilustrado breve y claramente la manera en que un programa malicioso puede ser utilizado para alcanzar objetivos e intereses muy particulares. Cada uno de los incidentes mencionados ha generado un verdadero impacto en sus víctimas, que les ha provocado modificar su conducta. Desde la recolección de inteligencia a través del ciberespionaje, como el caso de Duqu 2.0, hasta casos de sabotaje, como el caso de Stuxnet, han favorecido directa o indirectamente a sus creadores, brindándoles ventajas estratégicas que han utilizado a su favor en múltiples ocasiones.

Los ciberataques han ido aumentando en sofisticación y complejidad con el paso del tiempo, lo que ha provocado que sean capaces de generar mayores efectos con impacto social, económico y político importantes, y por lo mismo, volviéndolos más efectivos. En los últimos 20 años, cada nuevo programa malicioso ha superado al anterior en peligrosidad y riesgo de desencadenar severas acciones fuera del control de sus creadores, por lo que en la actualidad podemos observar cada vez más casos en los que actores internacionales se ven afectados por ciber incidentes que merman sus capacidades.

NotPetya es uno de los casos en que el poder ejercido a través del ciberespacio puede ser observado de una forma más clara. Independientemente de la identidad de su creador, este programa malicioso fue dirigido específicamente a Ucrania, impactando fuertemente a su sociedad y provocando severos efectos en equipos computacionales, dentro y fuera de del país, disminuyendo temporalmente las capacidades de las víctimas.

Cada uno de los efectos que se describirán a continuación, provocaron consecuencias sustanciales en múltiples actores, que, dependiendo la manera en que fueron afectados, configuraron las decisiones que tomaron. El Estado ucraniano inmediatamente se mantuvo en estado de alerta y movilizó a su personal para iniciar la defensa de su red computacional. El pueblo ucraniano tenía miedo de que los efectos observados fueran irreversibles y que les podrían afectar directamente a su forma de vida. Incluso, las empresas afectadas, dentro y fuera del país, tuvieron que tomar decisiones de emergencia para evitar pérdidas económicas severas y para reestablecer sus operaciones por completo.

El análisis de los efectos producidos de un ciberataque es esencial al momento de estudiar este tipo de eventos, pues nos pueden dar una idea de las intenciones detrás de él y el posible actor que lo creó. En este capítulo se analizarán los efectos ocasionados por NotPetya en los equipos computacionales de las múltiples víctimas que sufrieron infecciones, así como los efectos que se desencadenaron por las afectaciones generadas. También, se identificarán los alcances de estos efectos y la manera en que pueden ser consideradas nuevas formas de poder.

3.1. Los efectos de NotPetya en Ucrania

Con el lanzamiento de NotPetya a través de los servidores de Linkos Group, el actor detrás del ciberataque se aseguró de que las primeras víctimas se encontraran localizadas dentro de Ucrania, generando afectaciones severas al funcionamiento de la sociedad dentro del territorio

ucraniano. Rápidamente aquellas instituciones que tenían instalado M.E.Doc en equipos con una versión desactualizada de Windows comenzaron a sufrir el impacto del ciberataque.

Similar a lo que había ocurrido anteriormente con WannaCry, los equipos infectados habían sido encriptados y no se podía hacer nada para recuperar su control, pero a diferencia de ese programa malicioso, NotPetya no infectaba a usuarios al azar a través del internet, sino que, en primer lugar, se dirigió a equipos muy específicos dentro del territorio ucraniano, para posteriormente obtener de ellos las credenciales necesarias para propagarse a otros equipos dentro de la misma red a la que estaban conectados, y posteriormente a otras redes, sin ningún tipo de oposición (Greenberg 2019).

Diversas dependencias gubernamentales esenciales fueron las primeras en ser infectadas, siendo el sector financiero uno de los primeros en presentar severas afectaciones en su funcionamiento. Múltiples bancos con oficinas en todo el país comenzaron a reportar fallas en sus equipos, provocando interrupciones en su servicio, al no poder monitorear todos los movimientos bancarios que se estaban realizando. También informaron que sus sistemas se encontraban bloqueados, por lo que tomaron la decisión de cerrar sus sucursales de manera temporal, y cesar todo tipo de operaciones bancarias para evitar mayores dificultades en el restablecimiento de sus servicios (Greenberg 2019).

Oleksiy Yasinsky, analista informático y jefe del Centro de Investigación y Laboratorios de ISSP, fue uno de los primeros en responder al incidente. En múltiples entrevistas ha compartido su experiencia en los primeros momentos del ciberataque, particularmente al llegar a las instalaciones de Oschadbank, el banco de ahorros de Ucrania y una de las instituciones financieras más importantes del país (Rhysider 2019).

Al llegar al edificio, Yasinsky narra que los empleados de la institución se mantenían en algo que describe como un “estado de shock”, al no saber cómo reaccionar a un ciberataque de tal

magnitud. La gran mayoría de computadoras de Oschadbank se había apagado simultáneamente dejando sin ningún equipo computacional al personal, imposibilitando su trabajo. Al reiniciarse, los equipos mostraban un anuncio exigiendo 300 dólares en Bitcoin para su rescate, y se había restringido el acceso a todos los archivos, dejando a la institución bancaria sin acceso a su propia información (Rhysider 2019).

Tras las investigaciones y el análisis forense realizado por ISSP, se determinó que el 90% de las computadoras de Oschadbank habían sido infectadas, incluyendo equipos de sucursales bancarias, cajeros automáticos, sistemas de cobro con tarjeta y equipos de oficina utilizados para labores administrativas. También se descubrió que el programa malicioso se había propagado a toda la red de la institución financiera en cuestión de segundos hasta saturar el sistema y desactivarlo por completo (Rhysider 2019).

Las afectaciones en Oschadbank se replicaron en diversas instituciones financieras en Ucrania. Múltiples bancos, la mayoría con oficinas centrales en Kiev, comenzaron a cerrar sus sucursales y a negar la atención a sus clientes por no poder proveer su servicio. El caos comenzó a propagarse rápidamente, ya que los ucranianos sólo contaban con el dinero en efectivo que poseían en ese momento, no podían utilizar sus tarjetas, ni otros sistemas de pago, para comprar bienes y no podían retirar dinero adicional. Sólo algunos cajeros se salvaron de las infecciones y continuaban con servicio normal, pero sus fondos se agotaban rápidamente o presentaban largas filas de clientes, por lo que la gente comenzó a preguntarse si contaba con el dinero suficiente para realizar sus actividades normales, o incluso, para comprar bienes necesarios como comida o medicinas (Greenberg 2019).

ISSP continuó con sus investigaciones, intentando responder rápidamente al incidente, y realizando mayores descubrimientos. La empresa detectó que NotPetya no poseía ninguna herramienta de desencriptación, y que, aún después de realizar el pago del rescate de $300 USD,

los archivos permanecían bloqueados, sin existir alguna forma conocida para recuperarlos, por lo que recomendó a las víctimas abstenerse de pagar el rescate (Greenberg 2019).

Por esta razón, se comenzó a creer que el anuncio que solicitaba el pago del rescate era tan sólo una estrategia para aparentar ser un incidente creado por cibercriminales comunes y no un ataque dirigido específicamente a un Estado. Una estrategia utilizada para confundir a los analistas y para ocultar el verdadero origen del ciberataque. Incluso se sugirió que NotPetya podía haber sido diseñado no sólo para afectar a Ucrania, sino también para implementar una táctica de "tierra quemada digital", con el propósito de obtener inteligencia, destruir información, imposibilitar la recolección de pruebas e, incluso, plantear nuevos programas e información oculta para ataques posteriores (Greenberg 2019).

Otro de los sectores que fue impactado rápidamente fue el energético, el cual ya había sido blanco de ciberataques en el pasado y tenía más experiencia en la respuesta de este tipo de incidentes. Se detectó que, nuevamente, se intentó dañar la red eléctrica de Ucrania para interrumpir la distribución de energía al país, y, en esta ocasión, la Planta Nuclear de Chernóbil también había sufrido infecciones.

Ukrenergo, la empresa de distribución eléctrica atacada anteriormente con Industroyer, aplicó un protocolo de acción diseñado para responder inmediatamente a ciberataques. Pocos minutos después de haber detectado la primera infección en uno de sus equipos, la empresa ordenó que se desconectaran todas sus redes y se apagaran las computadoras de sus instalaciones. Sólo algunas de sus computadoras fueron afectadas por NotPetya, y gracias a la desconexión de sus dispositivos, pudieron evitar la propagación del programa malicioso en el resto de sus instalaciones (Borys 2017).

A pesar de haber protegido a tiempo la gran mayoría de sus computadoras, los trabajadores no tuvieron la infraestructura digital con la que cuentan habitualmente, por lo que tuvieron que

realizar sus tareas sin bases de datos y sistemas, dificultando y retrasando el proceso. La red eléctrica no sufrió ningún daño destacado y no se reportó la interrupción de luz eléctrica en ninguna parte del país. Sin embargo, en algunas subestaciones tuvieron que continuar trabajando sin el apoyo de equipos digitales, y algunas afectaciones secundarias menores tardaron hasta 10 días en ser reparadas (Borys 2017).

En la Central Nuclear de Chernóbil, se presenciaron las mismas escenas que fueron observadas en Oschadbank: Múltiples computadoras del sitio se comenzaron a apagar y a reiniciar mostrando el mensaje de encriptación. Siete minutos después de la primera infección, se ordenó apagar y desconectar de la red más de mil equipos esparcidos en toda la central, con el objetivo de evitar daños críticos a los sistemas utilizados para el monitoreo de desecho radioactivo (Greenberg 2019; BBC Mundo 2017).

El personal de la central tuvo que realizar sus actividades sin sensores digitales por la desconexión de equipos, por lo que los niveles de radiación tuvieron que ser vigilados continuamente de manera manual para evitar accidentes. La planta logró mantener el funcionamiento de sus actividades y no se reportaron fallas mayores, por lo que, tras asegurar el correcto funcionamiento de sus equipos después del ciberataque, pudieron reanudar sus actividades normales (Greenberg 2019; BBC Mundo 2017).

El sistema de salud fue otro de los sectores afectados por NotPetya, y presentaron retrasos y fallas en los equipos utilizados para diagnóstico. Similar a lo ocurrido con el NHS en Reino Unido tras WannaCry, diversos hospitales de Ucrania comenzaron a reportar que aquellos equipos con el sistema de Windows se encontraban encriptados, y que sólo podían utilizar los dispositivos con Linux o IBM que se encontraban aislados de la red.

El Ministerio de Salud se vio fuertemente afectado al perder el acceso al sistema encargado de diversas actividades esenciales, no sólo para el funcionamiento de clínicas y hospitales, sino

también para la sociedad ucraniana en general. Este sistema es el encargado de administrar la nómina de los trabajadores, el inventario de farmacias y la base de datos nacional de donantes y receptores de órganos, por lo que todas estas funciones tuvieron que ser pausadas mientras se restablecía el funcionamiento de equipos (Greenberg 2019).

En diversos hospitales, únicamente los equipos de la empresa General Electric funcionaban con normalidad, por ejemplo, los equipos de imagen por resonancia magnética, por lo que, por un tiempo, se continuaron utilizando con normalidad, sin embargo, en diversas clínicas se optó por apagar los equipos como medida preventiva, reduciendo sus actividades (Borys 2017).

La ley ucraniana establece que todas las instituciones pertenecientes al sistema de salud deben mantener la información de sus pacientes por al menos 25 años, por lo que la pérdida de esta información provocaría serios problemas legales a aquellas instituciones afectadas. A pesar de que algunos equipos presenciaron infecciones, los hospitales contaron con respaldos suficientes y sólo en casos muy particulares se perdió información detallada de los pacientes. El proceso de captura de datos de nuevos pacientes y la asignación de tratamientos fue más lento de lo usual, dificultando también la actualización de los expedientes, puesto que el personal optó por hacer estos procedimientos de manera manual. La Clínica Boris, la más grande de Kiev, reportó daños a sus equipos y fallas en sus sistemas que alcanzaron los $60,000 USD (Borys 2017).

Otro de los servicios que presentó importantes afectaciones fue el servicio postal. La oficina central de correos localizada en Kiev fue la primera en ser infectada, por lo que se ordenó la desconexión de las computadoras en el resto de las oficinas postales del país, inmovilizando el correo en toda Ucrania. En este país, el servicio postal es responsable no sólo del envío de correos, sino también de transferencias de dinero, suscripciones de periódico y el pago de pensiones a 4.5 millones de personas. Ninguna de estas actividades se pudo realizar hasta reestablecer el sistema,

incluyendo el pago de los 74,000 empleados del sistema postal y la gestión de los 2,500 camiones de reparto (Greenberg 2019).

Las consecuencias inmediatas en equipos de cómputo provocadas por NotPetya fueron importantes, pero el programa malicioso también ocasionó otro tipo de efectos sin la necesidad de propagarse por completo. En el caso de las oficinas de gobierno, se presentaron infecciones rápidamente, así como sucedió en el resto del país, pero se tomaron medidas para intentar contrarrestar el programa malicioso, las cuales ocasionaron otro tipo de afectaciones.

Tras haber observado la rapidez y efectividad con la que contaba NotPetya, se emitió una orden de emergencia por parte del gobierno de Ucrania para desconectar inmediatamente las computadoras de todas las dependencias con el propósito de evitar la propagación del programa malicioso. Los departamentos de Tecnologías de la Información de cada dependencia se apresuraron a realizar respaldos rápidos a la información que no había sido guardada y se planteaban si era realmente necesario desconectar todos sus equipos (Greenberg 2019).

Después de unas horas, existían dos panoramas en las instituciones gubernamentales: O habían seguido las instrucciones y se encontraban desconectadas del sistema sin poder trabajar con sus equipos, o no las habían seguido, y habían sido infectadas y sus equipos encriptados, cualquiera de las dos opciones había provocado que las dependencias gubernamentales no pudieran funcionar de manera normal, y en algunos casos, se encontraran completamente deshabilitadas (Greenberg 2019).

Volodymyr Rmelyan, el entonces ministro de infraestructura de Ucrania, afirmó que el gobierno estaba prácticamente "muerto", la red nacional de transporte paralizada, y que NotPetya había infectado el Sistema de Emisión de Boletos del transporte público, el Aeropuerto Borypsil de Kiev y el Sistema Nacional de Ferrocarriles, deteniendo el movimiento de los ciudadanos en todo el país (Greenberg 2019).

Al final del día, las afectaciones ocasionadas por NotPetya reportadas abarcaron 4 hospitales en Kiev, 6 compañías de energía, 2 aeropuertos, 22 bancos, cajeros automáticos, sistemas de pago con tarjeta y la inhabilitación de prácticamente la totalidad del gobierno federal. En el aspecto privado, ISSP estima que 300 compañías fueron afectadas dentro del territorio ucraniano y que aproximadamente el 10% de las computadoras en todo el país habían sido impactadas. La red ucraniana se encontraba deshecha tras el ataque (Greenberg 2019).

Las investigaciones de ISSP también arrojaron que el gran peligro de NotPetya provenía de la gran velocidad que poseía para infectar a sus víctimas. La red de Oschadbank tardó sólo 45 segundos en caer, e infecciones en otras instituciones fueron a una velocidad similar, o menor. Una gran parte del sistema de transporte urbano de Ucrania fue infectada en aproximadamente 60 segundos, y Ukrenergo, sufrió infecciones en un tiempo similar (Greenberg 2019).

Después de dos días de continuas infecciones, la policía de Ucrania reportó la recepción de denuncias de más de 1,500 instituciones a lo largo de todo el país, provenientes de organizaciones privadas y agencias gubernamentales. Por lo anterior, Ucrania inició un proceso penal contra los creadores de NotPetya por violar el artículo 361 del Código Penal de Ucrania, que prohíbe "la interferencia no autorizada con el funcionamiento de dispositivos electrónicos (computadoras), sistemas automatizados, redes informáticas o redes de telecomunicaciones" (Ukrayinska Pravda 2017).

La División de Delitos Cibernéticos del Ministerio del Interior de Ucrania fue la encargada de realizar la investigación oficial correspondiente tras el ciberataque y se esperaba que sus análisis llevaran a la captura de los autores del ciberataque. Señalaron que era posible que los atacantes hubieran robado información financiera confidencial de las empresas, antes de encriptar su información, por lo que existía la posibilidad de aumentar las cifras de daños económicos. Tampoco

descartaban ciberataques posteriores como complemento a NotPetya y se mantuvieron alerta en caso de otro incidente (Borys 2017).

3.2. Los efectos de NotPetya en el mundo

NotPetya fue dirigido específicamente a Ucrania, pero, como se ha mencionado anteriormente, debido a la interconexión del mundo y la rápida propagación del programa malicioso, en cuestión de horas cruzó fronteras hasta obtener un alcance global. Al infectar los equipos de empresas multinacionales con oficinas en Ucrania, NotPetya logró propagarse en las redes de esas instituciones, hasta esparcirse a oficinas de esas mismas empresas localizadas en otros países.

Se comenzaron a reportar infecciones en compañías que aparentemente no tenían una relación directa, y que se encontraban localizadas en países, o incluso continentes, diferentes. Las afectaciones provenían desde grandes empresas multinacionales de logística, hasta clínicas y hospitales regionales, y sus efectos fueron diversos.

La gigantesca naviera danesa, A.P. Moller-Maersk, reportó que presentaba fallas para procesar el cargamento y los pedidos en diversos puertos alrededor del mundo, mientras que la empresa de paquetería TNT Express, subsidiaria de FedEx, alertó que sus oficinas también presentaban infecciones. El mismo día de su lanzamiento, reportes de NotPetya comenzaron a surgir de otros países, como Argentina, Australia, Dinamarca, Corea del Sur, Francia, Estados Unidos e, incluso, Rusia, demostrando que el programa malicioso ya había obtenido un alcance mundial (Auchard, Stubbs, y Prentice 2017; Henley y Solon 2017).

Haciendo otra analogía a los contagios de virus biológicos, Nicolas Duvinage, jefe de la unidad de delitos digitales de las fuerzas armadas de Francia, afirmó que los reportes de NotPetya eran similares a una "epidemia de gripe en invierno", por la rapidez de su propagación y la cantidad

de casos detectados, agregando que el riesgo de nuevos ciberataques en los meses siguientes se había incrementado súbitamente por el evento (Henley y Solon 2017).

Agencias de inteligencia y de ciberseguridad de los países afectados, así como las empresas infectadas comenzaron a tomar medidas como respuesta al ciberataque. La empresa alemana de correo electrónico, Posteo, comunicó que los creadores de NotPetya solicitaban que se enviara la confirmación del pago de $300 USD para el rescate de los equipos a una cuenta de su empresa, por lo que habían tomado la decisión de eliminarla, considerándolo un uso inadecuado de sus servicios. Esto ocasionó que no existiría una manera de ponerse en contacto con los hackers y que tampoco existiera manera de obtener la clave de desencriptación, si es que existía (Henley y Solon 2017).

Por otro lado, algunas víctimas decidieron pagar el rescate de sus equipos con la esperanza de restablecer su funcionamiento inmediatamente y continuar con sus actividades. Una compañía surcoreana confirmó haber pagado $1,000,000 USD para recuperar su información, pero que, a pesar de haber transferido los fondos, no recuperó sus datos y continuó con las mismas afectaciones (BBC Mundo 2017).

En Estados Unidos, los hospitales afectados decidieron suspender la atención de sus pacientes, especialmente aquellos que tenían una cirugía programada. En Australia, diversas empresas tuvieron que detener producción, destacando una fábrica de chocolates perteneciente a Cadbury, localizada en Tasmania, cuyas afectaciones también detuvieron la distribución de sus productos a nivel internacional. Mientras que la farmacéutica Merck detuvo la producción y distribución de productos médicos, incluyendo vacunas importantes (Greenberg 2019).

Las víctimas y sus afectaciones fueron diversas en todo el mundo, y si bien no se puede identificar la secuencia que NotPetya siguió para alcanzar a sus víctimas, se puede decir que una de las empresas que fue determinante en la expansión global del programa malicioso fue Maersk. La naviera danesa no sólo cuenta con oficinas en todo el mundo, sino que también mantiene

relaciones con otras empresas para proveer sus servicios. Además, sus oficinas en Kiev y Odesa, son esenciales para el control y la logística de transporte en la región, especialmente a través del Mar Negro.

A continuación, se describirá el impacto de NotPetya en las víctimas detectadas fuera del territorio ucraniano y los efectos producidos por el programa malicioso en las instalaciones afectadas.

3.2.1. Maersk

Maersk es una de las compañías de logística más importantes de todo el mundo al ser responsable del transporte de bienes y servicios esenciales para la cadena de suministros global. Posee oficinas en múltiples países y son responsables de al menos una quinta parte de los cargamentos transportados en todo el mundo. El 27 de junio de 2017, fueron una de las principales empresas afectadas por NotPetya y se cree que fueron la causante principal de que el programa malicioso lograra trasladarse a otros países (Greenberg 2018).

Maersk posee dos oficinas en Ucrania, las oficinas centrales regionales ubicadas en la capital, Kiev, y oficinas adicionales en el puerto de Odesa, enfocadas en el transporte de mercancías en el Mar Negro. Horas después de las primeras infecciones detectadas en Ucrania, la red de Maersk se mantenía a salvo y no se habían detectado afectaciones en ningún servicio. Sin embargo, una sola computadora cambiaría el panorama (Rhysider 2019; Greenberg 2018).

Días previos al ciberataque, un ejecutivo financiero de Maersk solicitó al equipo de TI de la empresa instalar M.E.Doc en una única computadora en las oficinas de Odesa para poder cumplir con sus obligaciones fiscales ante Ucrania. Una sola computadora fue lo único que NotPetya necesitó para propagarse a toda la red de Maersk y en cuestión de horas inhabilitar la cadena de transporte global de la empresa (Greenberg 2018).

Por la tarde de ese mismo día, las computadoras de las oficinas de Odesa comenzaron a apagarse rápidamente. Al inicio, los equipos de TI habían considerado que sólo se trataba de alguna actualización de rutina que había sido programada a horas inusuales, pero al percatarse de la cantidad de equipos que se encontraban en la misma situación, comenzaron a sospechar que se trataba de una situación más compleja (Greenberg 2019).

A partir de esa única computadora con M.E.Doc, NotPetya había logrado propagarse a todos los equipos en las oficinas de Odesa, posteriormente propagándose a las oficinas de Kiev para finalmente infectar a otras oficinas de Maersk en otros países a través de su propia red. Minutos después de los reportes de las primeras infecciones en las oficinas de Odesa, se comenzaron a recibir informes de la misma situación en oficinas de otros países (Cramon, Frederiksen, y Glismand 2017; Greenberg 2018).

El hecho de que un único dispositivo haya sido suficiente para propagarse a la red entera de Maersk, demuestra lo difícil que es la defensa en el ciberespacio, ya que, mientras los que buscan proteger a sus equipos en contra de las diferentes amenazas existentes deben de ser exitosos todo el tiempo, los creadores de NotPetya sólo necesitaron ser exitosos una vez para provocar sus efectos devastadores.

La protección computacional se complica aún más si consideramos que muy rara vez los dispositivos electrónicos se encuentran completamente aislados o desconectados de las redes, por lo que un programa malicioso tan infeccioso, como lo fue NotPetya, puede rápidamente acceder a otros equipos sin ninguna oposición. Los expertos especializados en seguridad informática deben de prestar atención no sólo a los potenciales riesgos externos por los que sus equipos pueden resultar severamente afectados, sino también, de las diferentes rutas de acceso que los programas maliciosos pueden obtener para alcanzar sus objetivos, incluso utilizando las mismas conexiones de una red que es considerada “segura”.

Este fue el caso de las oficinas de Maersk en Ucrania, en el que la infección exitosa en la computadora localizada en Odesa fue como una "puerta de entrada" a las redes de la empresa, la cual favoreció a que NotPetya pudiera continuar su propagación a través de las redes internas, llegando a equipos que no poseían M.E.Doc y expandiéndose a una gran velocidad.

Al observar el rápido desarrollo de la situación, el equipo de TI de la oficina central de Maersk en Copenhague ordenó la inmediata desconexión de la red global de la compañía. Se desconectaron computadoras personales, dispositivos electrónicos de los puertos y teléfonos celulares. Tras dos horas de trabajo, Maersk había desactivado toda su red y se encontraba sin el respaldo de su infraestructura digital, ocasionando severas consecuencias logísticas y económicas (Cramon, Frederiksen, y Glismand 2017; Greenberg 2018).

El programa malicioso afectó principalmente los sistemas esenciales de tres empresas subsidiarias de Maersk cruciales para la logística y dedicadas al transporte de cargamentos a través de contenedores por barco y tráiler: Maersk Line[45], el Sistema de Terminales APM[46] y Damco[47]. (Cramon, Frederiksen, y Glismand 2017).

Maersk sufrió graves afectaciones, principalmente en su área logística y de transporte, que ocurrieron, en primer lugar, por las infecciones de NotPetya en los equipos que componen las redes de estas empresas, pero, posteriormente, también por la desconexión ordenada por las oficinas centrales de Copenhague. Así como en diversos ciberataques, en ocasiones, las afectaciones pueden ser por efectos secundarios que no habían sido visualizados al momento de diseñar el programa malicioso con el que se realiza, y, en este caso, la desconexión de la red global de Maersk fue un efecto secundario, que a su vez provocó otras afectaciones importantes en sus operaciones, que

[45] Empresa subsidiaria de Maersk especializada en el transporte de mercancía por contenedores.
[46] Empresa perteneciente a Maersk especializada en operaciones portuarias.
[47] Damco era la empresa dedicada al área de logística de Maersk especializada en la cadena de suministro y el transporte de carga a nivel internacional de la empresa. Se disolvió en 2020.

fueron desde retrasos, hasta cancelación de órdenes de envío, que pudieron no haber sido planeadas desde un inicio.

Para que las terminales portuarias de Maersk puedan realizar su trabajo, es necesario su sistema digital, que se encarga de administrar y organizar la carga y descarga de contenedores de los buques que arriban al lugar. Las terminales APM, son responsables de "leer" el contenido de los contenedores para determinar la logística de carga y descarga de buques y tráileres y trazar la ruta que debe seguir la mercancía (Greenberg 2019; Rhysider 2019).

Sin estos sistemas, los puertos se encontraban completamente paralizados; los barcos no podían ser descargados sin saber hacia dónde dirigir su cargamento, por lo que después de unas horas, diversos puertos comenzaron a presentar largas filas de barcos esperando su turno de atracar. Mientras que, por tierra, largas filas de tráileres que llegaban a kilómetros de distancia esperaban su turno para poder entrar a los puertos y recibir sus cargamentos. El tráfico se encontraba detenido por mar y por tierra (Greenberg 2019; Rhysider 2019).

Los bienes que son transportados a través de Maersk son diversos y abarcan todo tipo de industrias, y el cierre de sus puertos ocasionó complicaciones imprevistas que tuvieron que ser resueltas lo más pronto posible para evitar mayores problemas. Aquellos contenedores que poseían cámaras frigoríficas en su interior, tuvieron que ser transportados inmediatamente a almacenes locales en donde pudieran ser conectados para evitar la pérdida de los productos, mientras que otros contenedores de la cadena de suministros, vitales para la producción en fábricas localizadas en otros países, tuvieron que buscar alternativas de transporte, ya sea en otras compañías navieras, o a través de transporte aéreo, ambas con tarifas elevadas por la premura de la situación (Cramon, Frederiksen, y Glismand 2017; Greenberg 2018; Rhysider 2019).

Como podemos observar en los párrafos anteriores, los efectos que un programa malicioso puede provocar directamente a sus víctimas son graves, pero aquellos que puede generar de manera

indirecta, pueden desencadenar consecuencias igual, o más severas. Debido a que los nuevos programas maliciosos son cada vez más sofisticados, existe el riesgo de que generen efectos no deseados en sus víctimas, por lo que el riesgo de que un incidente de este tipo se salga de control es cada vez mayor.

En el caso de Maersk, se considera que los efectos secundarios que impactaron directamente a sus clientes no habían sido previstos, y sus afectaciones tuvieron que ser resueltas improvisando soluciones al momento, puesto que las largas filas de buques y tráileres comenzaban a afectar no sólo a la empresa naviera, sino también al tráfico marítimo y terrestre de los puertos afectados.

De las 76 terminales portuarias de Maersk a nivel mundial, 17 se encontraban totalmente inoperativas, mientras que el resto presentaba serias afectaciones. La empresa reportó que no se perdió el control de ningún buque, y que mantenía continua comunicación con aquellos que aún se mantenían en ruta a su destino, asegurando que no detectaban ningún cambio que generara peligro a su tripulación y que ningún trabajador se encontraba en riesgo. También informó que sus sitios web, dedicados a la recepción y programación de pedidos, se encontraban totalmente inhabilitados, así como diversos servicios de correo electrónico, por lo que se encontraban utilizando medios de comunicación alternativos para recibir solicitudes de sus clientes (Cramon, Frederiksen, y Glismand 2017; Pownall 2019).

De las diferentes divisiones de Maersk, únicamente las dedicadas a la explotación petrolera y al sector energético no fueron perjudicadas y mantuvieron operaciones normales. También informaron que NotPetya únicamente había dañado el funcionamiento de sus equipos, pero que ninguna información confidencial había sido perdida o expuesta a terceros (Cramon, Frederiksen, y Glismand 2017; Pownall 2019).

Para el restablecimiento de la red de Maersk, se tuvo que recuperar un disco duro localizado en las oficinas de la empresa en Ghana, el cual poseía el respaldo de la información necesaria para

reconstruir los sistemas perdidos. Debido a un corte de electricidad ocasionado por un apagón en la ciudad, las oficinas de Maersk en Ghana fueron las únicas en no ser infectadas por el programa malicioso, pues los equipos se encontraban apagados al momento de que NotPetya intentaba esparcirse, y se conservó la información crucial para el restablecimiento de los servicios de la compañía (Greenberg 2018).

La empresa detectó aproximadamente 50,000 equipos infectados con NotPetya, además de miles de aplicaciones y servidores localizados en 600 ubicaciones en 130 países. Tras la recuperación del disco duro de Ghana, Maersk comenzó la reconstrucción de su infraestructura tecnológica, restableciendo todas las funciones esenciales en 10 días, pero logrando la restauración completa de todos sus servicios hasta después de 3 meses del ciberataque (Palmer 2019).

Si bien fue por casualidad, la información recuperada de las oficinas de Ghana nos demuestra la importancia de mantener los equipos esenciales para el funcionamiento de redes siempre actualizados, respaldados, y si es posible, aislados, para evitar la pérdida total de información. Con las actualizaciones se pueden evitar infecciones de programas dañinos para el equipo, mientras que el respaldo de la información, como en el caso de Maersk, es crucial para el restablecimiento de infraestructura digital en caso de pérdida total o parcial de la misma.

Como se mencionó anteriormente, es raro que existan dispositivos que se encuentren totalmente aislados de las redes, puesto que dificultaría su actualización y sus funcionalidades serían reducidas. Sin embargo, en este tipo de casos, sistemas completamente aislados del internet y de otro tipo de redes pueden eludir por completo una infección, y la información almacenada en ellos puede ser utilizada para la fase de recuperación tras el incidente. Debido al apagón en la ciudad, Maersk logró aislar un dispositivo de manera accidental, que funcionó como pieza clave para el restablecimiento de su red global.

La recuperación de la infraestructura tecnológica de Maersk fue relativamente rápida, y tras lograrlo, sus servicios se lograron restablecer fácilmente. Sin embargo, la empresa reportó una pérdida de aproximadamente $300,000,000 USD por pérdida de ingresos, costos del restablecimiento de la red global, y costos adicionales de operación. Además, implementando una nueva política de prevención de ciber incidentes, la empresa invirtió en el fortalecimiento de ciberseguridad y la compra de un seguro en caso de ciberataques, incrementando los gastos realizados (Frederiksen, Glismand, y Olsen 2018).

La infección de Maersk fue una pieza clave para la propagación mundial de NotPetya, puesto que una empresa multinacional de logística de tal tamaño, se encuentra en constante contacto y comunicación con todo tipo de empresas alrededor del mundo. Fue una especie de "puente" para el programa malicioso, ya que, lo que comenzó con la infección de un solo equipo una sola oficina de la empresa localizada en Ucrania, desencadenó una oleada de infecciones en múltiples países en cuestión de segundos.

Este fenómeno demuestra, una vez más, la estrecha interconexión del mundo, y cómo un caso dirigido específicamente a una víctima en particular, que, inició como un evento "aislado" en Ucrania, provocó consecuencias globales en cuestión de segundos. Hoy en día, no importa el lugar en el que un programa malicioso tan sofisticado y agresivo, como lo es NotPetya, es lanzado, puesto que la rápida difusión de información, el internet, y el alcance global de las redes computacionales facilitan que cualquier incidente pueda afectar a un gran número de personas a nivel global, aun cuando ésta no sea la intención original.

El caso de Maersk también resalta la importancia de mantener siempre actualizados los programas de seguridad informática de las computadoras. En el campo de la ciberseguridad actual, la ofensiva posee una ventaja muy grande sobre la defensa. Mientras los hackers se encuentran en constante evolución, creando nuevas herramientas tecnológicas y diseñando nuevos programas

maliciosos, aquellos dedicados a la protección de equipos no pueden trabajar a la misma velocidad al tener que prestar atención a todas las amenazas presentes en la red.

Mientras que los atacantes necesitan ser exitosos una sola vez para cumplir sus objetivos, la defensa de los equipos digitales tiene que ser exitosa siempre. Maersk fue uno de los miles de empresas que, por omisiones en la seguridad de sus sistemas o por la falta de actualización de sus equipos, cayeron víctimas de NotPetya, por lo que es importante destacar que, para evitar eventos de tal magnitud, la cultura de prevención es crucial.

3.2.2. Víctimas en Rusia

Como se ha mencionado anteriormente, diversos gobiernos han señalado a Rusia como el más probable responsable de NotPetya, a través del grupo *Sandworm*. Si los señalamientos son correctos, se podría decir que el programa malicioso fue mucho más infeccioso de lo planeado, saliendo incluso del control de sus creadores, pues existieron víctimas importantes con pérdidas económicas destacadas dentro del territorio ruso, que podrían haber sido involuntarias.

Rosneft, la empresa petrolera más grande de Rusia y una de las más importantes a nivel mundial por el volumen de crudo que producen, confirmó que sus sistemas computacionales habían sido afectados el mismo día en el que comenzó el ciberataque. Afirmaron que los servidores de la compañía habían sufrido "un poderoso ataque de hackeo" que ocasionó "serias consecuencias" en los sistemas utilizados para la producción de petróleo (Stubbs y Polityuk 2017).

La empresa estatal no dio detalles sobre cuáles eran las afectaciones específicas a sus sistemas, mencionando únicamente “indisponibilidad de sistemas y servicios informáticos básicos”, sin embargo, afirmaron que se encontraban trabajando para evitar la propagación del programa malicioso y reestablecer rápidamente los equipos afectados. También expresaron que la producción y refinería de petróleo no se había detenido, pues comenzaron a utilizar un sistema de

producción alternativo para evitar mayores infecciones dentro de sus instalaciones y evitar cualquier incidente adicional (Rosneft 2018, 237; Stubbs y Polityuk 2017).

Los sitios web de Rosneft se mantuvieron inaccesibles por varias horas y se presentaron interrupciones en la infraestructura digital de la compañía. Sin embargo, no se reportaron pérdidas económicas considerables, sólo afectaciones en los procesos de producción, que pudieron ser evitados momentáneamente mientras se reparaban las fallas en los sistemas (Stubbs y Polityuk 2017).

La empresa multinacional británica dedicada a la siderurgia y minería, Evraz, fue otra de las empresas mayormente afectadas dentro del territorio ruso. Si bien la empresa posee sus oficinas centrales en Reino Unido, la gran mayoría de sus operaciones se desarrollan dentro de Rusia, siendo propiedad de Román Abramóvich, multimillonario ruso. La empresa reportó que sus sistemas de TI se encontraban infectados también y que presentaban serias afectaciones en toda su infraestructura digital, sin especificar cuales (Sahuquillo y Domínguez 2017; Stubbs y Polityuk 2017).

Confirmaron que NotPetya había logrado propagarse a sus sistemas, y que habían puesto en marcha un plan para recuperarlos. También aseguraron que la información expuesta había sido recuperada y que los datos financieros confidenciales, tanto de la empresa, como la de sus clientes, habían sido protegidos. No detectaron ninguna exfiltración de información por parte de los atacantes y no reportaron pérdidas económicas significativas (Abramov et al. 2018).

Debido a los efectos del programa malicioso, Evraz diseñó e implementó inmediatamente un plan de mitigación de riesgos de ciberseguridad, reconociendo que los riesgos a través del ciberespacio eran comunes y prioritarios para la empresa. El plan incluía un cronograma de implementación de medidas de prevención que se llevarían a cabo durante el 2017 y 2018, que sería actualizado continuamente para incluir nuevas amenazas y evaluar el progreso del

fortalecimiento de la seguridad informática, con el propósito de que no volviera a suceder algo como lo ocurrido con NotPetya (Abramov et al. 2018).

Rosneft y Evraz son tan sólo dos de los miles de víctimas detectadas dentro del país, que abarcan desde computadoras personales y pequeñas empresas, hasta redes de grandes instituciones. Dentro de los afectados también se encontraron la empresa de tecnología médica, Invitro, y diversas instituciones financieras, como Sberbank, que presentaron afectaciones muy similares a las observadas en las instituciones financieras ucranianas, obligándolos a suspender sus actividades hasta restaurar las redes infectadas (Greenberg 2019).

Rusia fue uno de los países más afectados por NotPetya, sufriendo aproximadamente el 30% de las infecciones globales iniciales (Palazuelos 2017). Si bien la geografía deja de ser un factor crucial en el ciberespacio, es importante recalcar que la cercanía de ambos territorios genera continuas interacciones importantes para el funcionamiento de ambas sociedades, principalmente a través del comercio. Esto genera a su vez, interacciones a través del ciberespacio, por ejemplo, a través de redes sociales o de comunicación por medios digitales, lo que ocasionó las numerosas infecciones dentro del territorio ruso; incluso cuando éstas no hubieran sido intencionales, era inevitable sufrir "daños colaterales" por la interdependencia de ambas naciones.

3.2.3. Merck

Merck es una empresa multinacional alemana dedicada al diseño y fabricación de productos farmacéuticos y biotecnológicos enfocados principalmente para su uso en el campo de la medicina. Entre sus actividades se encuentran la comercialización de vacunas, la investigación científica en torno a diagnóstico y tratamiento de enfermedades, diseño de productos químicos, y el impulso a la alta tecnología. Esta empresa se destaca a nivel internacional por su presencia en múltiples países

y por sus productos de tratamiento que abarcan una gran parte del mercado mundial (Merck KGaA 2018).

Merck fue otra de las principales víctimas impactadas por NotPetya, pues el mismo día del lanzamiento del programa malicioso comenzaron a presenciarse efectos muy similares a los observados en Maersk y en las miles de organizaciones víctimas del ciberataque. Las computadoras en las oficinas de Merck comenzaron a mostrar el fatídico mensaje de NotPetya en el que se notificaba de la encriptación de los archivos del usuario y el posible rescate de estos a cambio de 300 dólares en Bitcoin. La disrupción de sus equipos ocasionó la interrupción súbita de las actividades de la empresa, incluyendo la manufactura de sus productos, el área de investigación y operaciones de venta (Voreacos, Chiglinsky, y Griffin 2019).

Se estima que el programa malicioso logró infectar a más de 30,000 equipos computacionales dentro de la empresa, incluyendo laptops y computadoras de escritorio, así como 7,500 servidores utilizados para mantener la infraestructura tecnológica global de Merck. Las divisiones de venta y manufactura de la empresa fueron las impactadas con mayor gravedad, al tener que detener todas sus actividades por tiempos prolongados y en algunos casos particulares, perdiendo información equivalente a hasta 15 años de investigación (Voreacos, Chiglinsky, y Griffin 2019).

NotPetya se esparció con tal velocidad y efectividad dentro de las instalaciones de Merck, que, incluso, provocó severas afectaciones a las instalaciones dedicadas a la producción de "Gardasil 9", la principal vacuna utilizada en contra del Virus del Papiloma Humano (VPH) uno de los principales causantes del cáncer cervicouterino. La empresa tomó la decisión de solicitar un préstamo de 1.8 millones de dosis a la Reserva Nacional Pediátrica de los Estados Unidos para cubrir la demanda de las vacunas y evitar mayores complicaciones a la salud de pacientes. El valor

de este préstamo fue de $240 millones de dólares y Merck tardó 18 meses en devolver las vacunas que había recibido[48] (Greenberg 2019; Voreacos, Chiglinsky, y Griffin 2019)

El ciberataque dañó con tal magnitud la infraestructura de Merck, que, por dos semanas, en algunas oficinas de la empresa, se suspendieron actividades por completo para restaurar las redes dañadas por NotPetya. En el aspecto económico, Merck fue la víctima con mayores pérdidas económicas en el mundo, reportando una pérdida de $870 millones de dólares, ocasionada principalmente por el alto a su producción y la inhabilidad de cubrir la demanda de sus productos (Greenberg 2018; Coburn, Leverett, y Woo 2019).

El caso específico de Merck es muy importante a resaltar por dos principales razones; La primera, los daños económicos que reportó son sumamente elevados, y demuestran, una vez más, el poder que se puede ejercer a través del ciberespacio. En cuestión de horas y con un solo programa informático, se logró perjudicar a una empresa multinacional de gran tamaño, quizás inintencionalmente, pero generando efectos observables en el mundo real y afectando a una víctima, aun cuando no era el principal objetivo.

Y, en segundo lugar, genera un importante debate acerca del significado de definiciones utilizadas tradicionalmente en torno al conflicto y la manera en que éstas han evolucionado con la aparición del ciberespacio y sus efectos a nivel internacional.

Merck consideró que las pérdidas económicas sufridas por NotPetya tenían que ser cubiertas por su póliza de seguro, pues en el contrato se especificaba la cobertura de hasta $1,750,000,000 USD por daños o destrucción a su infraestructura computacional. Sin embargo, las aseguradoras de Merck rechazaron el reclamo al considerar que NotPetya había sido una acción

[48] El Centro para el Control y Prevención de Enfermedades de los Estados Unidos confirmó el préstamo y afirmó que no afectaba la disponibilidad de medicamentos, pues la reserva tenía dosis suficientes para cubrir los 18 meses que necesitó Merck para reponer el préstamo (Voreacos, Chiglinsky, y Griffin 2019).

"hostil" o "bélica" que los excluía de pagar la póliza[49] (Wheeler y Wolff 2022; Voreacos, Chiglinsky, y Griffin 2019).

Las aseguradoras argumentaron que el Departamento de Defensa de los Estados Unidos había determinado en años anteriores que el sabotaje computacional podría ser considerado un acto de guerra, y que, por ende, los efectos producidos por NotPetya eran consideradas consecuencias inevitables de un conflicto bélico, excluyéndolos de cubrir la póliza. Si bien es cierto que el Departamento de Defensa de Estados Unidos considera al sabotaje como un posible acto de guerra, no específica con profundidad el tipo de acciones que pueden ser consideradas como sabotaje, manteniendo el término ampliamente ambiguo y dejando a interpretación diversos aspectos, por lo que Merck decidió demandar a sus aseguradoras, como Allianz SE y American International Group, por incumplimiento de contrato y reclamando $1,300,000,000 USD en pérdidas (Wheeler y Wolff 2022; Voreacos, Chiglinsky, y Griffin 2019).

Merck argumentó ante la corte que NotPetya no podía ser considerado un evento hostil, ya que los ciberataques no eran "actos tradicionales de guerra", por lo que las aseguradoras no podían ser excluidas del pago de la póliza. Por otro lado, tanto el gobierno ucraniano, como el gobierno estadunidense, determinaron que NotPetya había sido creado y lanzado por las fuerzas armadas de Rusia con intenciones geopolíticas claras, por lo que las aseguradoras utilizaron estos señalamientos para declarar que, al haber sido una acción implementada por el ejército de un Estado, el programa malicioso y sus efectos eran claramente producto de un conflicto entre dos países, y que, incluso si Merck no se encontraba localizada en ninguno de estos territorios, sus

[49] La Exclusión de Guerra es una disposición utilizada ampliamente por las aseguradoras en sus pólizas, en la que se establece que en caso de pérdidas provocadas por acciones bélicas o guerras, la empresa se deslinda del pago y la reposición de los daños.

afectaciones habían sido ocasionadas directamente por el combate, aún si este era a través del ciberespacio, y que por lo tanto no tenían obligaciones a reparar los daños (Wheeler y Wolff 2022).

La demanda se extendió por años, hasta que, en diciembre de 2021, un juez de Nueva Jersey falló en favor de Merck determinando que los eventos generados por NotPetya no podían ser considerados por las aseguradoras para evitar el pago de la póliza. El juez declaró que no se utilizaron a las fuerzas armadas en un conflicto directo, y que el derecho de exclusión de pago de las aseguradoras era únicamente aplicable en el caso de "formas tradicionales de guerra", por lo que Merck debía de ser remunerado por completo debido al incumplimiento de contrato (Wheeler y Wolff 2022).

La demanda realizada por Merck hacia sus aseguradoras despierta un debate en torno al significado de múltiples términos cuyos significados tendrían que ser ampliados tras el surgimiento del ciberespacio. NotPetya es considerado por algunos expertos como un acto de guerra al haber sido ocasionado muy probablemente por un actor estatal y al haber sido dirigido a otro Estado con la finalidad de perseguir intereses nacionales.

Sin embargo, en la actualidad los ciberataques son tan comunes y varían tanto en sus objetivos, métodos y víctimas que otros expertos argumentan que la ciberguerra no puede existir por sí sola, y que para que actos dañinos a través del ciberespacio puedan ser considerados como actos bélicos, deben de realizarse con el uso de la fuerza en otros dominios de combate.

A pesar de que el ciberespacio depende de la infraestructura física que lo hace funcionar, la gran mayoría de las actividades realizadas a través de él ocurren en un “mundo virtual” que no puede ser observado. Los programas informáticos carecen de características físicas, no pueden ser manipulados y no pueden existir sin toda la infraestructura digital que hace funcionar este “mundo virtual”. La naturaleza abstracta del ciberespacio ha presentado dificultades para asignar características específicas a los fenómenos presentes en él. Sin embargo, a pesar de que estas

acciones no son detectadas más que en un mundo virtual, sus efectos son observados en el mundo real.

No podemos observar la manera en que NotPetya se fue propagando en cada una de los equipos de Merck ni la manera en que los fue encriptando, pero podemos percibir claramente las consecuencias provocadas por estas acciones ocurridas en un mundo virtual. En el mundo "real", los trabajadores de Merck dejaron de trabajar al no poder realizar sus actividades, cadenas de producción se detuvieron por no poseer información localizada en equipos particulares y la manufactura de vacunas tuvo que ser detenida.

Es cierto que los ciberataques no han ocasionado víctimas mortales, así como lo han hecho armas "tradicionales" de guerra, como un cañón o un cohete, pero la realidad es que el ciberespacio ha provocado que ya nada sea "tradicional". Las interacciones globales se han transformado y evolucionado para utilizar esta herramienta. Anteriormente tampoco se utilizaban tarjetas de crédito y débito, pero el uso de dinero digital es ya una realidad en el mundo, y su existencia e influencia en la economía global no puede ser negada. Las redes sociales y los foros de internet han provocado el surgimiento de subculturas urbanas que abarcan individuos de diferentes países y orígenes, y que han comenzado a generar sentido de pertenencia a estos grupos que poseen intereses en común, por lo que podemos decir que las interacciones a través del ciberespacio han transformado también a la sociedad.

Incluso la política ha sido transformada con el ciberespacio, ahora es común observar reuniones entre mandatarios a través de videollamadas y que información gubernamental oficial sea compartida a través del internet. El ciberespacio ha transformado el mundo y sus interacciones, por lo que es natural que transforme también otros aspectos, incluyendo el conflicto moderno, y claro, el poder.

Las afectaciones sufridas por Merck si pueden ser considerados como efectos de un acto bélico, pero no fueron acciones dirigidas hacia ella. Merck fue tan sólo una víctima inintencional de un acto dirigido a otra nación, que, por la interconectividad del mundo, resultó en consecuencias no premeditadas en sus equipos.

3.2.5. Otras empresas afectadas

Las instituciones dentro del territorio de Ucrania fueron las más afectadas, seguidas por empresas multinacionales, como Maersk y Merck, y empresas localizadas en Rusia, pero NotPetya logró esparcirse a miles de víctimas alrededor del mundo, incluyendo instituciones con una amplia variedad de tamaños, capacidades y localizaciones. A continuación, se mencionarán algunos ejemplos para representar una imagen más completa del impacto global del programa malicioso.

3.2.5.1. Nuance

Estados Unidos fue otro de los países con un número importante de víctimas detectadas, y en su caso particular, se presentaron condiciones muy similares a las observadas en el NHS del Reino Unido durante el ciberataque de WannaCry y a lo sucedido en la Clínica Boris de Kiev durante NotPetya: Los equipos médicos dentro de los hospitales fueron severamente afectados, afectando directamente la atención de pacientes.

En el caso de NotPetya, el virus no infectó directamente las instalaciones de hospitales y clínicas, sino que afectó a una empresa especializada en el desarrollo de programas informáticos de reconocimiento de voz e inteligencia artificial llamada "Nuance". Esta empresa provee servicios de transcripción y digitalización de registros médicos utilizados ampliamente por hospitales alrededor del mundo para agilizar la construcción y el almacenamiento del historial médico de sus pacientes (Greenberg 2018; Crosignani, Macchiavelli, y Silva 2020).

Así como sucedió con múltiples empresas, las primeras infecciones de Nuance comenzaron en Ucrania, y posteriormente se propagaron a sus oficinas internacionales hasta llegar a las oficinas centrales localizadas en Massachussets, Estados Unidos. Las afectaciones en sus sistemas provocaron pérdidas económicas importantes: $68,000,000 USD en pérdida de ingresos y $24,000,000 USD en costo de reparaciones, dando un total de $92,000,000 USD (Greenberg 2018; Crosignani, Macchiavelli, y Silva 2020).

Comparando las pérdidas económicas de Nuance con las de otras empresas multinacionales, la cifra resulta notoriamente menor, sin embargo, el caso de esta empresa sobresale por los efectos producidos en el mundo real que impactaron directa e inmediatamente a miles de pacientes, particularmente en Estados Unidos.

Los sistemas de Nuance funcionan de tal manera que los médicos pueden dictar instrucciones sobre los cuidados que deben ser brindados a sus pacientes a los dispositivos de la empresa, para que los cambios sean aplicados en tiempo real y el historial médico se mantenga actualizado continuamente a través de la nube. Los doctores de diversos hospitales comenzaron a reportar que los cambios que habían dictado no se reflejaban en los sistemas de Nuance, por lo que se tuvieron que retrasar o cancelar diversos procedimientos médicos, como cirugías, trasplantes de órganos y tratamientos (Greenberg 2019).

Al final del 27 de junio de 2017, Nuance tenía millones de instrucciones sin actualizar y sus sistemas se encontraban saturados por los cambios sin procesar. En algunos casos, como el del Sistema de Salud Heritage Valley[50], NotPetya se había propagado de los equipos de Nuance a los sistemas internos de los hospitales, por lo que las afectaciones fueron mayores y el número de actividades que podían ser realizadas se redujeron drásticamente (Greenberg 2019).

[50] El Sistema de Salud de Heritage Valley es una red de hospitales localizados en Pensilvania, Estados Unidos.

La empresa confirmó que las severas afectaciones en sus dispositivos habían sido ocasionadas por NotPetya, y recalcó que ninguna información confidencial había sido expuesta, haciendo énfasis en que la información privada de cada uno de sus pacientes, incluyendo datos biométricos, se mantenía a salvo. Expresaron que el programa malicioso había sido diseñado con intenciones destructivas, y que no encontraron ningún indicio de exfiltración de datos personales (Nuance Communications Inc. 2017).

Nuance también informó que, como medida precautoria, decidieron desconectar su red global y desactivar todos sus servicios, especialmente aquellos conectados a través de la nube, para evitar la propagación y el aumento de infecciones en su red, por lo que presenciaron afectaciones adicionales a las provocadas por el programa malicioso. Inmediatamente implementaron medidas para el diagnóstico de sus equipos y la reparación de aquellos que habían sido impactados por NotPetya, pero existió información que había sido perdida permanentemente, como el historial de diversos pacientes, que tuvieron que ser reconstruidos por completo (Nuance Communications Inc. 2017).

El caso de Nuance prueba la estrecha relación entre el mundo virtual y el real, puesto que un ciberataque de mayor gravedad dirigido a dispositivos electrónicos utilizados por instituciones de salud, pude provocar daños a la salud de diversos pacientes, o incluso en casos muy severos, la muerte. Existen hospitales que mantienen una gran dependencia a este tipo de equipos para brindarle tratamiento a sus pacientes, y la falta de información o la corrupción de datos puede ser causante de serios accidentes que dañen la salud de las personas.

Afortunadamente, durante las infecciones de NotPetya, no se presenciaron este tipo de consecuencias en los hospitales afectados, pero demuestra la importancia que la seguridad informática debe tener hoy en día en todos los sistemas, sobre todo en aquellas redes de las que la sociedad depende en mayor medida.

3.2.5.2. FedEx y TNT Express

FedEx, así como Maersk, es una compañía dedicada a la logística y transporte de bienes a nivel internacional. La empresa multinacional estadunidense sufrió interrupciones súbitas en el área de entrega y ventas tras haber sido infectada por NotPetya a través de una computadora localizada en Ucrania que poseía M.E.Doc. El transporte de mercancías tuvo que ser detenido temporalmente en algunas sucursales de FedEx, particularmente las localizadas en Europa y se retrasó la entrega de paquetes a nivel internacional (Palmer 2017).

El mayor impacto de NotPetya en FedEx fue a través de TNT Express, una empresa neerlandesa de entrega y logística que adquirió en 2016 y que se encontraba en un proceso de integración. El programa malicioso afectó severamente a la mayoría de computadoras que formaban parte de la red de TNT Express, dificultando en gran medida las operaciones realizadas por la empresa, que depende de la información de sus equipos para determinar la ruta de la mercancía transportada (Nash, Castellanos, y Janofsky 2018).

Debido a las infecciones, las actividades de FedEx y TNT Express fueron retrasadas o canceladas, particularmente en Europa, en donde se presenció el mayor número de equipos dañados dentro de la empresa. Los directivos de FedEx informaron que ninguna información confidencial había sido exfiltrada y que el programa malicioso no se había propagado a los sistemas esenciales a nivel internacional, por lo que no había riesgo de que ocurrieran mayores daños (BBC News 2017a).

A pesar de las afectaciones y las complicaciones de no poseer la infraestructura digital, FedEx y TNT Express decidieron no suspender actividades y continuar con sus operaciones manualmente. En algunos casos, se optó por utilizar medios de comunicación alternativos, como el servicio de mensajería instantánea, WhatsApp, para acordar detalles con los clientes, y el proceso

de empaquetado y envío de productos fue más lento de lo usual. Existieron errores en las operaciones, como el envío de productos diferentes, el envío a destinatarios equivocados o el retraso de hasta meses de paquetes, pero la empresa asegura que fueron afectaciones menores y que mantener sus actividades había sido la decisión correcta (BBC News 2017a).

FedEx reportó la pérdida de $400,000,000 USD causada principalmente por la pérdida de ganancias en TNT Express debido a NotPetya. Las empresas tardaron meses en restaurar por completo sus sistemas, y por al menos dos meses, TNT Express continuó realizando sus operaciones manualmente y sus clientes sufrieron de retrasos importantes en sus envíos (Crosignani, Macchiavelli, y Silva 2020).

3.2.5.3. Reckitt Benckiser

Reckitt Benckiser fue otra de las empresas que sufrieron mayores afectaciones por NotPetya al tener que detener su producción en múltiples fábricas. La empresa multinacional británica dedicada a la producción y venta de productos de consumo también detuvo la entrega de bienes a clientes de diversos países y dejó de recibir pedidos por un periodo de tiempo prolongado (Monaghan 2017).

El programa malicioso logró infectar un gran número de computadoras con el sistema operativo Windows, las cuales se encontraban encargadas del área de producción, el manejo de pedidos y la logística, por lo que las actividades en algunas instalaciones tuvieron que ser suspendidas por completo hasta la recuperación de la información perdida (Monaghan 2017).

La empresa reportó una pérdida económica de $100,000,000 USD, ocasionada por el alto a la producción, la falta de ingresos y el costo de reparación de los equipos afectados. Esta pérdida representó el 1% de sus ganancias anuales, mostrando una seria disminución de su proyección de

crecimiento para ese periodo (Crosignani, Macchiavelli, y Silva 2020; Reckitt Benckiser Group plc R 2018).

Como consecuencia directa del ciberataque, Reckitt Benckiser cambió su política de ciberseguridad, impartiendo capacitaciones a todo su personal e invirtiendo en la actualización de equipos y en la creación de plataformas para la detección y corrección de vulnerabilidades en sus sistemas (Reckitt Benckiser Group plc R 2018).

3.2.5.4. Mondelez

La empresa estadunidense dedicada a la producción de confitería y aperitivos, Mondelez International, fue otra de las víctimas de NotPetya al presentar interrupciones súbitas en su producción. En fábricas de la compañía, las computadoras de sus empleados se congelaron súbitamente, el servicio de correo electrónico se inhabilitó y el acceso a los archivos de la red empresarial se restringió. Sus programas informáticos dedicados a la logística también se detuvieron por completo, evitando que se pudieran rastrear envíos y confirmar pedidos (Satariano y Periroth 2019).

La cadena de suministros de la empresa de alimentos se vio duramente interrumpida por el programa malicioso, generando importantes afectaciones económicas. Se detuvo la producción en diversas fábricas de la compañía, destacando las dedicadas a la producción de barras de chocolate localizadas en Australia, Alemania y Suiza. La reparación de la infraestructura digital de Mondelez y el análisis forense requerido tras el ciberataque tuvo un costo de $84,000,000 USD, que, sumados a la pérdida de ventas, da un total de $180,000,000 USD perdidos por NotPetya (Crosignani, Macchiavelli, y Silva 2020).

Mondelez International sufrió un caso similar a lo ocurrido con Merck, pues sus aseguradoras se negaron a pagar los costos en los que incurrieron por el programa malicioso,

argumentando que la compañía había sido impactada por un acto bélico. Mondelez demandó a Zurich Insurance Group por incumplimiento de contrato, y se espera que la resolución del caso sea muy similar a lo ocurrido con Merck (Satariano y Periroth 2019).

Estas fueron algunas de las compañías con mayores pérdidas económicas por NotPetya, si bien fueron las más afectadas, no fueron las únicas, pues el programa malicioso logro propagarse a múltiples instituciones en todo el mundo. A continuación, se presenta una tabla, exponiendo algunas de las principales víctimas y sus pérdidas económicas.

Tabla 3
Principales víctimas de NotPetya y sus pérdidas económicas.

Nombre	**Descripción**	**Afectaciones principales por NotPetya**	**Pérdidas (En dólares)**
Merck	Empresa farmacéutica estadounidense.	Interrupción de la manufactura de la vacuna contra el VPH.	$870,000,000
FedEx/TNT Express	Empresa de logística estadunidense y su filial neerlandesa.	Interrupción de sus operaciones en Europa.	$400,000,000
Saint-Gobain	Empresa francesa de materiales de construcción.	Caída de sus sistemas.	$384,000,000
Maersk	Empresa danesa de logística y transporte de mercancía.	Afectaciones en el servicio de sus 76 terminales portuarias, inhabilitando 17.	$300,000,000
Mondelez International	Empresa estadunidense de alimentos.	Interrupción de la producción y logística.	$180,000,000
Reckitt Benckiser	Empresa británica de productos de consumo.	Interrupción de la producción y logística.	$100,000,000
Nuance	Desarrolladora de programas informáticos estadunidense.	Inhabilitación de dispositivos médicos en hospitales.	$92,000,000
Beiersdorf	Empresa alemana de productos de consumo.	Interrupción de la producción y logística.	$43,000,000
WPP	Agencia británica de publicidad.	Inhabilitación de la red empresarial.	$15,000,000
Evraz	Empresa rusa de acero y minería.	Afectaciones en sistemas informáticos.	No Reportado
Oschadbank	Banco estatal de Ucrania.	Cierre de sucursales y afectaciones en cajeros automáticos.	No Reportado
Rosneft	Compañía estatal rusa de petróleo.	Afectaciones en sus servidores sin impactar la producción petrolera.	No Reportado
Aeropuerto de Borýspil	Aeropuerto Internacional de Ucrania en la región de Kiev.	Retraso y cancelación de vuelos.	No Aplica

Ukrenergo	Compañía estatal ucraniana de energía.	Afectaciones en servidores sus servidores sin impactar la red eléctrica.	No Aplica
Planta de Nuclear de Chernóbil	Parte de la generación de energía de Ucrania.	Inhabilitación de los sensores digitales de radiación.	No Aplica
Instituciones Gubernamentales de Ucrania	Oficinas del gobierno de Ucrania.	Cese completo de las actividades.	No Aplica

NotPetya logró propagarse a instituciones localizadas en todo el mundo generando diferentes afectaciones en cada una de ellas y provocando pérdidas millonarias a grandes empresas multinacionales. *Tabla de elaboración propia con información de Greenberg (2018), Coburn, Leverett, y Woo (2019) y Crosignani, Macchiavelli, y Silva (2020).*

3.3. NotPetya como expresión de poder

3.3.1. Identidad del autor de NotPetya

La identificación del autor de un ciberataque siempre es una labor complicada que requiere de análisis forenses complejos y que en ocasiones pueden arrojar resultados inexactos debido a la facilidad que poseen los hackers de encubrir las evidencias de sus actos. Sin embargo, en incidentes que provocan consecuencias de gran magnitud, como lo fue NotPetya, los líderes de diversas naciones se apresuran a señalar a quienes creen como el más probable autor del ciberataque, especialmente cuando existen intereses geopolíticos de por medio.

En ocasiones, existen ciertas características particulares que pueden sustentar la teoría de que cierto actor se encuentra detrás de un incidente, pero a pesar de aparentemente poseer todas las pruebas necesarias para acusar a algún individuo, grupo, o incluso Estado, las acusaciones se pueden negar muy fácilmente, sin generar implicaciones de gravedad en el Sistema Internacional.

NotPetya fue un ciberataque de gran magnitud, no sólo por el severo impacto económico que generó en el mundo y el gran número de víctimas que infectó en múltiples países en todos los continentes, sino por las propiedades que poseía, que hicieron creer a múltiples expertos que, no sólo un actor estatal se encontraba tras la creación del programa malicioso, sino que pudieron incluso señalar muy específicamente a los posibles responsables.

Como se mencionó en el capítulo anterior, uno de los datos más importantes a resaltar es la víctima principal que sufrió las primeras infecciones: Ucrania. Debido a la complejidad del programa malicioso y la manera en que fue lanzado, se afirma que NotPetya fue creado con claras intenciones de impactar a un Estado específico. Si bien, el impacto fue mucho mayor y existió un mayor número de víctimas localizadas fuera del territorio ucraniano, el programa malicioso logró prácticamente inhabilitar toda la red informática del país y afectar de gravedad el funcionamiento normal de la sociedad.

Asimismo, otras características muy relevantes del caso, como el lanzamiento del programa malicioso a través de un programa informático utilizado por un gran número de usuarios, M.E.Doc, hasta el día seleccionado para comenzar el ciberataque, un día feriado en el que un número importante de la población se ausentaría a trabajar, denotan que NotPetya fue diseñado muy claramente para dañar a Ucrania de manera rápida y efectiva, y que su lanzamiento fue planeado estratégicamente en un día específico en el que las acciones de respuesta al programa malicioso serían complicadas de realizar, aumentando la peligrosidad del programa malicioso.

Este tipo de particularidades en el incidente, hacen creer que el creador de NotPetya es un actor con importantes intereses en Ucrania. Si bien, existe una amplia gama de actores que participan activamente en ciberamenazas en el mundo, no se detectan intereses económicos para afirmar que el actor es un cibercriminal buscando enriquecerse con la información obtenida; no se difundió ningún mensaje o ideología, descartando la posibilidad de que fueran hacktivistas o grupos extremistas; y la creación del virus requirió de profundos conocimientos técnicos y una amplia disponibilidad de recursos económicos y tiempo, por lo que sería muy poco probable que actores internos o buscadores de emociones se encontraran detrás del incidente.

Descartando las otras posibilidades y notando que NotPetya fue utilizado para mermar las capacidades informáticas de Ucrania, que existen intereses geopolíticos en la región y que se pudo

haber obtenido inteligencia por la información encriptada y ventajas estratégicas durante su lanzamiento, se cree que un actor estatal, o un grupo de hackers patrocinados por un Estado, es quien creó el programa malicioso.

A pesar de que existe una barrera de acceso muy baja a la información a través del ciberespacio y que hay una gran diversidad de actores participando en el Sistema Internacional actual, el Estado continúa siendo el principal actor dominante por los recursos y capacidades con los que cuenta, por lo que no es de extrañar que se recurran a este tipo de estrategias para cumplir con objetivos e intereses nacionales.

Debido a los intereses en la región y la historia de confrontamientos entre ambos países, diversas autoridades señalaron al gobierno de Rusia como el responsable de NotPetya, utilizando el programa malicioso como una herramienta para "sancionar" a Ucrania y presionar al país con motivo del conflicto que había estallado por la anexión de la península de Crimea al territorio ruso. También considerándolo como una estrategia de "advertencia" de lo que sucedería posteriormente y como preparativos de posibles ciberataques posteriores.

El gobierno ucraniano fue el primero en señalar a su vecino del este como el culpable, afirmando que, tras las investigaciones realizadas e información obtenida gracias a la cooperación de diversas compañías de seguridad informática internacionales, habían descubierto que el grupo detrás de NotPetya era el mismo que había atacado en años anteriores a Ucrania, señalando específicamente el programa malicioso BlackEnergy. Afirmaron que las características de NotPetya y su relación con incidentes anteriores eran pruebas de la clara participación de los servicios de inteligencia de Rusia (Polityuk 2017).

También declararon que las intenciones de NotPetya nunca fueron la obtención de ganancias económicas, sino que buscaban destruir información importante e interrumpir súbitamente el funcionamiento de instituciones públicas y privadas en Ucrania con intenciones de

provocar pánico en la sociedad. Aseguraron que Rusia muy probablemente había subestimado las capacidades de propagación que NotPetya tenía, por lo que se había salido de su control y por ello se habían generado tantas infecciones a nivel global (Polityuk 2017).

El gobierno de Reino Unido fue otro de los países en señalar a Rusia como el responsable de NotPetya, pues el entonces secretario de defensa, Gavin Williamson, aseguró que el gobierno ruso había utilizado el programa malicioso para "socavar la democracia" y afectar directamente a Ucrania, así como lo había hecho anteriormente, dañando a los sectores financiero, de energía y gubernamental del país con otros ciberataques (Marsh 2018).

Williamson también declaró que el incidente marcaba una nueva era de guerra, y que se estaba presenciando un nuevo tipo de dominio estratégico, en el que existía una "mezcla destructiva y mortal" del poder militar convencional y las operaciones a través del ciberespacio con programas maliciosos (Marsh 2018).

Por último, Estados Unidos fue otro Estado que responsabilizó públicamente a Rusia por el incidente; medida que resultó sorpresiva debido a la poca disposición de atribuir ciberataques anteriormente por parte del gobierno estadunidense y por las intenciones de acercamiento al gobierno ruso por parte de la administración de Donald Trump. La secretaria de prensa de la Casa Blanca, Sarah Sanders, emitió un comunicado en el que se culpabilizaba a Rusia por NotPetya expresando que el programa se había extendido a todo el mundo provocando miles de millones de dólares en daños en Europa, Asia y América (Volz y Young 2018).

Asimismo, Sanders también afirmó que el incidente era una parte más de los esfuerzos del gobierno ruso para "desestabilizar Ucrania" y que se observaba claramente su participación activa en el conflicto. Calificó lo sucedido con NotPetya como un ciberataque "imprudente e indiscriminado" y afirmó que existirían severas consecuencias internacionales (Volz y Young 2018).

Mientras el comunicado por parte del gobierno de Ucrania fue emitido tan sólo unos días después del ciberataque, los gobiernos estadounidense y británico esperaron varios meses para realizar sus declaraciones y respaldar la postura ucraniana, y tras su publicación, otros países comenzaron a emitir comunicados similares de sus agencias de inteligencia también señalando a Rusia como el culpable de atacar Ucrania, como Canadá, Australia y Nueva Zelanda (Greenberg 2019).

A pesar de que diversos países respaldaron la postura ucraniana y afirmar que existirían severas consecuencias y sanciones importantes en contra de Rusia por lo sucedido, éstas nunca ocurrieron. Algunos expertos afirman que quizá es resultado de la posibilidad de que no estén completamente seguros de que el Kremlin se encuentre detrás del incidente, mientras que otros afirman que no tomaron represalias para tener la posibilidad de crear programas maliciosos de similares capacidades sin sufrir consecuencias, o incluso, para evitar también ser impactados por ciberataques con efectos similares (Greenberg 2019).

La posibilidad de que las fuerzas de inteligencia del ejército ruso se encuentren detrás de NotPetya, o incluso el grupo Sandworm, es muy probable debido a las continuas tensiones en la relación bilateral entre ambos países. En un sistema internacional en el que la guerra se utiliza con el fin de obtener poder, la ciberguerra es también una herramienta para alcanzarlo y ejercerlo.

Si retomamos la visión de Waltz, podemos recordar que la razón de la interminable búsqueda del poder por parte del Estado es para asegurar la supervivencia del mismo, por lo que podríamos decir que los intereses de Rusia en Ucrania siguen esta visión, al considerar el territorio ucraniano vital para su existencia. Desde la anexión de la península de Crimea y las continuas tensiones y conflictos entre ambos territorios, Rusia busca obtener y ejercer este poder para asegurar su supervivencia y la disminución de algunas amenazas consideradas por su gobierno, que pueden ir desde la expansión de la Organización del Tratado del Atlántico Norte al Este de Europa,

hasta la expansión de la influencia estadunidense en territorios vecinos, similar a lo observado durante la Guerra Fría.

También es importante recordar lo mencionado por Nye, quien refiere que los actores utilizan el poder, y en este caso particular el basado en recursos informáticos, para alcanzar objetivos nacionales muy específicos y transformar la conducta de otros actores. Rusia ejerció el poder haciendo uso de sus capacidades basadas en herramientas informáticas, las cuales le permitieron realizar un ciberataque de gran magnitud que le favorecía en gran medida a sus intereses territoriales en la región. De la misma manera, transformó la forma de actuar de Ucrania, que tuvo que tomar acciones de emergencia para su defensa y se mantiene en continua alerta de sufrir nuevos ataques de similar o mayor magnitud.

La visión de Wendt también puede ser aplicada al ejercicio de poder de Rusia a Ucrania en el caso particular de NotPetya, pues el autor menciona que la estructura del Sistema Internacional determina las características y roles que un actor posee. Podemos decir que Rusia mantiene su papel de potencia regional y considera tener el derecho de, no sólo buscar obtener más territorio, sino también realizar este tipo de actividades, al ser su rol en la estructura del Sistema Internacional.

NotPetya tuvo severas consecuencias económicas y sociales, pero también tuvo efectos no intencionales en el Sistema Internacional, como favorecer estratégicamente a Rusia, e indirectamente, provocar el fortalecimiento de las capacidades de defensa de Ucrania, al mantenerse alerta de nuevos posibles ciberataques.

3.3.2. Un ransomware diferente

NotPetya puede ser considerado a simple vista como un gusano de tipo *ransomware* por su manera de actuar. Como se ha explicado anteriormente, la encriptación de archivos y el bloqueo de equipos fue su método de acción principal, acompañado de una falsa promesa de devolución de

la información perdida a cambio de un rescate en Bitcoin. Sin embargo, el programa malicioso fue sumamente complejo y se utilizaron tácticas para aparentar ser otro tipo de incidente.

Un *ransomware* es creado usualmente por criminales para obtener grandes cantidades de dinero a cambio del rescate de los documentos, por lo que sus intenciones son económicas. NotPetya fue diferente, a pesar de cumplir con las características de un ransomware, la falta de un método de desencriptación de archivos, fallas en el método para transferir fondos, la escasa obtención de dinero y la existencia de intereses políticos, contribuye a considerar que el incidente no podría haber sido ocasionado por un cibercriminal común.

NotPetya fue un falso *ransomware,* que se aprovechaba de las técnicas de este tipo de programas maliciosos, pero que las utilizaba para crear disrupción, destrucción de información y pánico, en lugar de obtener dinero. Algunos expertos lo han llegado a catalogar como *wiper*[51], un tipo de programa malicioso utilizado comúnmente para borrar datos de una computadora, y debido a los efectos observados tras el incidente, se podría decir que NotPetya fue utilizado para crear la mayor cantidad de caos y desorganización posible dentro del territorio ucraniano.

Este hecho nos demuestra claramente los altos niveles de sofisticación que han alcanzado los programas maliciosos, puesto que, en la actualidad, no se puede estar completamente preparado para un ciberataque. NotPetya fue un falso *ransomware,* creado por un Estado en la búsqueda de generar disrupción y sabotaje. La combinación de estas características no sólo hace que el programa sea sumamente dañino, sino también efectivo.

Así como el poder ejercido a través del ciberespacio, NotPetya fue utilizado sin el conocimiento de sus víctimas, fue como una "causa invisible" de la que sólo se podían observar sus efectos. No podía ser detenido, porque no podía ser observado, y no se tenía conocimiento de

[51] En español podría interpretarse como "limpiador"

él. Como se mencionó anteriormente, en la ciberseguridad, aquellos dedicados a la ofensiva mantienen una ventaja estratégica muy importante, pues ¿Cómo se puede defender de algo de lo que no se tiene conocimiento?

Dentro de la informática, NotPetya abre las puertas a la creación de nuevos programas maliciosos que puedan combinar técnicas de pasados incidentes y de nuevas tecnologías para generar ciberataques más dañinos y peligrosos. La sofisticación puede continuar aumentando, y puede ocasionar el surgimiento un programa malicioso que llegue a infectar a un mayor número de víctimas y producir efectos de mayor gravedad en la sociedad.

En el campo de las Relaciones Internacionales, NotPetya demuestra que los programas maliciosos son una de las herramientas utilizadas en la actualidad para ejercer poder. Basta con la infección de una computadora esencial dentro de una institución para detener por completo sus actividades, o la obtención de información confidencial de un gobierno para transformar sus actitudes.

Recordemos que, según lo mencionado por Demchak, el control de la información es crucial para cumplir objetivos estratégicos a través del ciberespacio, y que la reducción de capacidades de actores rivales y el aprovechamiento de sus debilidades, puede facilitar el proceso. Para realizar un efectivo control de la información, no sólo se puede determinar el contenido de esta o regular su acceso a los usuarios, sino también se puede destruir con diferentes propósitos como evitar que la información sea expuesta y conocida por el público en general, o como estrategia de defensa, para que no sea utilizada en contra de quien quiere eliminarla.

Rusia habría buscado perseguir sus intereses nacionales utilizando el ciberespacio, ocasionando sabotaje y disrupción, mermando las capacidades de Ucrania y posiblemente eliminando cierta información que podría haber sido utilizada en su contra. Ambos factores le

brindarían grandes ventajas estratégicas, que le permitirían ejercer aún más poder sobre su vecino y determinar resultados que le favorecen.

NotPetya demuestra que el ciberespacio es una forma crucial de interacción entre los diversos actores del Sistema Internacional, que deben de desarrollar sus capacidades para poder incursionar en él. Así como han sucedido eventos con anterioridad como Stuxnet, Aurora, WannaCry y NotPetya, sucederán nuevos eventos en un futuro, que afectarán a una diversidad de actores y que tendrán que ser analizadas bajo nuevos enfoques de la disciplina.

3.3.3. NotPetya como conflicto en el dominio de la información

Anteriormente se ha mencionado la dificultad de acordar una definición sobre lo que actualmente significa "ciberguerra", puesto que nos encontramos en un periodo en el que nuevos términos deben de surgir, o algunos otros deben de ser reconsiderados, para describir la realidad del mundo. NotPetya es un caso muy importante para considerar en este debate, puesto que involucra a dos actores estatales que se han mantenido con tensiones diplomáticas y conflictos desde hace algunos años.

A pesar de que no han existido víctimas fatales a través de ciberataques, incluyendo NotPetya, es claro que existieron consecuencias visibles en el mundo real que, si hubieran sido ocasionadas por armas tradicionales u otro tipo de acciones coercitivas, podrían ser consideradas como un conflicto bélico.

NotPetya paralizó cadenas de suministros, redes de infraestructura esencial, detuvo compañías de logística, produjo daños económicos severos y afectó directa e indirectamente a la población civil de múltiples países. Si un Estado utilizara sus fuerzas armadas para provocar las consecuencias anteriormente enlistadas, se consideraría una agresión que podría detonar en un

conflicto bélico importante. El ciberespacio ha transformado esto, y debido a sus características, ha provocado que, hasta cierto grado, este tipo de acciones sean aceptadas y normalizadas.

Los actores internacionales que participan en el ciberespacio pueden realizar acciones que anteriormente hubieran generado consecuencias de gran magnitud en el Sistema Internacional. Bombardear una estación eléctrica de un país para privar a sus ciudadanos del servicio es inaceptable, pero interferir sus sistemas para desactivarlos manualmente a través de un programa malicioso y provocar el mismo efecto parece ser tolerado en mayor medida por la comunidad internacional.

El poder a través del ciberespacio es entonces una herramienta alternativa utilizada en la actualidad por los actores internacionales para alcanzar objetivos sin tener el mismo riesgo que tradicionalmente se tenía al utilizar medidas coercitivas. Y claramente podemos observar algunas de las características explicadas por Foucault, que describen en la actualidad la naturaleza del poder y su uso en el nuevo tipo de conflicto existente el quinto domino de combate. Este tipo de poder es enigmático, visible e invisible, presente y oculto, investido en todas partes y difuso, pero ejercido en mayor medida por un grupo dominante en favor de sus intereses.

A pesar de que el ciberespacio está conformado por una parte real, siendo ésta la infraestructura que lo compone, la gran mayoría de interacciones se da a través de un mundo virtual observado sólo a través de dispositivos electrónicos. A pesar de que no podemos ver una transferencia electrónica en el mundo real, las transacciones de este tipo existen y tienen un verdadero impacto en la economía internacional. Y, así como no se pueden observar los programas maliciosos utilizados para el ciberespionaje, éstos existen y son utilizados continuamente.

NotPetya no puede ser observado, y su lanzamiento fue inadvertido, pues no hay manera de detectar un programa malicioso, más que con dispositivos electrónicos. Sin embargo, no se puede negar su existencia, y a pesar de no ser observable, sus efectos y el impacto que realizó en

el mundo real pueden ser percibidos claramente. Así como con otros programas maliciosos, el poder puede ser ejercido en el combate a través del ciberespacio, con el uso de herramientas "invisibles" que desencadenan efectos "visibles".

El ciberespacio también ha provocado que ciertas características geográficas dejen de ser limitantes para la realización de actividades. Se encuentra presente en todos los lugares del planeta en donde existe una conexión a internet y hay una interacción a través de la red, sin importar su localización en el mundo. Un hacker localizado en una montaña de un país sin acceso al mar, con las herramientas y habilidades adecuadas, puede afectar a una compañía dedicada al transporte marítimo, sin la necesidad de estar presente en el lugar ni conocer el territorio en el que ésta se encuentra.

NotPetya logró provocar efectos severos en la economía de Ucrania y en su población sin la necesidad de un despliegue de tropas. El uso de un programa malicioso con las características propias de un *ransomware* facilitó que este tipo de efectos se pudieran obtener sin que existiera una intervención física en los equipos computacionales y desplegando la operación fuera de las fronteras ucranianas, donde los creadores no podían ser capturados.

Es sencillo de ejercer, porque cualquier individuo con conocimientos básicos de computación puede aprender fácilmente a desarrollar o lanzar programas maliciosos a la red. O incluso, puede realizar otro tipo de actividades a través del ciberespacio que lo favorezcan a cumplir sus objetivos. Como se ha mencionado anteriormente, existe una barrera de acceso muy baja, por lo que una gran cantidad de personas, y una variedad de actores interactúan diariamente a través del ciberespacio.

Se puede decir que el poder a través del ciberespacio no es exclusivo, puesto que anteriormente el Estado era el único que podía ejercerlo para transformar el actuar de otros Estados. En la actualidad, cualquier actor que participa en el ciberespacio tiene la posibilidad de ejercer

poder a todo tipo de actores, incluyendo los estatales. Esto se puede observar con el caso de Edward Snowden, pues un solo individuo fue capaz de exponer importantes instituciones de inteligencia y seguridad de un estado con grandes capacidades de defensa, como lo es Estados Unidos.

Sin embargo, a pesar de la baja barrera de acceso y que cualquier actor internacional pueda tener las capacidades suficientes para influir en el Sistema Internacional, la realidad es que los Estados siguen siendo los actores que poseen las herramientas, el financiamiento y la infraestructura necesaria para llevar a cabo operaciones en el ciberespacio que les permiten tener un nivel de influencia importante.

No se niega que NotPetya podría haber sido creado por otro tipo de actor internacional, como un hacker individual, un grupo de hackers o alguna empresa u organización de mediano o gran tamaño, sin embargo, hay una mínima probabilidad de que esto sea cierto, debido al nivel de complejidad del programa malicioso, y todos los requisitos que se necesitaron para desplegar el ciberataque, por lo que se puede afirmar que un Estado era el único actor internacional con los recursos necesarios para lanzarlo. Como Foucault menciona, el poder puede ser ejercido por varios actores, pero sigue siendo ejercido en mayor medida por un grupo dominante en favor de sus propios intereses.

Debido a que diversas instituciones se siguen rigiendo bajo preceptos tradicionales de conflicto y agresiones, el conflicto a través del ciberespacio no se encuentra regulado, y no existen reglas establecidas que prohibían o permitan cierto tipo de acciones. Este espacio continúa siendo una zona de experimentación, en la que los países continúan descubriendo las capacidades que pueden obtener ejerciendo su poder a través del ciberespacio. Debido a esto, los actores se permiten realizar todo tipo de acciones y continuamente crean nuevas herramientas que incrementan sus capacidades.

El poder del ciberespacio es efectivo, pues objetivos que anteriormente requerían de grandes cantidades de recursos, pueden ser logrados de una manera más rápida y precisa, utilizando menores cantidades de dinero y personal. Los programas maliciosos son tan sofisticados y adaptables, que fácilmente se pueden crear nuevos con intenciones específicas para completar los objetivos deseados. Todas estas características definen al poder en el ciberespacio, y la manera en que el conflicto a través de este se ha realizado en los últimos años. Y fácilmente, podemos observar cada una de ellas en el caso específico de NotPetya.

El poder continúa siendo enigmático y difícil de detectar, puesto que, por meses, Linkos Group fue infiltrada sin su conocimiento, y no fue hasta observar los efectos producidos en las computadoras de Ucrania y del mundo que se pudo saber de la existencia del programa malicioso. También se puede decir que, con las condiciones adecuadas, el poder puede ser muy fácil de ejercer a través del ciberespacio, pues tras las exfiltraciones de la NSA, sólo se necesitaron de conocimientos técnicos para incorporar todas las partes del programa malicioso para lanzarlo. Y, sin duda alguna, una de las características que más describen al poder y al mismo ciberespacio, es la disminución de limitantes geográficas, puesto que NotPetya fue lanzado desde las oficinas de inteligencia de Rusia sin la necesidad de que alguna persona cruzara la frontera para ocasionar los efectos que generó.

Fue un poder omnipresente, porque, a pesar de que fuera dirigido a Ucrania, el programa malicioso se propagó muy rápidamente a redes fuera del país y cada computadora relacionada de alguna manera a las que ya habían sido infectadas, podían ser vulneradas fácilmente. No tuvo regulaciones de uso porque, a pesar de que unos días antes había sucedido WannaCry y existieron efectos muy similares, no se crearon regulaciones que evitaran que un evento de la misma magnitud volviera a suceder.

Fue muy efectivo, puesto que en cuestión de horas logró desestabilizar económicamente a Ucrania y paralizar su estructura gubernamental, sin la necesidad de recurrir a medidas coercitivas. Y fue un poder ejercido no exclusivamente por el gobierno, puesto que se necesitaron de actores privados, para la obtención de algunas herramientas para la creación de NotPetya, además de que grandes empresas tuvieron que cooperar para la defensa del programa malicioso.

NotPetya y sus efectos son una muestra clara de las nuevas interacciones que existen en la actualidad a través del ciberespacio y ejemplifica claramente una de las formas en que los actores internacionales pueden ejercer el poder a nivel internacional.

Conclusiones

Desde sus inicios, el ciberespacio representó un cambio radical en la sociedad, impactando todo tipo de aspectos de la vida diaria, desde simples interacciones a través de redes sociales entre individuos, hasta al mismo Sistema Internacional y la manera en que los actores internacionales participan en él. La llegada de este dominio de información, marcó un cambio con el que las actividades "tradicionales" comenzaron a realizarse de diferente manera con ayuda de la tecnología, y, con este cambio, surgieron nuevas interacciones y nuevas realidades que hoy en día son muy comunes.

A lo largo de esta investigación se ha buscado examinar y presentar las interacciones entre actores internacionales a través del ciberespacio, que han dado pie a nuevas expresiones de poder que no fueron consideradas en las teorías clásicas de las relaciones internacionales debido a su contexto histórico. Se tomó el caso específico del ciberataque NotPetya a Ucrania, ocurrido en 2017, como un ejemplo para mostrar que las acciones realizadas a través del ciberespacio pueden provocar severas consecuencias en el mundo real, y el virtual, y que pueden influir directa e indirectamente en la conducta de un actor internacional.

NotPetya es tan sólo uno de los casos en los que se puede observar este fenómeno, sin embargo, debido al rápido avance tecnológico y la continua creación de herramientas que dotan de nuevas capacidades a los actores internacionales, son cada vez más los incidentes que ocurren, en los que se producen efectos indeseables que cruzan fronteras internacionales. El uso del ciberespacio es cada vez más común, y la sociedad depende cada vez más de él, por lo que su uso para modificar la forma de actuar de otros actores es cada vez más frecuente.

Debido a la naturaleza del ciberespacio, la gran mayoría de actividades se realizan en el mundo virtual, por lo que no pueden ser observadas tan fácilmente y, por la misma razón, el ejercicio del poder entre actores es todavía más difícil de detectar. Sin embargo, podemos considerar los efectos que un incidente ocasiona, particularmente aquellos ocasionados por programas maliciosos de gran sofisticación, y a través de ellos, podemos observar el impacto que tiene en su víctima y la manera en que ésta transforma su conducta. Los efectos indeseables que perjudican a un actor y lo obligan a modificar su conducta son una manera en la que el poder a través del ciberespacio puede ser detectado.

Para poder enfocarnos en los efectos de NotPetya y su impacto en Ucrania y las diferentes víctimas internacionales que sufrieron infecciones, se presentó primeramente el proceso llevado a cabo para su construcción y liberación, puesto que existieron múltiples eventos destacados que tuvieron que ser considerados al momento de realizar este estudio.

Asimismo, en la parte final, se realizó un enfoque más específico en las consecuencias del programa malicioso y las expresiones de poder observadas en ellas, con el propósito de confirmar o rechazar la hipótesis inicial, que expresa que las acciones dirigidas a Ucrania en el ciberataque de NotPetya son nuevas expresiones de poder al haber generado consecuencias importantes en el país, afectándolo económica, política y socialmente e influyendo directamente en su forma de

actuar. Antes de argumentar si la hipótesis puede ser aceptada, es prudente realizar algunas consideraciones finales del trabajo de investigación.

En primer lugar, se deben de realizar algunos comentarios con respecto al ejercicio del poder a través del ciberespacio, puesto que es uno de los temas centrales de esta investigación. Como se ha mencionado anteriormente, específicamente en el capítulo uno, el poder es utilizado por los actores internacionales para alcanzar sus objetivos y perseguir sus intereses. Si bien, éste puede ser obtenido y ejercido por diferentes métodos en el mundo real, en el ciberespacio, claramente la información es la principal fuente de poder.

No obstante, el ciberespacio está conformado por una infraestructura física presente en el mundo real, el verdadero valor de este dominio es la información que continuamente es transmitida a través de sus redes. Con el control de la información se puede obtener una gran influencia en los usuarios que tienen acceso a ella, ya que el permitir o denegar acceso a ciertos datos, mostrar información parcial, o sacada de contexto, o incluso modificarla para que sea afín a objetivos particulares puede determinar decisiones y conductas en individuos y actores internacionales.

Esto puede ser observado a través de las múltiples amenazas existentes en el ciberespacio, desde las operaciones de espionaje, hasta las de sabotaje, las cuáles se realizan en la búsqueda del control de la información, con el principal propósito de usarla para favorecer estratégicamente a quien la desea controlar. Aquél que logre controlar la información, puede a su vez controlar el ciberespacio.

Para lograr este control de la información es necesario obtenerlo de aquellos que lo tienen. Similar a la visión de Waltz, en la que los Estados se mantienen en constante lucha por la obtención del poder, una característica importante del ciberespacio actual es la existencia de la ciber guerra entre diferentes actores con el propósito de obtener mayor control de la información.

Como se ha expresado en algunos párrafos anteriores, una ciber guerra con víctimas mortales y destrucción física nunca ha ocurrido, sino que las operaciones en el ciberespacio se realizan en mayor medida con el propósito de apoyar operaciones en otros dominios, y no tanto como un método principal de combate. Por lo tanto, los incidentes que se observan en la actualidad tienden a funcionar como soporte a otras operaciones, y como una herramienta para obtener información que favorezca estratégicamente la realización de otro tipo de acciones.

Asimismo, podemos agregar que la ciber guerra posee un costo y duración significativamente menores en comparación al combate utilizando métodos tradicionales. A pesar de no generar daños materiales o afectar físicamente a una población, las consecuencias inmediatas de las operaciones a través del ciberespacio generan un impacto de tal magnitud, que en ocasiones no es necesario desplegar ejércitos o realizar más acciones coercitivas para alcanzar ciertos objetivos. La gran efectividad de los programas maliciosos y la facilidad con la que pueden ser utilizados, han favorecido a que los actores internacionales los utilicen para perseguir sus intereses.

Con lo descrito en los párrafos anteriores, podemos decir que, con el ciberespacio, la guerra se sigue utilizando en el Sistema Internacional con el mismo objetivo, pero a través de diferentes métodos y con nuevos actores con capacidades suficientes para participar en ella. La ciber guerra es utilizada para obtener ventajas estratégicas, mermar las capacidades de otros actores y para obtener información o, en otras palabras, para obtener poder.

A pesar de que existen cada vez más actores internacionales que incursionan en actividades en el ciberespacio y que llegan a realizar ciberataques para perseguir sus intereses, los Estados continúan siendo los que poseen mayores capacidades económicas, técnicas y de infraestructura, por lo que se han mantenido como el actor dominante en el Sistema Internacional. Este fenómeno puede ser observado claramente en la cronología compartida al inicio del capítulo dos, en la que la gran mayoría de incidentes, particularmente los ocurridos en los últimos veinte años, han sido

llevados a cabo por hackers o grupos de hackers pertenecientes a Estados o patrocinados por ellos con intereses geopolíticos muy claros, y NotPetya es uno de ellos.

El ciberataque en el que se ha enfocado esta investigación tuvo características particulares que demuestran perceptiblemente que un actor estatal se encontró detrás de él. Fue lanzado en una fecha específica elegida intencionalmente debido a la falta de personal disponible al ser un día feriado, por lo que estratégicamente, el programa malicioso tendría mayores ventajas para propagarse e infectar fácilmente a la mayor cantidad de computadoras posible dentro de Ucrania.

Además, debemos tomar en cuenta que, usualmente, una de las medidas coercitivas más efectivas son las medidas económicas, observadas a través de aranceles y bloqueos que crean presión a los Estados para modificar sus conductas. En este caso, NotPetya fue lanzado utilizando un programa computacional fiscal muy importante para la economía ucraniana, buscando lograr el mismo objetivo de dañar económicamente al país. Debido a que un gran número de computadoras pertenecientes al sector empresarial y privado de Ucrania tenía instalado M.E.Doc, el primer sector, y el más afectado, fue precisamente el económico. Y, a pesar de que grandes empresas multinacionales fueron afectadas, cuyas oficinas centrales no se encuentran en el país, la economía ucraniana fue la que sufrió mayores afectaciones, pues el 90% de todas sus empresas detectó infecciones en sus equipos.

Asimismo, la existencia de la posible "vacuna"[52] encontrada dentro de los datos de NotPetya, sugiere que sus creadores consideraron que el programa malicioso podía salirse de control, por lo que podrían haber premeditado una manera para proteger computadoras específicas, cuya encriptación no hubiera favorecido sus intereses. El utilizar un programa malicioso en la red,

[52] El archivo con nombre y terminación "perfc.dat", el cual, al estar presente en una computadora, evitaba la encriptación de archivos y mantenía el funcionamiento normal del dispositivo, evadiendo los efectos del programa malicioso.

que puede infectar a cualquier dispositivo, menos a algunos muy específicos seleccionados intencionalmente, puede brindar ventajas muy importantes.

Estas son tan sólo algunas de las características que favorecen la teoría de que un actor estatal se encontró detrás de la creación de NotPetya, y como se ha mencionado anteriormente, debido a la historia que mantiene con Ucrania y a las continuas tensiones que ha tenido con el país, Rusia se ha mantenido como el principal sospechoso y más probable culpable de crear el programa malicioso.

Hay tres factores que son importantes en el caso de NotPetya al haber sido un incidente creado por un actor estatal y que deben ser resaltados. En primer lugar, se debe de hablar del tipo de programa malicioso que fue creado. Si bien es considerado por la literatura como un *ransomware* por los efectos que ocasionó en sus víctimas, siendo la encriptación su principal método de actuar, debemos recordar que no existía ningún método para recibir dinero a cambio de la desencriptación de los datos y la recuperación la información, por lo que NotPetya no fue diseñado con intenciones de obtener ganancias económicas, sino que utilizó los métodos de un *ransomware* únicamente con la intención de generar sus efectos.

Este hecho nos lleva al segundo punto, la intención. Si obtener dinero no fue un propósito en el diseño del programa malicioso, entonces podemos decir que el sabotaje y la creación de afectaciones severas en sus víctimas fue la principal finalidad de su creación. Sin embargo, así como lo han señalado diversos expertos, existe la posibilidad de que NotPetya también haya sido liberado para recolectar información o eliminar datos específicos, ambas opciones con el propósito de facilitar otros ciberataques a futuro. Lo que sí tenemos por seguro es que el programa malicioso fue liberado, logrando su propósito: Generar disrupción de tipo cascada, provocando afectaciones importantes en los equipos de sus víctimas y generando daños importantes a la red informática ucraniana.

Sin embargo, si la intención fue crear daños y afectaciones sin recibir ganancias económicas a cambio, el tercer punto sería determinar la razón detrás de querer generar estos efectos. Y este punto confirma nuevamente la teoría de que un actor estatal es quien se encontró detrás del ciberataque, pues es el único tipo de actor internacional que se beneficia de un evento de este tipo. Considerando a Rusia como el principal sospechoso, podemos decir que los efectos producidos en Ucrania le pudieron otorgar importantes ventajas, como por ejemplo, actividades de apoyo para otro tipo de operaciones en los otros dominios de combate, el debilitamiento de las capacidades de defensa de Ucrania, afectaciones económicas para crear mayor presión sobre el país, impacto a su soberanía e independencia, obtención de superioridad en el ciberespacio, e incluso, el poner a prueba nuevas herramientas tecnológicas que nunca habían sido probadas para observar sus efectos y analizar alternativas en caso de lanzar ciberataques posteriores.

Las ventajas que pudo haber obtenido Rusia debido al ciberataque refuerzan el argumento de que fue el actor responsable de realizarlo, y que posiblemente el grupo de hackers denominado *Sandworm* es quien llevó a cabo la mayor parte de las operaciones. Sin embargo, a pesar de que el involucramiento del Estado es claro, los actores no estatales también fueron una parte muy importante del ciberataque, pues gracias a su participación, aunque de manera indirecta, fue que se difundió en mayor medida el programa malicioso.

Es importante hablar de la responsabilidad que este tipo de actores tiene en el ciberespacio, particularmente las grandes empresas, puesto que muchos servicios e infraestructura que proveen son necesarios para mantener al internet y las múltiples redes existentes en el mundo. Si bien Rusia pudo haber creado NotPetya, no lo pudo haber logrado difundir si Microsoft hubiera detectado y corregido con tiempo las vulnerabilidades de su sistema operativo. De la misma manera, si no hubieran logrado intervenir los sistemas de Linkos Group y el programa fiscal M.E.Doc, es posible que el virus no hubiera tenido la misma difusión. Igualmente, si empresas de seguridad informática

y antivirus, como Kaspersky, ESET o ISSP Global, hubieran detectado la amenaza a tiempo y hubieran alertado a las potenciales víctimas, es posible que el programa malicioso no hubiera tenido alcances mayores.

Estas empresas, sin importar su tamaño, son una parte muy importante del ciberespacio y se configuran también como actores internacionales con capacidades suficientes para ejercer poder. Ya sea de manera consciente e intencional, como Microsoft, Google, Amazon o hasta la misma Kaspersky, grandes empresas multinacionales de tecnología que están conscientes de que sus recursos, capacidades y decisiones pueden configurar el panorama del internet; O de forma inconsciente y no intencional, como Linkos Group, cuyo mercado abarca principalmente Ucrania y que subestimó la interconexión del mundo, pues no creían ser blancos de un ciberataque como NotPetya, ni ser los causantes de un gran número de infecciones a nivel global.

En cualquiera de los dos casos, las empresas deben de responsabilizarse de las acciones que realizan a través del ciberespacio, puesto que sus decisiones pueden desencadenar severas consecuencias para la seguridad informática. Para lograrlo, una opción es crear leyes y acuerdos que regulen su actividad y especifiquen claramente protocolos de protección a la información y seguridad informática, que ayuden a desincentivar este tipo de acciones y favorezcan que el ciberespacio no sea dominado por completo por las grandes empresas multinacionales de tecnología. Sin embargo, como se ha mencionado en múltiples ocasiones, debido a que la geografía ya no es una limitante, y la gran dificultad existente de que los Estados lleguen a un acuerdo en materia de ciberseguridad que sea respetado por la comunidad internacional, se cree que este escenario tiene una baja probabilidad de ocurrir.

A pesar de esta proyección, es necesario resaltar la importancia de la participación de los actores no estatales en el ciberespacio, ya que, a pesar de que el Estado continúa siendo el principal actor en el escenario internacional, sus decisiones, acciones y omisiones pueden tener

repercusiones importantes. NotPetya también puede ejemplificar esta afirmación puesto que, si analizamos atentamente el incidente, podemos notar que el ciberataque pudo ser prevenido por diferentes actores, en diferentes momentos, y que los actores no estatales jugaron un papel muy importante en la construcción y liberación del programa malicioso.

El primer actor no estatal cuyas acciones fueron determinantes para la liberación de NotPetya fue The Shadow Brokers. Este grupo de hackers privado fue esencial para la obtención de las herramientas tecnológicas necesarias para la creación del programa malicioso. Sus infiltraciones a las redes de la NSA y la divulgación a todo el público de una variedad de recursos informáticos fueron clave, no sólo para la liberación de NotPetya, sino también de otros programas maliciosos. Si las autoridades competentes hubieran tomado en serio sus amenazas y hubieran alertado a tiempo a Microsoft para lanzar los parches de actualización con mayor tiempo de anticipación, los daños generados por el programa malicioso podrían haber sido considerablemente menores.

Pero la empresa tecnológica norteamericana no puede excusarse de no haber lanzado los parches a tiempo debido a la falta de aviso por parte de la NSA, puesto que también tuvieron una oportunidad de contribuir a incrementar la defensa de los equipos computacionales con bastante tiempo de anticipación. En el caso de Microsoft, si no hubieran ignorado las advertencias de Benjamin Delpy y hubieran corregido las vulnerabilidades detectadas por el hacker francés, *Mimikatz* nunca hubiera existido, y sus capacidades de extracción de contraseñas nunca hubiera sido utilizadas.

Linkos Group es, sin duda alguna, otro de los actores no estatales que fueron clave para el incidente, puesto que sus omisiones fueron cruciales para la liberación del programa malicioso. Si la empresa no hubiera subestimado su alcance dentro y fuera de Ucrania y le hubiera dado una mayor importancia a la seguridad informática y protección de sus equipos, podrían haber detectado

la amenaza a tiempo, eliminándola y evitando que llegara a todas las víctimas a las que infectó, principalmente a sus clientes, quienes mantienen una estrecha relación con la compañía y continuamente pagan por sus servicios.

Tras las consideraciones finales mencionadas anteriormente, podemos determinar si la hipótesis inicial de este trabajo de investigación puede ser aceptada o rechazada. Para realizar este proceso, recordemos que se planteó lo siguiente:

> "Las acciones dirigidas a Ucrania a través del ciberataque NotPetya en 2017 pueden ser consideradas como nuevas expresiones de poder en el Sistema Internacional debido a que los autores del ciberataque lograron desarrollar suficientes capacidades en el ciberespacio para aprovecharse de vulnerabilidades que no habían sido detectadas, produciendo consecuencias importantes en los objetivos que atacó y afectando al país económica, política y socialmente, por lo que fue una seria amenaza para su seguridad nacional e influyó directamente en la forma de actuar de Ucrania"

En primer lugar, podemos decir que para la creación de NotPetya, Rusia sí necesitó incrementar sus capacidades y aumentar las herramientas tecnológicas que tenía a su disposición para lograr desencadenar el nivel de impacto que el programa malicioso generó. Se requirieron de varios años de prueba con otros ciberataques, dirigidos a Ucrania, para observar sus efectos y la manera en que el país respondía a ellos; también fue necesario la incorporación de elementos de otros programas maliciosos pasados y la integración de cada una de las herramientas informáticas de tal manera, que le brindaran el nivel de complejidad, sofisticación y peligrosidad necesarios para llevar a cabo una operación de tal magnitud.

En segundo lugar, podemos decir que estas capacidades desarrolladas fueron utilizadas con el principal objetivo de descubrir y aprovecharse de vulnerabilidades que no habían sido detectadas, ni por Microsoft, ni por Linkos Group, que les permitieron llevar a cabo el ciberataque de una manera efectiva y secreta. Al ser el único actor con las suficientes capacidades desarrolladas para

aprovecharse de las vulnerabilidades, y con el conocimiento de éstas, lograron realizarlo sin ninguna oposición real.

En tercer lugar, los efectos que NotPetya ocasionó en los equipos computacionales a los que infectó, tuvieron un gran impacto en sus víctimas, especialmente en aquellos pertenecientes a empresas, que sufrieron pérdidas económicas destacadas. También se debe destacar las afectaciones, particularmente el alto total de las actividades realizadas por las víctimas, ya sean los actores privados impactados por el programa malicioso, o el gobierno ucraniano y sus dependencias gubernamentales, ya que NotPetya impidió que pudieran realizar cualquier acción, en contra de su voluntad y sin manera de evitarlo.

En cuarto lugar, podemos decir que Ucrania sí fue el objetivo con mayor impacto y el que sufrió mayores consecuencias por el ciberataque. Sin embargo, podríamos cuestionar el alcance de las consecuencias que sufrió y plantearnos si realmente afectaron al país de manera social y política. Así como los actores no estatales afectados, el país sufrió de importantes pérdidas económicas y serias afectaciones que detuvieron temporalmente su economía. También podríamos argumentar que la frustración y pánico generado en el pueblo de Ucrania, sumado al miedo de sufrir ciberataques adicionales, puede ser considerado como un efecto social destacado. Pero, no se logran detectar cambios significativos en el aspecto político, puesto que el gobierno del país no sufrió ninguna transformación importante, y las tensiones que mantenía con el gobierno ruso, y los continuos choques con su vecino, no se modificaron radicalmente.

En quinto lugar, sí se puede afirmar que NotPetya fue una seria amenaza para la seguridad nacional de Ucrania, puesto que el ciberataque puso en riesgo su economía, instituciones y soberanía. También representó un riesgo importante para su independencia energética, sistema de salud y para su red de telecomunicaciones y transportes, elementos de primera necesidad para el funcionamiento del país.

Por último, podemos decir que NotPetya sí modificó directamente la forma de actuar de Ucrania, principalmente por dos razones. La primera, porque la completa inhabilitación de su sistema de gobierno provocó que el Estado se encontrara completamente paralizado, sin ninguna manera de coordinarse para defenderse o contraatacar, e incluso, sin tener las capacidades de reestablecer los sistemas averiados. En contra de su voluntad, se mantuvieron completamente sin operar.

En segundo lugar, NotPetya, y el resto de los ciberataques que ha sufrido el país, lo han orillado a reforzar sus sistemas computacionales, asignar recursos adicionales para el incremento de capacidades en el ciberespacio, mantenerse en un estado de alerta elevado y estar preparado a restaurar sus redes en caso de una nueva penetración, al ser un blanco continuo de programas maliciosos y de ciberataques. Ucrania no puede bajar la guardia, pues está consciente de que en cualquier momento puede recibir otro impacto, y al mismo tiempo, ha intentado desarrollar nuevas capacidades que le permitan estar a la ofensiva, pero esto no ha sido posible.

Cuando un país se ve forzado a mantenerse en alerta en todo momento y se mantiene recibiendo ataques continuos, de cualquier tipo, no puede perseguir sus intereses libremente y se ve forzado a únicamente desarrollar las capacidades suficientes para salva guardar su existencia, por lo que Ucrania no ha tenido otra opción, más que defenderse y recuperarse de cada ciberataque del que ha sido blanco, incluyendo y destacando NotPetya.

Por lo anterior, podemos decir que la hipótesis inicial puede ser aceptada casi en su totalidad, puesto que, a pesar de que NotPetya no generó un impacto político sobresaliente, sí generó consecuencias importantes para el país, que definitivamente ha modificado su actuar, por lo que el ciberataque puede ser considerado como una expresión de poder a través del ciberespacio.

NotPetya es uno de los casos de incidentes en el ciberespacio más destacados en la historia de la ciberseguridad y de las Relaciones Internacionales por los efectos que produjo en sus víctimas,

y es en esos efectos en los que podemos observar el poder de una mejor manera. La ciberseguridad es, sin duda alguna, uno de los temas más relevantes en múltiples áreas científicas, y las Relaciones Internacionales, al ser un área multidisciplinaria, no se queda sin ser influenciada por ella. Un fenómeno que quizás ya se encuentra tan integrado en nuestra vida diaria, debe ser estudiado con mayor profundidad a partir de diferentes enfoques para comprender nuestra realidad de una mejor manera.

Fuentes de información

Ablon, Lillian. Marzo 15 2018. *The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.* The RAND Corporation (Washington D.C.).

Abramov, Alexander, Alexander Frolov, Karl Gruber, Deborah Gudgeon, Alexander Izosimov, Sir Michael Peat, Eugene Shvidler, y Eugene Tenenbaum. 2018. *Making the World Stronger. Annual Report & Accounts 2017.* Evraz.

Albahar, M. 2019. "Cyber Attacks and Terrorism: A Twenty-First Century Conundrum." *Sci Eng Ethics* 25 (4): 993-1006. https://doi.org/10.1007/s11948-016-9864-0. https://www.ncbi.nlm.nih.gov/pubmed/28058619.

Alperovitch, Dmitri. 2011. *Revealed: Operation Shady RAT.* McAfee (Santa Clara). http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf.

Apen Soluciones Informáticas. 2022. "¿QUE ÉS EL HARDWARE?". https://apen.es/glosario-de-informatica/hardware/.

Applegate, Scott. 2015. "Cyber Conflict: Disruption and Exploitation in the Digital Age." En *Current and Emerging Trends in Cyber Operations*, editado por Frederic Lemieux. Londres: Palgrave Macmillan.

Auchard, Eric, Jack Stubbs, y Alessandra Prentice. 2017. "New computer virus spreads from Ukraine to disrupt world business." *Reuters*, 2017. https://www.reuters.com/article/us-cyber-attack-idUSKBN19I1TD.

BBC Mundo. 2017. "Un nuevo ciberataque de gran escala afecta a compañías e instituciones de todo el mundo." *BBC*, 2017. https://www.bbc.com/mundo/noticias-internacional-40422053.

BBC News. 2017a. "NotPetya cyber-attack cost TNT at least $300m." *BBC News*, 2017a. https://www.bbc.com/news/technology-41336086.

---. 2017b. "Ransomware cyber-attack: Who has been hardest hit?" *BBC News*, 15 de mayo, 2017b. Accesado el 26 de junio de 2019. https://www.bbc.com/news/world-39919249.

Bencsáth, Boldizsár, Gábor Pék, Levente Buttyán, y Márk Félegyházi. 2011. *Duqu: A Stuxnet-like malware found in the wild.* Laboratory of Cryptography and System Security (Budapest).

---. 2012. "The Cousins of Stuxnet: Duqu, Flame, and Gauss." *Future Internet* 4 (4): 971-1003.

Betz, David, y Tim Stevens. 2011. *Cyberspace and the state: toward a strategy for cyber-power*. Vol. 424 *Adelphi*. Londres: IISS, The International Institute for Strategic Studies.

Bilić, Denise Giusto. 2016. "Petya: El personal de RRHH, otra vez blanco de ransomware." Kaspersky Lab. https://www.welivesecurity.com/la-es/2016/04/18/petya-rrhh-blanco-ransomware/.

Bindra, Ashok. 2017. "Securing the Power Grid: Protecting smart grids and connected power systems from cyberatttacks." *IEEE Power Electronics Magazine* 4 (3): 20-27. https://doi.org/10.1109/MPEL.2017.2719201.

Borys, Christian. 2017. "Ukraine braces for further cyber-attacks." *BBC News*, 2017. https://www.bbc.com/news/technology-40706093.

Butterfield, Andrew, Gerard Ekembe Ngondi, y Anne Kerr. 2016. *A Dictionary of Computer Science*. 7a ed. Oxford: Oxford University Press.

Canadian Centre for Cyber Security. 2020. *An Introduction to the Cyber Threat Environment.* Government of Canada.

Centro de Innovacion y Soluciones Empresariales Tecnológicas (CISET). 2022a. "¿Qué es un cortafuegos o firewall? Definición." https://www.ciset.es/glosario/444-firewall?dt=1663171697826.

---. 2022b. "Software - Concepto y tipos de software." https://www.ciset.es/glosario/480-software-concepto-y-tipos.

Cherepanov, Anton. 2017. "Industroyer: la mayor amenaza para sistemas de control industrial desde Stuxnet." ESET. https://www.welivesecurity.com/la-es/2017/06/12/industroyer-amenaza-control-industrial/.

Choo, Kim-Kwang Raymond. 2011. "The cyber threat landscape: Challenges and future research directions." *Computer & Security* 30: 719-731. https://doi.org/10.1016/j.cose.2011.08.004.

Coburn, Andrew, Eireann Leverett, y G. Woo. 2019. *Solving cyber risk : protecting your company and society*.*Wiley finance series*. Hoboken, New Jersey: Wiley.

Council on Foreign Relations. 2021a. "Compromise of a power grid in eastern Ukraine." Cyber Operations. https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine.

---. 2021b. "Duqu." Cyber Operations. https://www.cfr.org/cyber-operations/duqu.

---. 2021c. "GhostNet." Cyber Operations. https://www.cfr.org/cyber-operations/ghostnet.

---. 2021d. "Operation Aurora." Cyber Operations. https://www.cfr.org/cyber-operations/operation-aurora.

---. 2021e. "Titan Rain." Cyber Operations. https://www.cfr.org/cyber-operations/titan-rain.

Cramon, Jesper, Stig Frederiksen, y Finn Glismand. 2017. *Interim Report Q2 2017.* A.P. Møller-Mærsk A/S (Copenhague).

Crosignani, Matteo, Marco Macchiavelli, y André F. Silva. 2020. *Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains.* Federal Reserve Bank of New York (Nueva York).

Daly, Joseph P. 1993. "The Computer Fraud and Abuse Act - A New Perspective: Let the Punishment Fit the Damage." *Journal of Computer & Information Law* 12 (3).

Deloitte. 2022. "¿Qué es la Industria 4.0? Davos y la Industria 4.0." https://www2.deloitte.com/es/es/pages/manufacturing/articles/que-es-la-industria-4.0.html.

Demchak, Chris. 2012. "Cybered Conflict, Cyber Power, and Security Resilience as Strategy." En *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, editado por Derek S. Reveron, 246. Washington, DC: Georgetown University Press.

Detection and Response Team (DART), y Microsoft 365 Defender Research Team. 2021. "Web shell attacks continue to rise." https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/.

Ehrenfeld, Jesse M. 2017. "WannaCry, Cybersecurity and Health Information Technology: A Time to Act." *Journal of Medical Systems* 41 (7): 104. https://doi.org/10.1007/s10916-017-0752-1.

Eisenberg, Ted, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, y Thomas Santoro. 1989. "The Cornell Commission: On Morris and the Worm." *Communications of the ACM* 32 (6): 706-709. https://doi.org/10.1145/63526.63530

Eken, Hanim. 2013. "Software Security of Web Application and Web Attacks." *International Journal of eBusiness and eGovernment Studies* 5 (2): 70-78.

Entous, Adam, y Danny Yadron. 2015. "Spy Virus Linked to Israel Targeted Hotels Used for Iran Nuclear Talks" In "The Wall Street Journal." https://www.wsj.com/articles/spy-virus-linked-to-israel-targeted-hotels-used-for-iran-nuclear-talks-1433937601.

ESET. 2017. "Industroyer: Biggest malware threat to critical infraestructure since Stuxnet." https://www.eset.com/int/industroyer/.

---. 2022. "Sobre parches y actualizaciones: ¿Microsoft podría haber detenido a WannaCryptor?". https://www.welivesecurity.com/la-es/2017/07/14/parches-y-actualizaciones-microsoft-wannacryptor/#:~:text=Si%20vamos%20a%20una%20definición,pero%20aplicado%20al%20mundo%20digital.

Euroinnova. 2022. "Sistema operativo." https://www.euroinnova.mx/sistema-operativo.

Fayi, Sharifah Yaqoub A. 2018. "What Petya/NotPetya Ransomware Is and What Its Remediations Are." *Information Technology - New Generations* 738: 93-100. https://doi.org/10.1007/978-3-319-77028-4_15.

Fernández, Yúbal. 2021. "Deep Web, Dark Web y Darknet: éstas son las diferencias." Xataka. https://www.xataka.com/servicios/deep-web-dark-web-darknet-diferencias.

Foucault, Michel. 1979. *Microfísica del Poder*. Traducido por Julia Varela y Fernando Alvarez-Uría. Madrid: Las Ediciones De La Piqueta.

Frederiksen, Stig, Finn Glismand, y Jesper Riddler Olsen. 2018. *2017 Annual Report.* A.P. Møller-Mærsk A/S (Copenhague).

Froehlich, Andrew. 2021. "Payload (computing)." TechTarget. https://www.techtarget.com/searchsecurity/definition/payload.

Froehlich, Andrew, y Madelyn Bacon. 2022. "white hat hacker." TechTarget. https://www.techtarget.com/searchsecurity/definition/white-hat.

Frost, Laurence, y Naomi Tajitsu. 2017. "Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plants." *Business Insider*, 15 de mayo, 2017. Accesado el 26 de junio de 2019. https://www.businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5.

Furnell, Steven, y Eugene H. Spafford. 2019. "The Morris Worm at 30." *ITNOW* 61 (1): 32-33. https://doi.org/10.1093/ITNOW/BWZ013.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (2): 41-73. https://doi.org/10.1162/ISEC_a_00136.

Gartzke, Erik, y Jon R. Lindsay. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24 (2): 316-348. https://doi.org/10.1080/09636412.2015.1038188.

Gendron, Angela. 2013. "Cyber threats and multiplier effects: Canada at risk." *Canadian Foreign Policy Journal* 19 (2): 178-198. https://doi.org/10.1080/11926422.2013.808578.

Gibbs, Samuel. 2015. "Duqu 2.0: Computer Virus "linked to Israel" found at Iran nuclear talks venue" In "The Guardian." https://www.theguardian.com/technology/2015/jun/11/duqu-20-computer-virus-with-traces-of-israeli-code-was-used-to-hack-iran-talks.

Gobierno de Colombia. 2022. "Equipo de Computo." https://minciencias.gov.co/glosario/equipo-computo#:~:text=Dispositivo%20electrónico%20que%20almacena%20y,el%20software%20(parte%20intangible).

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*: 52-63.

---. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Nueva York: Doubleday.

Grupo de Trabajo de Ciberriesgos de AGERS - ISMS FORUM. 2017. *Guía de Terminología de Ciberseguridad*. Madrid: Asociación Española de Gerencia de Riesgos y Seguros.

Haji, Alan. 2021. "Industroyer – Crash Override (2016)." https://cyberlaw.ccdcoe.org/wiki/Industroyer_–_Crash_Override_(2016).

Henley, Jon , y Olivia Solon. 2017. "'Petya' ransomware attack strikes companies across Europe and US." *The Guardian*. https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe.

Horton, Jeffrey, y Jennifer Seberry. 1997. "Computer Viruses An Introduction." 20th Astralasian Computer Science Conference, Sídney, Australia, Febrero 5-7.

IBM Corporation. 2020. *Cost of a Data Breach Report 2020*. IBM (Armonk, Nueva York).

IDERA Inc. 2021. "Master File Table." https://www.idera.com/glossary/master-file-table.

Intel Corporation. 2021. "Glosario de términos." https://www.intel.la/content/www/xl/es/support/topics/glossary.html#v.

International Telecommunication Union. 2019. *Global Cybersecurity Index (GCI) 2018*. Ginebra: ITU Publications.

Johnson, Dominic D. P. , y Monica Duffy Toft. 2014. "Grounds for War: The Evolution of Territorial Conflict." *International Security* 38 (3): 7-38. https://doi.org/10.1162/ISEC_a_00149.

Kamiński, Mariusz Antoni. 2020. "Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme." *Security & Defence Quarterly* 29 (2): 63-71. https://doi.org/10.35467/sdq/121974.

Kaspersky Lab. 2014. "The Wages of Hacking: How Much Cybercrime Pays." https://usa.kaspersky.com/resource-center/infographics/how-hackers-earn-money.

---. 2015a. Duqu 2.0: Frequently Asked Questions.

---. 2015b. *The Duqu 2.0: Technical Details.* Kaspersky Lab (Moscú).

---. 2021a. "Ataques de APT BlackEnergy en Ucrania." https://latam.kaspersky.com/resource-center/threats/blackenergy.

---. 2021b. "Closed-source software (proprietary software)." Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/glossary/closed-source/.

---. 2021c. "Phishing." Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/glossary/phishing/.

---. 2021d. "VBS (Visual Basic Script)." Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/glossary/vbs-visual-basic-script/.

---. 2021e. "What is WannaCry ransomware?". https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

---. 2022a. "¿Qué es la biometría?". https://latam.kaspersky.com/resource-center/definitions/biometrics.
---. 2022b. "What is a Black-Hat hacker?". https://www.kaspersky.com/resource-center/threats/black-hat-hacker.
---. 2022c. "What is VPN? How It Works, Types of VPN." https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn.
---. 2022d. "Wiper." https://encyclopedia.kaspersky.com/glossary/wiper/.
Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38 (2): 7-40. https://doi.org/10.1162/ISEC_a_00138.
Kinsta Inc. 2020. "¿Qué Es un Sistema de Gestión de Contenidos (CMS)?". Kinsta Inc. https://kinsta.com/es/base-de-conocimiento/sitema-de-gestion-de-contenido/.
Kosciuszko Institute, y CYBERSEC. 2019. "Oleh Derevianko." Kosciuszko Institute. https://2019.cybersecforum.eu/en/speakers/oleh-derevianko/.
Kulkarni, Pradeep, Sameer Patil, Prashant Kadam, y Aniruddha Dolas. 2018. "EternalBlue: A prominent threat actor of 2017-2018." *Virus Bulletin*: 1-15.
Kushner, David. 2013. "The Real Story of Stuxnet." *IEEE Spectrum* 50 (3): 48-53. https://doi.org/10.1109/MSPEC.2013.6471059.
Lee, Dave. 2019. "Baltimore ransomware attack: NSA faces questions." *BBC News*, May 27.
Lee, Newton. 2015. *Counterterrorism and Cybersecurity*. Cham: Springer.
Levi, Ran, y Amit Serper, "Malicious Life Podcast: Inside NotPetya, Part 1," 3 de marzo, 2021a, en *Malicious Life Podcast*, producido por Cybereason, 32:48, https://www.cybereason.com/blog/malicious-life-podcast-inside-notpetya-ransomware-part-1.
---, "Malicious Life Podcast: Inside NotPetya, Part 2," 22 de marzo, 2021b, en *Malicious Life Podcast*, producido por Cybereason, 26:17, https://www.cybereason.com/blog/malicious-life-podcast-inside-notpetya-ransomware-part-2.
Lika, Reyner Aranta, Danushyaa Murugiah, Daksha Ramasamy, y Sarfraz Nawaz Brohi. 2018. "NotPetya: Cyber Attack Prevention through Awareness via Gamification." *International Conference on Smart Computing and Electronic Enterprise*: 1-6. https://doi.org/10.1109/ICSCEE.2018.8538431.
Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365-404. https://doi.org/10.1080/09636412.2013.816122.
Lindsay, Jon R., y Erik Gartzke. 2020. "Politics by many other means: The comparative strategic advantages of operational domains." *Journal of Strategic Studies*: 1-34. https://doi.org/10.1080/01402390.2020.1768372.
Linkos Group. 2021a. "Linkos Group." https://www.linkos.ua.
---. 2021b. "M.E. Doc." https://medoc.ua.
Luhn, Alec. 2017. "Ukrainian military intelligence officer killed by car bomb in Kiev." *The Guardian*, 2017. https://www.theguardian.com/world/2017/jun/27/ukraine-colonel-maksim-shapoval-killed-car-bomb-kiev.
Malwarebytes. 2019. "EternalRomance." https://blog.malwarebytes.com/glossary/eternalromance/.
Malwarebytes Labs. 2017. "Keeping up with the Petyas: Demystifying the malware family." Last Modified 2021. https://blog.malwarebytes.com/cybercrime/2017/07/keeping-up-with-the-petyas-demystifying-the-malware-family/.
Mansfield-Devine, Steve. 2016. "Ransomware: Taking businesses hostage." *Network Security* (10): 8-17. https://doi.org/10.1016/S1353-4858(16)30096-4.

---. 2017. "Ransomware: The Most Popular Form of Attack." *Computer Fraud & Security* 2017 (10): 15-20.
Markoff, John. 2009. "Vast Spy System Loots Computers in 103 Countries." *The New York Times*, 2009. https://www.nytimes.com/2009/03/29/technology/29spy.html.
Marsh, Sarah. 2018. "US joins UK in blaming Russia for NotPetya cyber-attack." *The Guardian*, Febrero 15, 2018. https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine.
Merck KGaA. 2018. "Compañía/Quiénes Somos." https://www.merckgroup.com/mx-es/company/who-we-are.html.
Microsoft. 2016. "Server Message Block Overview." https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831795(v=ws.11).
---. 2017. "Microsoft Security Bulletin MS17 - 010 - Critical." Microsoft. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.
Mohammad, Adel Hamdan. 2020. "Analysis of Ransomware on Windows platform." *International Journal of Computer Science and Network Security* 20 (6): 21-27. https://doi.org/10.13140/RG.2.2.11150.59202.
Mohurle, Savita, y Manisha Patil. 2017. "A brief study of Wannacry Threat: Ransomware Attack 2017." *International Journal of Advanced Research in Computer Science* 8 (5): 1938-1940. https://doi.org/10.26483/ijarcs.v8i5.4021.
Monaghan, Angela. 2017. "Massive cyber-attack could cost Nurofen and Durex maker £100m." *The Guardian*, 2017.
Nash, Kim S., Sara Castellanos, y Adam Janofsky. 2018. "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs." *The Wall Street Journal*, 2018. https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.
Norton-Taylor, Richard. 2007. "Titan Rain - how Chinese hackers targeted Whitehall." *The Gaurdian*, 2007. https://www.theguardian.com/technology/2007/sep/04/news.internet.
Nuance Communications Inc., 2017, "Letter to Healthcare Customers," https://www.nuance.com/content/dam/nuance/en_us/collateral/healthcare/demo/dmo-incident-notification-letter-to-customers-en-us.pdf?PID=8200811.
Nye, Joseph S. 2005. *Power in the global information age : from realism to globalization*. Londres: Routledge.
---. 2011. *The Future of Power*. Nueva York: PublicAffairs.
Orman, Hilarie. 2003. "The Morris Worm: A Fifteen-Year Perspective." *IEEE Security & Privacy Magazine* 1 (5): 35-43. https://doi.org/10.1109/MSECP.2003.1236233.
Palazuelos, Félix. 2017. "El nuevo ataque 'ransomware' usa la misma vulnerabilidad que WannaCry." *El País*, 2017. https://elpais.com/tecnologia/2017/06/27/actualidad/1498580805_974901.html.
Palmer, Danny. 2017. "NotPetya cyber attack on TNT Express cost FedEx $300m." *ZDNet*, 2017. https://www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m/.
---. 2019. "Ransomware: The key lesson Maersk learned from battling the NotPetya attack." *ZDNet*, 2019. https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/.
Polityuk, Pavel. 2016. "Ukraine sees Russian hand in cyber attacks on power grid." *Reuters*, 2016. Ukraine sees Russian hand in cyber attacks on power grid.
---. 2017. "Ukraine points finger at Russian security services in recent cyber attack." *Reuters*, Julio 1, 2017. https://www.reuters.com/article/idUSKBN19M39P.

Posey, Brien. 2022. "What is a Server?". TechTarget. https://www.techtarget.com/whatis/definition/server#:~:text=A%20server%20is%20a%20computer,referred%20to%20as%20a%20server.
Pownall, Charlie. 2019. *The Context and Impact of Maerk's NotPetya cyber attack.* AI, Algorithmic and Automation Incidents and Controversies (AIAAIC) (Cambridge).
Reckitt Benckiser Group plc R. 2018. *Annual Report and Financial Statements 2017.* Reckitt Benckiser (Slough).
Reveron, Derek S. 2012. *Cyberspace and national security : threats, opportunities, and power in a virtual world*. Washington, DC: Georgetown University Press.
RFE/RL's Ukrainian Service. 2017. "Ukrainian SBU Colonel Killed By Blast In Donetsk Region." *Radio Free Europe/Radio Liberty*, 2017. https://www.rferl.org/a/ukraine-colonel-killed-by-blast-donetsk-region/28584475.html.
Rhysider, Jack, "EP 54: NOTPETYA," 2019, en *Darknet Diaries*, https://darknetdiaries.com/episode/54/.
Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Cyber War Will Not Take Place* 35 (1): 5-32. https://doi.org/10.1080/01402390.2011.608939.
Rogin, Josh. 2010. "The top 10 Chinese cyber attacks (that we know of)." The Cable. https://foreignpolicy.com/2010/01/22/the-top-10-chinese-cyber-attacks-that-we-know-of/.
Rosneft. 2018. *Annual Report 2017.* Rosneft (Moscú).
Russinovich, Mark. 2021. "PsExec v2.34." Microsoft. Accessed 2021. https://docs.microsoft.com/en-us/sysinternals/downloads/psexec.
Sahuquillo, M. R., y B. Domínguez. 2017. "Un potente ciberataque afecta a grandes empresas de todo el mundo." *El País*, 2017. https://elpais.com/internacional/2017/06/27/actualidad/1498568187_011218.html.
Sailio, Mirko, Outi-Marja Latvala, y Alexander Szanto. 2020. "Cyber Threat Actors for the Factory of the Future." *Applied Sciences* 10 (4334): 1-25. https://doi.org/10.3390/app10124334.
Saldana, Gustavo. 2018. "A un año de WannaCry el exploit EternalBlue sigue siendo un vector de infección." Kaspersky Lab. https://latam.kaspersky.com/blog/a-un-ano-de-wannacry-el-exploit-eternalblue-sigue-siendo-un-vector-de-infeccion/12952/.
Santander. 2022. "¿Qué es una vulnerabilidad informática?". https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20informática%2C%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.
Satariano, Adam, y Nicole Periroth. 2019. "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong." *The New York Times*, 2019. https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.
Seemma, P. S., S. Nandhini, y M. Sowmiya. 2018. "Overview of Cyber Security." *International Journal of Advanced Research in Computer and Communication Engineering* 7 (11): 125-128. https://doi.org/10.17148/IJARCCE.2018.71127.
Segal, Adam. 2013. "From TITAN RAIN to BYZANTINE HADES: Chinese Cyber Espionage." En *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, editado por Jason Healey, 165-173. Arlington: Cyber Conflict Studies Association.
Seung, Ho Na, Kim Kwanwoo, y Seungwon Shin. 2018. "Knowledge Seeking on The Shadow Brokers." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, Canada. https://doi.org/10.1145/3243734.3278512.
Singer, Peter W., y Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Nueva York: Oxford University Press.

Slowik, Joe. 2019. *CRASHOVERRIDE: Reassessing the 2016 UkraineElectric Power Event as a Protection-Focused Attack.* Dragos Inc. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.

Stiglitz, Joseph E. 2019. *People, Power, and Profits: Progressive Capitalism for an Age of Discontent*. Nueva York: W. W. Norton & Company.

Stubbs, Jack, y Pavel Polityuk. 2017. "WRAPUP 1-Cyber attack hits oil giant and banks in Russia and Ukraine." *Reuters*, 2017. https://www.reuters.com/article/cyber-attack-idUSL8N1JO3JA.

TechLib. 2022. "Componente." https://techlib.net/definition/component.html.

The Small Business Innovation Research (SBIR), y Small Business Technology Transfer (STTR). 2021. "Introduction to Cyberthreats." Cybersecurity for Small Business. United States Government. https://www.sbir.gov/tutorials/cyber-security/tutorial-2.

Tunggal, Abi Tyas. 2021. "What is an SMB Port? Ports 445 and 139 Explained." UpGuard. https://www.upguard.com/blog/smb-port#toc-2.

Ukrayinska Pravda. 2017. "Вірус Petya зачепив понад 1,5 тисячі юридичних і фізичних осіб." *Ukrayinska Pravda*, 2017. https://www.pravda.com.ua/news/2017/06/29/7148210/.

Van Creveld, Martin. 1991. *Technology and war : from 2000 B.C. to the present*. New York Toronto: Free Press.

van Haaster, Jelle. 2016. "Assessing Cyber Power." International Conference on Cyber Conflict (CyCon), Tallin.

Volz, Dustin, y Sarah Young. 2018. "White House blames Russia for 'reckless' NotPetya cyber attack." *Reuters*, Febrero 15, 2018. https://www.reuters.com/article/us-britain-russia-cyber-usa-idUSKCN1FZ2UJ.

Voreacos, David, Katherine Chiglinsky, y Riley Griffin. 2019. "Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?" *Bloomberg*, 2019. https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war.

Waltz, Kenneth N. 1979. *Theory of international politics.Addison-Wesley series in political science*. Reading, Mass.: Addison-Wesley Pub. Co.

---. 2018. *Man, the state and war : a theoretical analysis*. New York: Columbia University Press.

Wendt, Alexander. 2009. "La Anarquía es lo que los Estados hacen de ella: La construcción social de la política del poder." *El constructivismo y las relaciones internacionales,* editado por Arturo Santa Cruz, 138-197. México, D.F.: Centro de Investigación y Docencia Económicas (CIDE).

Wheeler, Tarah, y Josephine Wolff. 2022. "Why Insurance Companies Don't Want to Pay Out for Cyberattacks." Foreign Policy. https://foreignpolicy.com/2022/02/21/merck-insurance-cyberattack-russia-ukraine-notpetya/.

Zola, Andrew. 2021. "ping." TechTarget. https://www.techtarget.com/searchnetworking/definition/ping.