Universidad Nacional del Centro de la Provincia de Buenos Aires

Facultad de Ciencias Humanas

Licenciatura en Relaciones Internacionales

Tesis de grado:

“La influencia de la Seguridad Informática en las Relaciones Internacionales.

El rol de las grandes potencias: Estados Unidos, China y Rusia.”

Tesista: Emilio Nagy Gyuris

Director: Mg. Javier Luchetti

Co-director: Mg. Hugo Javier Curti

TANDIL

Diciembre de 2018

Agradecimientos

A mi papá, a mi mamá y a mi hermana por su apoyo incondicional.

A mis amigos de toda la vida, por acompañarme durante este proceso.

A mis compañeros y amigos de la carrera, que transitaron el mismo camino y comprenden la satisfacción por el logro obtenido.

A mi director Javier Luchetti, por alentarme desde el primer día con este proyecto, y por guiarme y respaldarme en el desarrollo de la tesis.

A mi co-director, Hugo Curti, por la pericia y dedicación en sus contribuciones, y el gran compromiso que demostró desde el primer día.

A la educación pública argentina, sin la cual nada de esto hubiese sido posible. En especial agradezco a la Universidad Nacional del Centro de la Provincia de Buenos Aires, y en particular a la Facultad de Ciencias Humanas.

Índice General

Índice de ilustraciones

Glosario

Algoritmo: conjunto ordenado y finito de operaciones —usualmente matemáticas— que permite hallar la solución a determinada clase de problema. Los algoritmos son utilizados usualmente en informática para realizar tareas de cálculo, de procesamiento de datos y de razonamiento automático.

Amenazas Persistentes Avanzadas (APT): usualmente abreviado APT por sus siglas en inglés de *Advanced Persistent Threat*, es un ataque informático que consiste de un conjunto de procesos silenciosos y continuos con el objetivo de penetrar un sistema informático específico.

Anonymous: grupo descentralizado de activistas informáticos autoconvocados, surgidos en comunidades de Internet, que inició sus actividades por diversión para luego transicionar a acciones de protestas a favor de la libertad de expresión, la independencia de Internet y derechos sociales, haciendo uso del *hacktivismo*.

ARPANET: fue una red de computadoras creada por encargo del Departamento de Defensa de los Estados Unidos para ser utilizada como medio de comunicación entre diferentes instituciones académicas y estatales.

Ataques de Denegación de Servicio (DoS): es un tipo de ataque informático que envía múltiples solicitudes a un servidor (generalmente de páginas web), sobrecargando su capacidad de respuesta, y volviendo el servicio parcial o totalmente inaccesible para las solicitudes de sus usuarios legítimos. Una variación de este tipo de ataque se conoce como Ataque de Denegación de Servicio Distribuido (DDoS), donde se hace uso de múltiples computadoras infectadas, o *botnets*, para realizar ataques de denegación de servicio de forma sincronizada y deslocalizada a un objetivo específico.

Ataque de Intermediario (MitM): tipo de ataque informático en el cual un *cracker* se posiciona entre dos partes que creen estar comunicándose directamente entre sí, teniendo la capacidad de espiar la comunicación, o inclusive alterar su contenido.

***Backbone*:** [*columna* en inglés] en referencia a Internet, se refiere a las principales rutas de comunicación entre redes de computadoras de gran tamaño, a las cuales los ISP se conectan para proveer a sus clientes una conexión a Internet.

***Backdoor* (vulnerabilidad)**: *puerta trasera* en español, se refiere en informática a un método oculto de eludir la autenticación o el cifrado de un sistema informático, y a menudo se utiliza para obtener el acceso remoto a una computadora.

***Botnet*:** grupo de computadoras infectadas por malwares, controlados por un atacante en forma remota, generalmente con fines maliciosos. Las botnets pequeñas pueden incluir cientos de computadoras, mientras que las mayores utilizan millones de equipos.

Ciberataque: o *ataque informático*, es un método por el cual un individuo, haciendo uso de un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático o red.

Conmutación de paquetes: método de envío de datos e información entre sistemas informáticos. A diferencia de la conmutación de circuitos tradicional (como las líneas telefónicas), no se establece un canal dedicado entre un emisor y receptor, sino que la información a transmitir se ensambla en paquetes que pueden ser entregados de manera descentralizada y por canales compartidos, y posteriormente re-ensamblados en el destino.

Cortafuegos: sistema de seguridad de redes que monitorea el tráfico entrante y saliente de una red, permitiéndolo o bloqueándolo en base a una serie de parámetros previamente establecidos.

Cracker: usuario que utiliza sus conocimientos técnicos para penetrar ilícitamente sistemas informáticos. La comunidad *hacker* alienta el uso de este término para referirse a aquellos usuarios que perpetran dispositivos con fines maliciosos.

Criptografía: disciplina dentro de la criptología que se ocupa de elaborar técnicas de cifrado para alterar las representaciones lingüísticas de un mensaje, con el fin de hacerlo irreconocible a lectores no autorizados. Los sistemas informáticos hacen uso de protocolos criptográficos que sirven, mediante la implementación de diversos algoritmos, para cifrar los mensajes informáticos.

Cultura *hacker*: se remonta al ARPANET y los inicios de Internet, y refiere a un conjunto de habilidades valores y creencias compartidas de un grupo de individuos, que entienden que los programas informáticos son producciones libres, colaborativas y comunitarias.

***Dark web*:** forma parte de la Internet profunda, aunque no la constituye. Usualmente es confundida con la Internet profunda, pero la *dark web* hace uso de protocolos

diferentes de comunicación para enmascarar —usualmente— contenido y comercio ilegal.

***Día Cero* (vulnerabilidad):** *zero day* en inglés, es una vulnerabilidad de un programa informático que es desconocida para aquellos interesados en mitigar sus efectos. Un *cracker* puede hacer uso de la vulnerabilidad para afectar un sistema informático de manera sorpresiva, al no existir registro ella. Su nombre proviene de la noción de que los ataques que utilizan estas vulnerabilidades el día cero de la conciencia que el resto del mundo tiene de la falla o debilidad en el sistema informático.

DNS: Sistema de Nombres de Dominio, por sus siglas en inglés de *Domain Name System*, es usualmente representado como la guía telefónica de Internet. Parte de la familia de protocolos de Internet, es un sistema de nomenclatura jerárquico y descentralizado para dispositivos conectados a redes IP.

Dominio: un dominio en Internet es un nombre único que identifica a un sitio web en Internet (**www.google.com** en vez de 172.217.28.164).

Dominio de nivel superior: categoría más alta de segmentación de un dominio, que indica su locación geográfica (.ar para Argentina, .uk para Reino Unido), o el tipo de organización (.com para comercios, .org para organizaciones).

Evil twin: *gemelo malvado* en inglés, es un tipo de ataque de intermediario que simula ser un punto de acceso legítimo a una red —usualmente de WiFi— para que los dispositivos se conecten a él, y poder así espiar el tráfico de los clientes.

Foro (Internet): sitio de discusión en la *web* donde las personas publican mensajes alrededor de un tema, creando de esta forma un hilo de conversación jerárquico (*thread* en inglés).

Hacker: usuario experto en el uso de computadoras y en programación, que utiliza su conocimiento técnico para resolver problemas. Tiene sus orígenes en la fundación de Internet y en la difusión libre de programas informáticos. Es comúnmente utilizado erróneamente para referirse a los *crackers*.

Hackers patrióticos: término utilizado para describir un grupo de *crackers*, usualmente ciudadanos o simpatizantes de un país, que realizan acciones ofensivas y defensivas en el ciberespacio contra lo que éstos perciben como enemigos de su Estado o nación.

***Hacktivismo*:** la utilización no-violenta de herramientas digitales legalmente ambiguas, usualmente al realizar acciones de protesta en el ciberespacio con el objetivo de instaurar agendas políticas o de cambio social.

Infraestructura crítica: instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las instituciones de un Estado o las administraciones públicas.

Internet of Things: usualmente abreviado IoT, en español Internet de las Cosas. Es un paradigma informático que plantea la interconexión de dispositivos cotidianos mediante Internet (luces, cerraduras electrónicas, etc).

Internet profunda: contenido de Internet que no está indexado por los motores de búsqueda convencionales.

***Internet Relay Chat* (IRC):** un protocolo de comunicación de Internet que permite la comunicación entre dos o más personas en tiempo real. Es un protocolo muy abierto y sencillo, por lo que se vuelve virtualmente imposible de controlar.

Jargon file: glosario de la jerga utilizada por programadores de computadoras y hackers.

LOIC: siglas de Low Orbit Ion Cannon (Cañón de Iones de Orbita Baja) es un programa informático diseñado para realizar un ataque de denegación de servicio.

Malware: Malware es la abreviatura del término en inglés "*malicious software*", programa malicioso, y engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento; dentro del grupo de Malwares se pueden encontrar términos como, por ejemplo, Virus, Troyanos, Gusanos (w*orms*), keyloggers, Ransomwares, entre otros. Es una de las palabras más utilizadas para referirse de manera genérica a cualquier programa informático malicioso.

***Phishing*:** intento fraudulento de obtener información sensible de un usuario, usualmente disfrazando una comunicación electrónica como una entidad de renombre (bancos, empresas).

Pila TCP/IP: del inglés Transmission Control Protocol/Internet Protocol (Protocolo de Control de Transmisión/Protocolo de Internet), es un conjunto de reglas y

procedimientos de comunicación utilizados para interconectar dispositivos de red en Internet.

Programa informático o *software*: es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora. Se considera que el *software* es el equipamiento lógico e intangible de un ordenador. En otras palabras, el concepto de software abarca a todas las aplicaciones informáticas, como los procesadores de textos, las planillas de cálculo y los editores de imágenes.

Punto de Acceso (AP): un punto de acceso inalámbrico es un dispositivo de red que permite la conexión de dispositivos inalámbricos a una red, sin la necesidad de conectar los dispositivos mediante cableados convencionales. La tecnología WiFi hace uso de puntos de acceso para acceder a Internet.

Ransomware: conjunción del inglés *ransom* (rescate) y *software* (programa informático). Es un tipo de ataque informático que usualmente cifra o amenaza con cifrar datos de una computadora, y no permite su uso a no ser que se pague un rescate por los mismos.

Script: *guion* en inglés, aunque en español prepondera su uso como *script*. Es un programa informático usualmente simple, almacenado en un archivo de texto, que da órdenes e instrucciones a una computadora.

Seguridad Informática: también conocida como *ciberseguridad*, es el área relacionada con la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.

Servidor: computadora cuya función es suministrar información a los usuarios que la requieran, que pueden ser tanto personas como otros dispositivos conectados.

Sistema Operativo: el software principal o conjunto de programas de un sistema informático que gestiona los recursos físicos y provee servicios a los programas de aplicación de software. Los más conocidos son *Windows* (Microsoft), *macOS* (Apple) y *GNU/Linux.*

Software Libre: es un movimiento fundado en 1983 por Richard Stallman, que aboga por la libertad de los usuarios de un programa informático de ejecutarlo, copiarlo, distribuirlo, estudiarlo, modificarlo y mejorarlo. Este tipo de software

se alza como alternativa al software privativo, que no abre su código fuente, imposibilitando cualquier tipo de estudio o modificación.

***Transport Layer Security*/*Secure Sockets Layer* (TLS/SSL):** son protocolos criptográficos que proporcionan comunicaciones cifradas y seguras por una red, comúnmente utilizados en Internet.

WikiLeaks: organización internacional no gubernamental y sin fines de lucro que publica en la web información secreta y confidencial provista por fuentes anónimas.

World Wide Web: sistema de distribución de documentos visualizables con un programa llamado navegador web. Es la plataforma utilizada para visualizar páginas web y servicios, y una de las tecnologías más utilizadas en Internet.

Lista de siglas, acrónimos y abreviaturas

APT: Advanced Persistent Threat (Amenaza Persistente Avanzada)

ARPANET: Advanced Research Projects Agency Network

ARPA-INTERNET: Advanced Research Projects Agency Internetwork

ASEAN: Asociación de Naciones del Sudeste Asiático

ccTLD: Country Code Top Level Domain

DDoS: Distributed Denial of Service Attack (Ataque de Denegación de Servicio Distribuido)

GNU: Gnu's Not Unix

ICANN: Internet Corporation for Assigned Names

ISP: Internet Service Provider (Proveedor de Servicios de Internet)

JCPOA: Joint Comprehensive Plan of Action (Plan de Acción Conjunto y Completo)

MIT: Massachusetts Institute of Technology

NSF: National Science Foundation

NSFNET: National Science Foundation Network

OIEA: Organismo Internacional de Energía Atómica

SCADA: Supervisory Control and Data Acquisition

TCP/IP: Transmission Control Protocol/Internet Protocol

Introducción

La presente tesis de Licenciatura en Relaciones Internacionales se propone abordar la influencia que tienen Internet y el ciberespacio en las relaciones internacionales, teniendo como eje de análisis a la seguridad informática, disciplina encargada de conservar la integridad de los sistemas informáticos que regulan y controlan las sociedades modernas. Para constatar la influencia de la virtualidad en las relaciones interestatales, se estudiarán casos empíricos de acciones ofensivas en el ciberespacio, las cuales ponen en relevancia el rol de la seguridad informática en la defensa de los intereses soberanos de un Estado. La necesidad de restringir el amplio abanico de casos, limitará el estudio empírico a las capacidades de acción más elaboradas en el ciberespacio, que involucran a las principales potencias del sistema internacional del siglo XXI: Estados Unidos, China y Rusia.

El mundo moderno se encuentra cada vez más interconectado por la tecnología. No hace falta más que una breve observación de las actividades cotidianas para reconocer que prácticamente todo se encuentra permeado por un sistema informático: desde las más visibles, como la comunicación, los medios de información o el transporte; hasta las menos evidentes, tales como los suministros de servicios públicos, el comercio o la producción. La transversalidad de este fenómeno es tal, que de hecho son cada vez son más escasas las actividades que no cuentan con un sistema informático subyacente.

Internet (abreviación del inglés *internetwork*), juega una parte crucial en esta realidad, y es definida por la Real Academia Española como “una red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación”. Si bien más adelante se profundizará sobre esta conceptualización, la noción principal está definida: lejos de ser una idea abstracta, etérea e incorpórea, como muchas veces se puede presentar, Internet es una conjunción de dispositivos físicos que se encargan de funcionar como medio de comunicación de datos e información.

Frente a la mencionada realidad de interconexión transversal de las actividades humanas, el renombrado sociólogo español Manuel Castells señala, en su formulación teórica de la “sociedad red”, que las sociedades modernas están constituidas por “redes de información”. Estas redes de información tienen la capacidad de procesar, transmitir

y almacenar información de una manera que las distingue del resto de los medios disponibles en otras sociedades previas: sin restricciones físicas de volumen, de distancia, ni temporales (Castells, 2000).

El autor español sostiene que las redes de información implican un quiebre con las configuraciones sociales previas, y que las capacidades que introducen crean una nueva morfología social denominada “sociedad red”. De este modo, Castells entiende que tanto los procesos de producción, como la experiencia, la cultura y hasta inclusive las formas y las concepciones del poder se vuelven a modelar desde nuevas perspectivas. Por consiguiente, sostiene que Internet y el ciberespacio son un factor clave en la articulación productiva y social del mundo moderno, equiparándolos con la innovación que representó el carbón para la sociedad industrial (Castells, 2001).

El reemplazo *de facto* que logró Internet por sobre el resto de los medios de comunicación convencionales se expresa en sus estadísticas de uso: la página web Internet World Stats contabilizó 16 millones de internautas a fines de 1995, número que escaló a 4157 millones a fines del 2017, es decir el 54,4% de la población mundial, y lo que representa un incremento del 25880% de la base de usuarios en veintidós años (Internet World Stats, 2017). Esta vertiginosa expansión y crecimiento exponencial en el número de usuarios, es uno de los primeros factores que invitan a preguntar si los usuarios son conscientes de las atribuciones que esta herramienta ha adquirido (Singer & Friedman, 2014, pp. 5-21).

Además del elemento cuantitativo, se vuelve cada vez más relevante el elemento cualitativo de la información que se trasmite mediante Internet: es un abanico tan amplio, que abarca desde videos de gatos asustándose por un pepino, hasta comunicaciones oficiales entre embajadas u organizaciones internacionales. La utilización de Internet para guardar y comunicar datos delicados y confidenciales para la soberanía de un país, desde una negociación internacional, hasta la identidad de sus ciudadanos, implica pensar la manera en la cual se protege la transmisión y el almacenamiento de esta información.

A pesar de la creciente importancia de Internet, sigue vigente lo que Eric Schmidt, director ejecutivo de Google del 2001 al 2017, manifestó en 1997: “Internet es lo primero que la humanidad ha construido, que la humanidad no comprende” (Singer y Friedman, 2014, p. 5). En términos generales, ni las personas de a pie, ni los dirigentes políticos, ni los empresarios conocen como funciona Internet; por ende, menos aún asimilan el funcionamiento de los sistemas informáticos que la subyacen. Y, si bien

entender cómo funciona la principal herramienta de comunicación del siglo XXI, no es una atribución necesaria para el usuario final, sí se torna relevante cuando son sensibles o estratégicos los datos que circulan por Internet. Entonces, como sostienen Singer y Friedman (2014, p. 5, traducción propia):

> "El campo se está volviendo crucial para áreas tan íntimas como la privacidad, y tan importantes como el futuro de la política mundial. Pero es un dominio conocido solo por "los informáticos". Toca todas las áreas importantes de interés del sector público y privado, pero solo los jóvenes y los expertos en informática están bien involucrados con él. A su vez, la comunidad técnica que entiende el funcionamiento con demasiada frecuencia ve el mundo solo a través de una lente específica, y puede no apreciar la imagen más amplia o los aspectos no técnicos. Por lo tanto, los problemas críticos quedan incomprendidos y, a menudo, sin debatir".

La creciente transversalidad que adquiere lo virtual en la dinámica de los Estados, pone en relevancia la importancia de la seguridad informática. Conocida también como ciberseguridad, es el área de la informática que se enfoca en la protección de la integridad y la privacidad de la información almacenada en un sistema informático, o circulante a través de una red de computadoras. Si bien se analizará en profundidad a lo largo de este trabajo de investigación, las posturas que adoptan las principales potencias del sistema internacional respecto a la seguridad informática son un indicio de la relevancia que adquiere. Las agendas de defensa de las principales naciones se ven cada vez más influidas por las estrategias virtuales: el ex presidente estadounidense, Barack Obama, sostuvo que la seguridad informática plantea algunos de los más serios desafíos económicos y de seguridad nacional del siglo XXI, y ésta es una postura que se ha repetido en muchos de los principales dirigentes políticos desde Gran Bretaña hasta China (Singer & Friedman, 2014).

Naturalmente, el bagaje teórico y técnico que subyace a la disciplina de la seguridad informática, requiere de un abordaje multidisciplinario si se pretenden comprender todas las aristas que surgen al estudiar su influencia en las relaciones internacionales. Cuando la seguridad informática se transforma, como se argumentará, en una herramienta estratégica para un Estado y su capacidad de preservar su soberanía, la temática se puede encauzar en el área de Defensa. Si se toma como ejemplo a Argentina, califican como de Defensa aquellas acciones que "tengan por finalidad

garantizar de modo permanente la soberanía e independencia de la Nación Argentina, su integridad territorial y capacidad de autodeterminación; proteger la vida y la libertad de sus habitantes" (Ley de Defensa Nacional Argentina, 1988). De este modo, toda herramienta informática que se inscriba en el campo de la seguridad informática, y que sirva para defender recursos informacionales cruciales para la soberanía de un Estado, o para repeler cualquier atentado virtual contra la integridad estatal, puede ser calificada como una acción de Defensa.

Frente a esta realidad, se procederá a definir las nociones principales que encarnan a Internet y a la virtualidad, para posteriormente ahondar en la influencia específica que posee sobre las relaciones internacionales, y finalmente se estudiarán casos específicos que demuestran la importancia de la implementación de políticas de seguridad informática. Las definiciones técnicas se limitarán a lo necesario para entender los procesos analizados, ya que independientemente de la interdisciplinariedad del trabajo de investigación, sigue siendo una tesis de Relaciones Internacionales. De todos modos, si bien no se profundizará sobre los procesos técnicos que subyacen todas las facetas analizadas, si se hará énfasis en definir con precisión las características abordadas, para desterrar abstracciones erróneas como la que entiende a Internet como una gran "nube" que almacena datos. De esta manera, se suplirán las limitaciones.

En términos de estructuración, el primer capítulo de este trabajo de investigación se centrará en realizar introducción de los conceptos más importantes, como Internet y el ciberespacio, y las cualidades que ameritan especial atención, como los actores que los conforman, las estructuras del orden y la gobernanza en el terreno virtual. A su vez, se realizará una definición integral sobre la seguridad informática, y se abordaran las principales amenazas que existen en el ciberespacio, con las cuales se pueden enfrentar tanto los actores individuales como los Estados.

La definición de estas cuestiones básicas permitirá que en el segundo capítulo se estudie más específicamente la influencia de todas estas variables en el sistema internacional y las relaciones internacionales, estudiando cuestiones como el ciberterrorismo, la posibilidad de que existan guerras virtuales, o que la virtualidad de lugar a nuevos tipos de conflicto. Además, se estudiarán cuáles son las estrategias de seguridad informática que un Estado posee para defender sus intereses frente a las mencionadas amenazas virtuales.

El énfasis sobre la necesidad de estrategias de seguridad informática requiere una comprensión de las amenazas que ameritan una defensa. Es por eso que en el tercer

capítulo se abordarán casos específicos de ataques informáticos internacionales, que utilizaron diferentes combinaciones de las estrategias ofensivas descritas en el primer capítulo. La particularidad de los ataques informáticos que se analizarán radica en que éstos se destacan en su capacidad de acción ya que fueron llevados a cabo por las grandes potencias del sistema internacional: Estados Unidos, China y Rusia, y todos fueron realizados con objetivos geopolíticos. El análisis de estos casos será funcional para constatar la relevancia empírica de las nociones teóricas introducidas en el primer y segundo capítulo, y servirán para aseverar cual es el potencial que tiene la virtualidad para afectar el equilibrio de poderes en el sistema internacional.

Objetivos e hipótesis

Objetivos generales

- Analizar la creciente influencia que la seguridad informática está teniendo en las relaciones internacionales.
- Analizar de qué manera la seguridad informática es un área que afecta los intereses de la Defensa de un Estado, describiendo las principales acciones llevadas a cabo por las grandes potencias, a partir del uso de herramientas informáticas.

Objetivos específicos

- Demostrar de qué manera las acciones en el terreno virtual remodelan las dinámicas de interacción entre los Estados, planteando nuevos desafíos y problemáticas.
- Distinguir las herramientas informáticas que los Estados tienen a su disposición para perfeccionar su seguridad informática (capacitación proactiva, Software Libre).
- Categorizar las principales amenazas informáticas que pueden afectar la soberanía de un Estado y su relación con otros Estados, analizando los casos de Estados Unidos, China y Rusia.

La **hipótesis** planteada es la siguiente:

La Seguridad Informática es una disciplina de especial interés para las Relaciones Internacionales, cada vez más influidas por Internet y el ciberespacio, cuya mayor evidencia reside en relaciones entre las grandes potencias, Estados Unidos, China y Rusia, y las acciones que éstas emprenden respecto a sus recursos informáticos.

Algunas cuestiones terminológicas y elección del marco teórico

Los fenómenos informáticos introducen un gran abanico de particularidades a la escena internacional, engendrando inclusive nuevos actores internacionales, previamente inconcebibles. A pesar de las variaciones en las conformaciones de las unidades, uno de los actores que más se destaca por su capacidad de acción en el ciberespacio es el Estado: las acciones en Internet se siguen atribuyendo a banderas nacionales (Singer y Friedman, 2014), y siguen enmarcándose en un esquema westfaliano, al ser los Estados aquellos actores con más recursos y capacidades virtuales. Es por este motivo que, desde la perspectiva de las Relaciones Internacionales, se utilizará como pilar teórico la teoría del realismo estructural defensivo (o neorrealismo), desarrollado por Kenneth Waltz, y será complementado por abordajes neorrealistas de la temática, con teóricos de las relaciones internacionales como Jervis, Adams y Mearsheimer.

El neorrealismo es una reformulación teórica del realismo, una teoría de las relaciones internacionales fundada, en parte, en la observación del deseo de poder y control de los humanos, y que ha sido refinada a lo largo del tiempo (Tuthill, 2012). Sus lineamientos principales fueron codificados en la posguerra por Hans Morgenthau, en el clásico “Política entre las naciones”, y, en resumen, el realismo sostiene que la cualidad principal del sistema internacional es la anarquía, entendida como ausencia total de un gobierno internacional. Los actores principales en el sistema internacional son los Estados nacionales, los cuales actúan de manera racional, en una constante búsqueda de supervivencia y preservación frente a la incertidumbre que plantea la anarquía previamente mencionada. Un elemento a destacar es que, a pesar de esta situación anárquica, sí existe una estructura jerárquica tácita, determinada por la capacidad militar ofensiva por parte de las grandes potencias, y el poder que éstas ostentan en relación a otros Estados.

Kenneth Waltz, en su “Teoría de la Política Internacional” de 1988, encapsula los conceptos realistas de anarquía, poder y autosuficiencia, en una teoría de carácter sistémico (Tuthill, 2012). De este modo, el autor entiende que el sistema internacional está compuesto por lo que él denomina una *estructura*, y por unidades interactuantes dentro de esta estructura, que son los actores internacionales. El elemento central en este esquema, es que la estructura se plantea como un elemento organizador que tiene la capacidad de moldear el comportamiento de las unidades, ya que los esquemas de conducta emergen de las limitaciones estructurales que el propio sistema les impone a los actores, afectando así su accionar (Waltz, 1988, p. 138). Esto, en palabras simples, refuerza la idea de anarquía, pero contenida en ciertos parámetros que sirven de eje ordenador del sistema internacional, y donde los actores más importantes son quienes establecen las reglas de juego: los Estados nacionales.

La anarquía sigue siendo, en la teorización de Waltz, la característica representativa del sistema internacional. En relación con el caso de análisis de este trabajo de investigación, uno de los principales lazos entre esta teoría y el ciberespacio reside en el concepto de anarquía: aunque como se verá, fue desarrollado por los Estados Unidos como una herramienta militar, Internet se expandió desde los círculos académicos al resto del mundo, convirtiéndose en una herramienta global, que amplió su estructura por todo el planeta (Tuthill, 2012). De este modo, la anarquía en Internet —a pesar de contar con sus particularidades— puede ser entendida como un espejo del sistema internacional anárquico, y se ha convertido en nuevo campo en el cual los Estados pugnan por competir y subsistir, especialmente a partir del momento en que este servicio se convirtió en el entramado comunicacional predominante (Petallides, 2012a).

El concepto de *poder* es central en la teoría realista de las relaciones internacionales, a tal punto que ha llegado a ser denominado “la divisa de la política internacional” por Mearsheimer (2007, citado en Tuthill, 2012, p. 14). Waltz, en su formulación teórica del neorrealismo, otorga un rol central al poder, y su forma de verlo será también útil para estrechar lazos entre el sistema internacional y el ciberespacio. Un elemento importante para lograr este fin es aclarar que Waltz sostiene que los Estados son indiferenciados respecto a las funciones que desarrollan. Como sus funciones no varían, el foco de análisis reside en el poder que los Estados tienen para lograr cumplir con estas funciones, es decir en sus capacidades. Y es aquí donde el poder entra como una de las variables principales en el esquema estructural de Waltz (1988, p. 144):

> “La forma, el tamaño, la riqueza y el poder de los Estados varían. Y, sin embargo, las variaciones de estos y otros aspectos son variaciones de unidades semejantes […] respecto a las tareas con que se enfrentan, pero no en sus capacidades de desarrollar estas tareas. Las diferencias son de capacidad, no de función.”

No obstante, y aquí si alejándose de la acepción realista más clásica de poder, en la perspectiva estructural que Waltz introduce, deja entrever que el poder en realidad no es la capacidad de un Estado de lograr sus objetivos de manera constante, sino que implica que un Estado pueda influir a otros, más que éstos a él (Waltz, 1988). El poder en sí, entonces, deja de ser un fin al que los Estados apuntan, y se convierte en una herramienta. De este modo, Waltz aclara:

> “La capacidad nos dice algo acerca de las unidades. Definir la estructura en parte en términos de la distribución de las capacidades parece violar mi indicación anterior de no incluir los atributos de las unidades en las definiciones estructurales. […] La distribución de capacidades no es un atributo de las unidades, sino más bien un concepto sistémico. […] Nos abstraemos de todas las cualidades particulares de los Estados y de todas sus conexiones concretas. Lo que emerge es un cuadro posicional, una descripción general de la disposición de una sociedad trazado en términos de la ubicación de las unidades y no en términos de sus cualidades” (Waltz, 1988, p. 145-147).

Resaltar esta particularidad estructural no es arbitrario en este análisis, ya que servirá para entender el abordaje de este trabajo de investigación sobre la seguridad informática, y cómo se entienden las estrategias ofensivas y defensivas en el territorio del ciberespacio: las capacidades individuales de cada Estado en términos de seguridad informática importan, pero algunos debates que se abarcarán (específicamente los concernientes a la atribución de los ataques informáticos, y la capacidad de desarrollar herramientas informáticas ofensivas y defensivas), hacen que sea más relevante lograr un análisis que adopte una perspectiva estructural, y que pueda extraer conclusiones observando los resultados de posicionamiento relativo de los actores luego de los sucesos en el ciberespacio.

La selección de Waltz como pilar teórico para la investigación adquiere más sentido al bosquejar la concepción del autor sobre la seguridad de los Estados. Como se

sostuvo, Waltz entiende que el objetivo primordial de un Estado es utilizar todo su poder para garantizar su supervivencia. Esta percepción implicaría una inversión constante de recursos, en pos de lograr un posicionamiento relativo mejor en el sistema internacional, logrando así una incertidumbre menor respecto a la supervivencia del Estado.

Una de las cuestiones que se analizarán respecto a estas acciones en el ciberespacio tienen que ver con el "dilema de la seguridad" desarrollado por Robert Jervis. En esta formulación teórica, el autor sostiene que en el ámbito doméstico los Estados tienen diversas maneras de incrementar su seguridad sin afectar al resto, ya que depende de las capacidades intrínsecas de cada actor. Sin embargo, aclara que en el sistema internacional se da la particularidad de que muchos de los medios por los cuales un Estado trata de incrementar su seguridad, se traducen en una amenaza que disminuye proporcionalmente la seguridad de otros Estados (Jervis, 1978, p. 169-170). En este caso, la clásica discusión entre las armas ofensivas y las armas defensivas se vuelve a reabrir en el plano cibernético, en tanto que una herramienta informática que pretende ser defensiva, pueda ser usada, por ejemplo, como un arma para dañar información o los recursos de otro Estado. El desconocimiento generalizado de las herramientas informáticas, sumado a la incertidumbre sobre las verdaderas intenciones que puedan tener, hace que la línea se vuelva cada vez más borrosa.

Estas cuestiones llevan a que el autor neorrealista James Adams sostenga que "el ciberespacio se ha convertido en un nuevo campo de batalla internacional" (Adams, 2001, p. 98), reforzando no sólo la noción de Internet como un sistema anárquico que se ajusta perfectamente al modelo de seguridad realista, sino también planteando dudas sobre la neutralidad del ciberespacio a la hora de incluir intereses mayores (Jervis, 2012). El autor analiza el Moonlight Maze, una serie de importantes ataques informáticos en 1999 contra sistemas informáticos estadounidenses, supuestamente provenientes de Moscú. Basado en este caso, Adams sostiene que es "sólo una muestra de los peligros que están por venir". A pesar de escribir su artículo "Defensa Virtual" en el año 2001, el autor advierte tempranamente sobre la posibilidad de penetrar sistemas de defensa, infraestructura pública y sistemas corporativos y económicos, y las consecuencias que esto puede tener. A su vez, con una perspectiva realista, sostiene que hay muchos países que intentarán avances en la arena del combate virtual, incrementando los recursos de los Estados en nuevas áreas de la defensa (Petallides, 2012a).

La cualidad interdisciplinaria de este trabajo de investigación, además de usar esta estructura realista para analizar las implicancias de las acciones en el ciberespacio, amerita la inclusión de autores que funcionen como puente entre las ciencias informáticas y las ciencias sociales, por lo que se utilizará la teorización de Manuel Castells, el quinto investigador de las ciencias sociales más citado del mundo. Su teoría de la "Era de la información" sostiene que nos encontramos en un período histórico caracterizado por la revolución tecnológica centrada en las tecnologías digitales de información y comunicación, concomitante con, pero no causante de, la emergencia de una estructura social en red (Castells, 2000). Así, Castells afirma que esta *sociedad red* está configurada en torno a las redes y no a los actores individuales, y que funciona a partir de un flujo constante de *información*, que se vuelve un elemento estratégico, a través de las tecnologías de la comunicación.

Si bien la teorización de Castells parece alejarse del esquema westfaliano de preeminencia del Estado como actor principal del sistema internacional, se pueden tender lazos entre ambas teorías, que ayudarán a ubicar la expansión de Internet, con sus múltiples fenómenos, en la cosmovisión neorrealista. Para enlazar las teorías es necesario volver a la teoría estructural de Waltz, quien, siempre reacio al cambio, sostiene que el cambio en el sistema internacional es poco común, y se da solamente en el caso de que cambie el principio ordenador, o por medio de una "variación en las capacidades de las unidades" (Waltz, 1988, p. 139).

Castells (2000, p. 30-31) entiende al nuevo paradigma tecnológico constituido alrededor de la tecnología de la información como una revolución, la cual implicó una nueva forma de organización social, una nueva interacción en la economía global y la geopolítica, y nuevas formas de producir, comunicar, gestionar y vivir. A pesar del ineludible tinte sociológico que el autor imprime a su concepción, no se aleja de la visión de Waltz sobre el cambio. La expansión de las herramientas informáticas a través de Internet implicó incuestionablemente un cambio en las "capacidades de los Estados" a las que Waltz hace alusión, alterando la forma en que éstos desarrollan sus funciones. De este modo, ambas teorías pueden consensuar un indudable cambio en el sistema internacional.

Establecido el cambio en las capacidades generales de los Estados, también es significativo comprender de qué manera se alteró la distribución de las capacidades en el esquema estructural neorrealista. La rápida expansión de Internet a escala global sin

dudas implicó una gran reducción de barreras temporales y espaciales, pero esta nueva tecnología también implica una fuente de debilidad en el caso de no contar con los conocimientos para proteger la información que se resguarda en algún medio digital. Stuxnet, un ataque informático que se supone creado por Estados Unidos en colaboración con Israel, y que embistió contra las turbinas de refinamiento de uranio en Irán entre 2005 y 2010; o la Operación Shady RAT, supuestamente proveniente de China, que se infiltró en más de 71 organizaciones, incluidas las Naciones Unidas y el Comité Olímpico Internacional; ilustran cómo esta tecnología tiene el potencial de volverse un arma de doble filo, cuando se incluye información sensible o estratégica en la ecuación (Singer & Friedman, 2014).

"Cybersecurity and Cyberwar" (*Seguridad Informática y Ciberguerras*, en español) es otro de los pilares que tomará este trabajo de investigación para su desarrollo, escrito por Allan Friedman, director de Iniciativas de Seguridad Cibernética en el Departamento de Comercio de los Estados Unidos, y por Peter Warren Singer, politólogo estadounidense de la Universidad de Harvard, especialista en relaciones internacionales y en guerra del siglo XXI. Este trabajo es ejemplar para ayudar a conectar las influencias de la seguridad informática e Internet sobre las relaciones internacionales. De este modo, como se sostuvo con los ejemplos citados, Singer y Friedman arguyen que aquellos actores que adquieren poder en el terreno cibernético tienen una correlación inmediata en la adquisición de poder en el sistema internacional.

"Las teorías realistas de disuasión, gestión de crisis y conflicto pueden usarse para comprender si el ciberespacio se está estabilizando o desestabilizando, si las tecnologías cibernéticas serán una nueva fuente de conflicto o de paz, y si los Estados participarán o no en carreras de armas cibernéticas", sostienen Reardon y Choucri (2012). Estas nociones son abordadas también por Singer y Friedman (2014), quienes buscan hacer un análisis técnico de las posibilidades de enfrentamiento en el ciberespacio.

El objetivo no es calificar a las herramientas informáticas como armas en potencia, porque esta categorización condicionaría el uso que se les puede dar, e inclusive puede ser estigmatizante. Sin embargo, cotejando la posibilidad de que existan armas virtuales, también se analizará la factibilidad de una "ciberguerra", y la postura que pueden adoptar los Estados en estos nuevos desafíos que plantea el siglo XXI en términos de defensa. En la medida en que pueden ser utilizadas como un elemento de

disrupción de otros Estados, alterando su capacidad de mantener la soberanía y la integridad, las herramientas informáticas adquieren cada vez mayor relevancia en el análisis de las relaciones intergubernamentales.

“Para definir la estructura, es necesario ignorar de qué modo se relacionan las unidades entre sí (cómo interactúan) y concentrarse en cuál es su posición mutua (cómo están dispuestas o posicionadas)”, sostiene Waltz (1988, p. 120). Este nivel de abstracción se intentará lograr para entender al sistema internacional interconectado por la tecnología del siglo XXI, unificando las cosmovisiones del neorrealismo, la sociedad red y la seguridad informática. Para esto será clave analizar de qué manera la estructura condiciona a las principales potencias en el área de la informática, es decir aquellos Estados que tienen los recursos para generar la mayor cantidad de avances —ofensivos y defensivos— en el ciberespacio: Estados Unidos, Rusia y la República Popular China. El análisis del equilibrio de poderes en el ciberespacio será de este modo un espejo del equilibrio de poder en el sistema internacional.

Si bien existen cuestionamientos (Tuthill, 2012; Craig & Valeriano, 2018) a la capacidad de adaptabilidad de las teorías realistas al cambiante sistema internacional del siglo XXI, que las nuevas tecnologías de la información y la comunicación han contribuido a modelar, es necesario aclarar por qué se elige la escuela de pensamiento neorrealista para enmarcar en términos teóricos este trabajo de investigación. Partiendo desde la base de que es imposible pretender un análisis objetivo de cualquier coyuntura basándose sólo en una teoría, el neorrealismo oficiará en este trabajo como una suerte de guía sobre la cual se encauzarán las diversas problemáticas a abordar. A su vez, se eligió esta teoría ya que no solo es una de las más longevas en la disciplina de las relaciones internacionales, sino que, como se intentará demostrar, también prueba su actualidad frente a las políticas de defensa y estrategias internacionales en términos de seguridad que las grandes potencias implementan en el sistema internacional.

Dunn (2007) afirma que es una tarea extremadamente difícil lograr evaluar las fortalezas y las limitaciones de la teoría de las relaciones internacionales en la era de la información. Esto se basa principalmente en que es una temática es de gran extensión, con fronteras indistintas e interdisciplinarias, y con un arsenal conceptual muy específico. Ligado a esto, surgen además preguntas sobre cómo entender la seguridad en la era de la información, y si ésta tiene algún tipo de similitud o diferencia con las concepciones tradicionales de seguridad.

Se vuelve aquí pertinente aclarar la definición de “seguridad” adoptada en este trabajo de investigación, y aquella que se adoptará para “defensa”, dos palabras que parecen intercambiables, pero que aluden a hechos diferentes. Cuando se utiliza la expresión “seguridad informática” o “ciberseguridad”, se hace alusión a la protección de la integridad de la información circulante o almacenada en un sistema informático, pero no se limita a la noción de estar libre de peligro, sino que está asociado a la presencia de un adversario. Un problema cibernético sólo se convierte en un problema de seguridad informática si un adversario busca obtener algo de la actividad, ya sea para robar información privada, socavar un sistema, o impedir su uso legítimo (Friedman & Singer, 2014, p. 34-36). Desde la perspectiva de las ciencias sociales, Héctor Saint-Pierre (2012, p. 42-43) sostiene que, en la mayor abstracción de las funciones de un Estado, es decir la de entenderlo como una institución jurídica que monopoliza el uso de la fuerza, sus funciones principales son dos: la de la seguridad, es decir proteger a los ciudadanos de amenazas internas, mediante la garantía del orden; y la de la defensa, es decir garantizar la soberanía frente a cualquier tipo de amenaza o intrusión foránea. De esta manera, la seguridad informática se alza como una estrategia válida tanto para las nociones de *seguridad* como de *defensa*, pero se abordará su utilización específicamente ligada a su faceta de *defensa* en tanto y en cuanto sirva para proteger los recursos Estatales.

Las particularidades que adquiere la temática de la seguridad en la era de la información requiere de una precisión extrema en términos conceptuales para lograr un análisis fructífero, ya que incluye terminologías provenientes de múltiples disciplinas. La usual confusión o mala utilización de términos, como argumenta Dunn (2007), se debe en primer lugar al desconocimiento generalizado que existe sobre el componente físico de la infraestructura de la información (es decir la conjunción de redes interactivas de alta velocidad, sistemas de comunicación satelitales, aéreas y terrestres, y todos los dispositivos que se usan para acceder a esta infraestructura, como computadoras, televisores y teléfonos celulares) y de su componente inmaterial (el tráfico constante de información y contenido que fluye a través de esta infraestructura, el conocimiento que éste crea, y los servicios que provee).

La decisión de utilizar al neorrealismo en el análisis no supone que este enfoque pueda explicar con precisión todas las aristas del desarrollo de relaciones digitales entre los Estados. De hecho, al ser una teoría que precede al acelerado desarrollo de las nuevas tecnologías de la información de las últimas tres décadas, su utilización implica

una prueba de la misma, para evaluar cuán bien se adapta a los cambios en la escena internacional. De este modo, entender cómo se transforma el concepto de seguridad en los tiempos de *Twitter*, *Amazon* y *WikiLeaks*, implica también estudiar nuevas cualidades de los Estados en su constante competencia por ser la unidad predominante dentro del sistema internacional.

Capítulo I. Internet y el ciberespacio, un espejo del Sistema Internacional

I. Introducción

Abordar una temática tan compleja e interdisciplinaria como la seguridad informática y su influencia en las relaciones internacionales amerita una organización particular en el desarrollo de este trabajo, sobre todo al existir una cierta distancia conceptual entre ambas disciplinas. Como punto de partida, es necesario introducir los conceptos principales que servirán de base para el análisis ulterior, siendo el principal *Internet*.

En el siglo XXI, y exponencialmente más en la segunda década del siglo, cualquier suceso que tenga lugar en el sistema internacional se ve influido, activa o pasivamente, por Internet. Las comunicaciones entre Estados, el comercio internacional, la cooperación, y cualquier otro acontecimiento está permeado por Internet. Sin embargo, parecería ser una de los avances técnicos menos comprendidos: muchos reconocen que existe y podrían inducir sus influencias, pero pocos podrían explicar cómo funciona, y cuáles son sus alcances reales.

Internet configura un terreno de acción muy particular, con similitudes y diferencias con otros terrenos del mundo material, donde interactúan una serie de actores muy disímiles, llamado *ciberespacio*. Este espacio virtual requiere de definiciones, porque se configura cada vez más como un terreno de intercambios entre Estados, así que deben ser presentadas y analizadas las principales acciones ofensivas y defensivas que pueden darse en el ciberespacio.

II. Internet, virtualidad y el ciberespacio

La palabra “internet”, utilizada como sustantivo, es una abreviatura en inglés que procede del término “*internetworks*”, es decir redes interconectadas. En informática, una *red* es un conjunto de equipos electrónicos y de programas informáticos que se organizan en estructuras, coordinadas por dispositivos físicos o inalámbricos, y que, mediante la utilización de estándares compartidos de comunicación, transportan datos, información, recursos y servicios. Cuando el sustantivo se utiliza con mayúsculas, es decir “Internet”, se hace referencia a una red de escala global, de la cual miles millones

de usuarios hacen uso diariamente. Si bien es difícil explicar qué es Internet sin caer en una definición relativamente tautológica, al definirlo como “redes interconectadas”, o en otra acepción ampliamente aceptada, “red de redes”, podemos entender su morfología esencial: es la infraestructura que permite la conexión entre múltiples redes de computadoras y dispositivos a nivel global, con el objetivo de establecer un medio de comunicación entre un emisor y un receptor, independientemente de sus respectivas ubicaciones geográficas.

Si bien el Internet que hoy usamos ha tenido inconmensurables cambios cualitativos y cuantitativos desde su creación, es importante tener una noción de cómo se convirtió en la principal plataforma de comunicación. Su origen y desarrollo no es meramente anecdótico, ya que, al igual que una significativa porción de los avances tecnológicos y de comunicación, Internet fue concebido en sus inicios como una plataforma de comunicación para usos militares, desarrollada por el Departamento de Defensa de los Estados Unidos, en conjunto con universidades estadounidenses.

Una organización sin fines de lucro estadounidense llamada Code.org, cuyo fin es promover la enseñanza de ciencias de la computación, realizó una encuesta en un video relatado por Vint Cerf, conocido como uno de los “padres fundadores del Internet”. En ella, realizan una sencilla pregunta a diferentes peatones: “*¿qué es Internet?*” Las respuestas varían desde “unos satélites voladores”, a “ondas en el aire que entran a los teléfonos celulares”, y llegan hasta definiciones mucho más establecidas como “una nube” (Code.org, 2016). Independientemente del tipo de muestra y la locación geográfica que se tomaron para realizar la encuesta, la situación no variaría mucho de país en país. La realidad es que la mayoría de los usuarios de Internet, no sabe qué es Internet.

Vint Cerf argumenta que las biromes, los inodoros o los cierres de las camperas, comparten algo con Internet, y es que son elementos que la mayoría de las personas utilizan diariamente, y que no se preguntan quién las inventó, o de donde provienen (Code.org, 2016). Lo cierto es que Internet es una red de redes global, que comunica miles de millones de dispositivos en todo el mundo, y su definición es neurálgica para encauzar este análisis de relaciones internacionales. Esto se debe a que, en primer lugar, la mayoría de los Estados utilizan a Internet como su medio de comunicación predilecto, muchas veces ignorando su verdadera naturaleza; y, en segundo lugar, permite comprender el terreno de juego que crea, denominado ciberespacio, en el cual los Estados nacionales tienen un lugar como actores, muy similar al que existe en el sistema

internacional. Racionalizar el funcionamiento de Internet y el ciberespacio es el primer paso para visualizar los desafíos en materia de seguridad informática que los Estados tienen en la actualidad.

1. Una breve historia de Internet

En octubre de 1957, la Unión Soviética colocó en la órbita terrestre el primer satélite artificial de la historia, el Sputnik 1. Este hito, enmarcado en la Guerra Fría, dio inicio a una carrera espacial entre Estados Unidos y la Unión Soviética, que implicó la utilización de enormes cantidades de recursos económicos y académicos en el esfuerzo por explorar el espacio, realizar misiones espaciales, y, en última instancia, llegar a colocar al ser humano en la luna.

Una de las respuestas del gobierno de Estados Unidos frente al lanzamiento del Sputnik 1 fue la creación, en 1958, de la Agencia de Proyectos de Investigación Avanzada (ARPA, por sus siglas en inglés correspondientes a *Advanced Research Projects Agency*), bajo la órbita del Departamento de Defensa. La misión principal de esta agencia, con el fin de evitar nuevas sorpresas tecnológicas, era realizar trabajos conjuntos con sectores académicos, industriales y gubernamentales, para formular y ejecutar proyectos de investigación y desarrollo, y así expandir las fronteras de la tecnología y la ciencia, ligados —aunque no taxativamente— a los requisitos militares inmediatos de los Estados Unidos (DARPA, 2018).

La Oficina de Técnicas de Procesamiento de Información (IPTO, por sus siglas en inglés, correspondientes a *Information Processing Techniques Office*), dependiente de la ARPA, comenzó —con el objetivo de estimular la investigación en el campo de la informática interactiva— en los primeros años de la década de 1960 a investigar un proyecto capaz de compartir el tiempo de computación de los ordenadores entre varios centros de informática y grupos de investigación de la Agencia (Castells, 2001, p. 23). La combinación de descubrimientos en diferentes disciplinas, desde la

Ilustración 1: ARPANET en 1969. Fuente: Europa Press (2015)

física y la química a la informática, se tradujo en la elaboración de una red de comunicaciones sin precedentes, bautizada *ARPANET*, que logró conectar en 1969 a un reducido número de computadoras, intercomunicando a cuatro universidades y centros de investigación estadounidenses (ver ilustración 1).

Desde la perspectiva norteamericana, la "*Crisis del Sputnik*" no sólo evidenció la brecha tecnológica que la Unión Soviética había establecido con los Estados Unidos, quienes se consideraban líderes mundiales en tecnología aeroespacial y misilística, sino que planteó el potencial peligro militar de un satélite artificial soviético en el espacio. Como sostiene Stanley Hoffman, una de las variables que configuraron las acciones llevadas a cabo durante la Guerra Fría fueron las percepciones que cada parte tuvo sobre la otra, ya que "[…] los Estados Unidos veían a la Unión Soviética como mucho más ambiciosa de lo que era y con más control sobre todo del que realmente tenía" (Hoffmann, 1991, p. 210-211). Esta percepción llevó al gobierno estadounidense a interpretar al Sputnik 1 como prueba de superioridad misilística, e inició una creciente ola de preocupación por la plausibilidad de un ataque nuclear intercontinental. ARPANET se constituyó entonces como una red descentralizada que tenía la capacidad de continuar operando aún bajo el supuesto de un ataque nuclear, ya que distribuía los envíos de información con una novedosa técnica de *conmutación de paquetes*.

Hasta el momento, se había generalizado la utilización de la tecnología de *conmutación de circuitos*, cuya representación máxima fueron las líneas telefónicas: para comunicarse, dos nodos establecen un canal dedicado de comunicación, que finaliza en el caso de ser interrumpido el canal. Lo revolucionario del método de *conmutación de paquetes* fue que permitió dividir un mensaje en muchas partes o *paquetes*, que se entregaban de manera descentralizada utilizando múltiples vías. Una vez que todos los paquetes llegaban al destino, se re-ensamblaban como un rompecabezas, y el mensaje se volvía disponible para el receptor (en el caso de cortarse uno de los canales de comunicación, el paquete podía utilizar otro canal dentro de la red para llegar a su destino).

La conmutación de paquetes aplicada a ARPANET, cuya intención principal fue esta resiliencia ante ataques nucleares, sigue configurando la esencia técnica de Internet en la actualidad, y hoy se encuentra generalizado, pero en la década de 1960 otorgó un dinamismo sin precedentes a la infraestructura de las comunicaciones, y fue uno de los factores que le permitió —luego de desarrollar estándares de comunicación

internacionales— que Internet adquiriera una escala global (Singer & Friedman, 2014, p. 17).

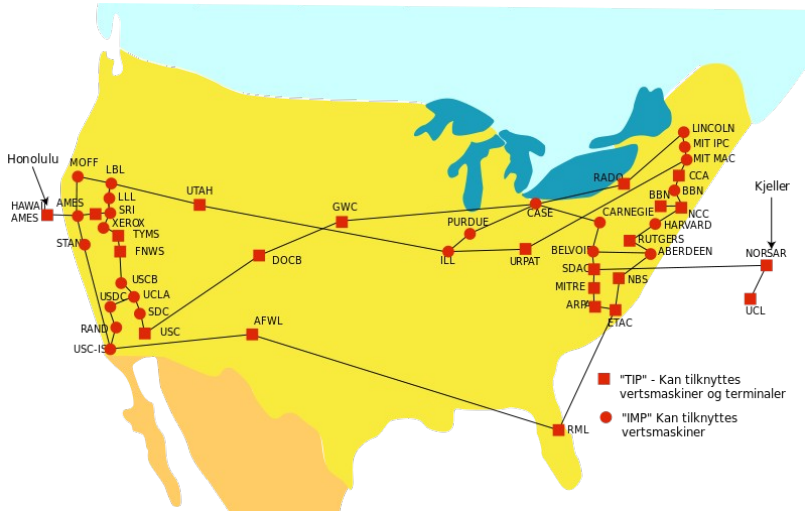

Ilustración 2: ARPANET en 1974. Fuente: Wikimedia Commons (2007)

Como sostiene Castells (2001), la anexión de nuevos desarrollos técnicos (adopción del protocolo TCP/IP como estándar de comunicación, la invención de la World Wide Web, la utilización generalizada de la norma POSIX introducida por el sistema operativo UNIX, ARPANET en 1974. Fuente: Wikimedia Commons (2007)el surgimiento del movimiento por el Software Libre como alternativa a los sistemas operativos privativos), permitió una escalabilidad cada vez mayor de la infraestructura, que se ve reflejada en los números de nodos: en 1969, ARPANET conectaba cuatro computadoras, que incrementaron su número a sesenta computadoras en 1974, y en 1977 a más de cien, no solo entre las costas este y oeste del territorio norteamericano, sino también con Hawái. Esta amplia red de computadoras, logró una arquitectura descentralizada, con una gran extensión territorial (ver ilustración 2), y se erigió como la primera forma de lo que hoy se conoce como Internet (Tuthill, 2012, p. 7).

Si bien ARPANET no fue la única fuente para la constitución de Internet, es relevante en este trabajo por dos motivos. En primer lugar, ARPANET fue una red pionera en la implementación de la tecnología de conmutación de paquetes, y la primera red en implementar la pila de protocolos TCP/IP, dos tecnologías que se convirtieron en la base técnica de Internet. En segundo lugar, el desarrollo histórico de ARPANET tiene un significado para las relaciones internacionales, ya que es una de las principales fuentes de Internet, y surge como resultado de un conflicto geopolítico enmarcado en la Guerra Fría.

Castells (2001, p. 51-77), realizando un análisis integral sobre la gestación de Internet, refuerza lo previamente expuesto, y argumenta que la rápida expansión y

evolución de Internet no puede circunscribirse exclusivamente al aspecto técnico, sino que existen tres importantes variables que propiciaron su difusión. En primer lugar, sostiene que hubiese sido imposible lograrlo sin una creencia tecnocrática del progreso humano a través de la tecnología, predominante en el mundo académico donde se originó Internet.

La segunda variable que el autor resalta como crucial en el desarrollo de Internet también es oriunda de los círculos académicos estadounidenses, y tiene sus orígenes más remotos en los laboratorios del Instituto Tecnológico de Massachusetts (MIT), y es la cultura *hacker*. Sostiene que esta filosofía para entender al *software* y a la tecnología, fue la que otorgó el carácter libre, abierto y comunitario a Internet. (Castells, 2001, p. 27-28). Uno de los movimientos que más sintetiza hasta la actualidad la "cultura *hacker"* descrita por Castells es el Movimiento por el Software Libre, fundado y dirigido por Richard Stallman. Esta corriente promueve la apertura del código fuente de los programas informáticos como un derecho de los usuarios, para evitar que el uso de la tecnología como herramienta se convierta en un tipo de dependencia. Sostiene así que la libertad de uso, modificación y distribución de los programas informáticos promueve la libertad de los usuarios, en contraposición a la dependencia generada por el software privativo (Sistema Operativo GNU, 2018a).

Es pertinente realizar aquí un apartado para definir a qué se refiere el autor con la palabra "hacker", ya que es la que se adoptará a lo largo del desarrollo de este trabajo. El Jargon File (un glosario y diccionario de referencia del léxico de los programadores de computadoras) define a un *hacker* como "una persona que disfruta explorar los detalles de los sistemas programables y cómo ampliar sus capacidades, a diferencia de la mayoría de los usuarios, que prefieren aprender solo el mínimo necesario", y también como "alguien que programa con entusiasmo (incluso obsesivamente) o que disfruta la programación en lugar de simplemente teorizar acerca de la programación" (Jargon File, 2003, traducción propia). Esta definición indica que la palabra *hacker*, entonces, no se refiere a lo que colectiva y periodísticamente está establecido, es decir la de aquella persona que vulnera sistemas informáticos. Por el contrario, se refiere a cualquier tipo de programador que disfruta de explorar los sistemas informáticos y las redes, y que trabaja activamente para desarrollarlos y mejorarlos.

Esta definición no niega la existencia de lo que comúnmente se percibe como *hacker*. El concepto de una persona que utiliza sus conocimientos informáticos con fines criminales, es enfáticamente definido por la comunidad *hacker* como "*cracker*"

(del inglés *crack*, quebrar o romper; y *cracker*, que en inglés medio se usaba para describir a una persona molesta o intrusiva). El Jargon File restringe la definición de *cracker* como “alguien que rompe seguridad en un sistema”, e inclusive aclara sarcásticamente que “aunque a los *crackers* a menudo les gusta describirse como *hackers*, la mayoría de los verdaderos *hackers* los consideran una forma de vida separada e inferior [sic]” (Jargon File, 2003, traducción propia).

Con el riesgo de sonar repetitivo, es necesario entonces repasar estos dos términos. La palabra *hacker* se utilizará a lo largo del trabajo para referirse a aquellos individuos pertenecientes a una cultura que se remonta al ARPANET y los inicios de Internet, que comparten un conjunto de habilidades, valores y creencias relacionadas a la producción de programas informáticos libres, colaborativos y comunitarios, que constituyen la base de lo que Castells (2001) denomina la *cultura de Internet*. Por el contrario, la palabra *cracker* se utilizará para denominar a aquellos individuos o grupos que utilizan sus conocimientos informáticos para penetrar sistemas y realizar ataques informáticos. Esta definición se comenzará a complejizar más adelante, cuando se abordarán este tipo de acciones que vulneran sistemas informáticos, pero los actores que las realizan son agencias estatales de diversos Estados nacionales.

Entonces, retomando el análisis de Castells (2001), además de la cosmovisión tecnocrática y la cultura *hacker*, el tercer factor decisivo en la expansión global de Internet fueron los empresarios emprendedores de Internet. La entrada de actores privados en la ecuación requirió de un proceso de progresiva privatización de los servicios que conformaban ARPANET, y la liberación de las tecnologías de su entorno militar, el cual aconteció durante los años ochenta.

El primer paso en esta dirección tuvo lugar en 1983, cuando ARPANET se encontraba en su mayor expansión hasta la fecha, y el Departamento de Defensa de los Estados Unidos decidió crear, por preocupaciones de seguridad, una red destinada exclusivamente a funciones militares, que se denominó MIL-NET. Por consiguiente, ARPANET pasó a llamarse ARPA-INTERNET, y se destinó a la investigación. El año siguiente, la Fundación Nacional para la Ciencia (NSF: *National Science Foundation*) de Estados Unidos creó su propia red, NSFNET, y en 1988 comenzó a utilizar ARPA-INTERNET como eje troncal (*backbone*). Para 1990, ARPANET estaba tecnológicamente obsoleto, y fue desmontado y transferido desde la órbita del Departamento de Defensa estadounidense a la NSF, liberándolo de su entorno militar y abriéndolo al dominio público. La combinación a principios de los noventa de la

liberación de estos conocimientos, y de un proceso de desregularización generalizada de las telecomunicaciones hizo que la NSF procediera inmediatamente a la privatización de Internet, y fue allí donde el sector privado comenzó a provocar su mayor impacto. Concibiéndolo como un servicio de comunicación revolucionario, y con una concepción comercial, aprovecharon las posibilidades de escalabilidad técnica que los descubrimientos hasta el momento brindaban, y comenzaron a invertir en la expansión global de Internet (Castells, 2001, p. 25-26).

El autor sintetiza este proceso en una frase, sosteniendo que “Internet nació en la insólita encrucijada entre la gran ciencia, la investigación militar y la cultura libertaria” (Castells, 2001, p. 31). Si bien es imposible realizar una sinopsis de la historia de Internet sin dejar por fuera personajes e hitos que lo definieron en su avatar actual, este breve repaso histórico tiene tres objetivos. En primer lugar, muestra cómo esta tecnología, inicialmente orientada al sector militar, recibió aportes del mundo académico, los cuales fueron cambiando su morfología, pero que indudablemente otro hubiese sido el resultado sin la participación académica y luego empresarial en la creación y difusión de Internet. En segundo lugar, y ligado al punto anterior, sirve para reconocer la naturaleza tangible de la gran infraestructura física que se requiere para que Internet, lejos de “ser magia”, sea hoy una red de redes a escala global. Por último, este repaso histórico sirve para ilustrar la esencia de Internet, la diversidad que se formó con la incorporación gradual de nuevos actores, y el carácter descentralizado que obtuvo al expandirse por todo el globo.

2. El ciberespacio

Habiendo esquematizado la naturaleza tangible de esta gran infraestructura comunicacional denominada Internet, es pertinente definir un espacio menos tangible y mucho más abstracto, denominado *ciberespacio*, que es crucial en este análisis ya que es el terreno de juego en el cual se desarrollan la mayoría de los casos abordados en este trabajo de investigación.

En el 2008, el Pentágono reunió un equipo de expertos que tardó más de un año en consensuar una definición del ciberespacio. Acordaron en definirlo como “el dominio global dentro del entorno de la información, conformado por una red interdependiente de infraestructuras de tecnología de la información, que incluyen a Internet, las redes de telecomunicaciones, los sistemas informáticos, y los procesadores y controladores integrados”. En esta amplia definición indica que el ciberespacio es principalmente un

entorno de información virtual, compuesto por datos digitalizados, que se almacenan y se comparten utilizando tecnologías de la comunicación. La cualidad inmaterial de la información circulante hace muy difícil de conmensurar en términos físicos al ciberespacio (Singer y Friedman, 2014, p. 13).

Entonces, si se entiende al ciberespacio como aquel entorno en el cual ocurren las comunicaciones entre redes de computadoras, ¿en qué se diferencia de los ecosistemas creados por otras tecnologías de la comunicación? El principal factor de diferencia es que su naturaleza descentralizada y libre le otorga un dinamismo sin precedentes, que permite no solo la anexión de nuevas tecnologías, sino que hace que la inclusión de un número cada vez mayor de actividades se pueda lograr de manera progresiva y resulte natural (Singer y Friedman, 2014).

Los avances técnicos que se desarrollaron desde la privatización y extensión masiva de Internet hicieron posible que diversas actividades se potenciaran con el uso del servicio. Una de las actividades pioneras en aprovechar el dinamismo de Internet fue el comercio, el cual encontró nuevas estrategias para funcionar, creando inclusive nuevos esquemas comerciales. Si bien son muchas las variables que alteraron al comercio desde la creación de Internet, es útil observar el volumen de productos que se comercializa utilizando esta plataforma. Una de las compañías de comercio electrónico más famosas del mundo, llamada *Shopify*, estima que para 2021, las ventas globales del comercio electrónico alcanzarán los 4.5 billones de dólares (Shopify, 2017). Para ilustrar cuan significativa es esta cifra, representa más que la suma de los PBI del 2017 de Argentina, Brasil, México, Chile y Venezuela.

Sin minimizar la importancia de Internet para la actividad privada en relación al comercio, que se constituye en un tema de investigación profundo y con múltiples aristas, desde la perspectiva de los Estados nacionales también hay diversas actividades que encontraron dinamismo en Internet. Hoy en día casi todos los Estados —nacionales e inclusive subnacionales— cuentan con sus páginas web, ya sea para promover el turismo o para permitir a sus ciudadanos realizar trámites administrativos en línea. La practicidad de Internet volvió natural la inclusión de más actividades estatales en la órbita del ciberespacio: ahora las identidades de los ciudadanos se almacenan en computadoras que están conectadas a Internet; las comunicaciones oficiales, confidenciales o militares se realizan haciendo uso de Internet; y la administración de servicios públicos se agiliza mediante Internet. Si bien es innegable el dinamismo que esta herramienta comunicacional otorga, la inclusión de estas actividades, que son

estratégicas para los intereses de un Estado, hacen que sea crucial entender el funcionamiento de Internet, y la naturaleza del ciberespacio.

Internet abarcó también muchas actividades productivas, y es hoy parte de la mayoría de las industrias, que interconectan sus maquinarias para eficientizar los procesos productivos. Las industrias que con más énfasis se vuelven relevantes aquí son las que conforman la denominada "*infraestructura crítica*" (Singer y Friedman, 2014; Dunn, 2007). Se entiende por infraestructura crítica a aquellos sectores industriales encargados de proporcionar los servicios que subyacen a la civilización moderna, tales como la provisión de energía, la distribución de combustibles, la salud, los servicios bancarios y financieros, o la distribución de alimentos. Todos estos servicios solían mantenerse aislados, pero ahora están todos conectados al ciberespacio a través de Internet.

Desde el punto de vista estratégico, los objetivos más tentadores para quienes desean causar una mayor cantidad de destrucción en una sociedad han sido históricamente estos sectores, ya que tienen la capacidad de disrumpir con el normal desarrollo de sus actividades cotidianas. De esta manera, los ataques perpetrados contra estas industrias tienen un efecto de "multiplicador de la fuerza", lo que permite que un ataque relativamente pequeño cause problemas en cascada en una serie de industrias y afecte la vida de muchas personas, volviéndose especialmente importante la forma en que se administra y se protege la infraestructura crítica conectada al ciberespacio (Dunn, 2007).

Un ejemplo que ilustra de mejor manera la dinámica entre la infraestructura crítica e Internet son los sistemas SCADA. Uno de los dispositivos que más preponderan en las industrias son los sistemas de control industrial (SCADA, de las siglas en inglés de *Supervisory Control And Data Acquisition*). Los sistemas SCADA son dispositivos físicos o programas informáticos que cumplen la función de controlar y monitorear partes específicas de un sistema o proceso industrial. A través de estos sistemas, se pueden administrar desde las válvulas de un sistema de distribución de gas o de agua, hasta la velocidad de rotación de una centrifugadora de uranio. La practicidad de conectar un sistema de control industrial a Internet otorga facilidades, como su interconexión con otros dispositivos similares, o la capacidad de poder operarlo desde otra ubicación geográfica (conocido como *acceso remoto*).

Sin embargo, la contracara de conectar este tipo de dispositivos a Internet es que también implica enfrentarlo a un ciberespacio que cuenta con una gran cantidad y

diversidad de actores. Dentro de estos actores, existen aquellos que podrían beneficiarse al alterar el funcionamiento de un sistema de control industrial de, por ejemplo, un país enemigo. Esto abre peligros potenciales ante atacantes que pueden alterar, mediante programas informáticos maliciosos, el normal funcionamiento de estos dispositivos, lo cual se puede traducir en pérdida de grandes recursos económicos, o aún peor en pérdida de vidas humanas. Como si esta potencialidad no fuera suficiente, BeepingComputer, una revista digital que aborda temáticas de seguridad informática, advierte que la mayoría de los sistemas SCADA son afectados por *malwares* ("virus" de computadora o programas maliciosos, se definirán a continuación) por accidente, ya sea por problemas de segmentación de sus redes, por falta de personal dedicado a la seguridad informática, o por empleados no capacitados en medidas de prevención (BeepingComputer, 2017).

Alguno de los ejemplos más resonantes de ataques a infraestructuras críticas, que se analizarán en detalle más adelante, son *Industroyer*, un malware que provocó apagones de luz en Ucrania en 2014; y aún más ejemplar *Stuxnet*, una serie de ataques con la intención de sabotear las instalaciones de refinamiento de uranio de Irán, llegando a causar inclusive explosiones. El ejemplo de los sistemas de control industrial es uno de los innumerables casos que requieren un análisis profundo a la hora de conectarlos a Internet, pero es abordado aquí como ejemplo por la importancia estratégica que poseen para un Estado.

La potencial vulnerabilidad que adquieren los sistemas informáticos al ser conectados a Internet resalta la relevancia de la seguridad informática, es decir el área de la informática que se encarga de proteger a los sistemas informáticos, y preservarlos frente a las amenazas que puedan surgir ante eventuales hostilidades. La dependencia cada vez mayor de los sistemas digitales significa cada vez más enfrentarse a la pregunta de cómo poder confiar en ellos, y cómo defenderse de potenciales peligros, para lo cual es clave entender el ciberespacio, es decir el terreno de juego en el cual interactúan estos sistemas informáticos.

3. Internet profunda y la *dark web*

Una de las partes centrales del ciberespacio se denomina World Wide Web, y se constituye como la herramienta principal que miles de millones de personas usan para interactuar en Internet. Consiste en un sistema de distribución de documentos visualizables con un programa llamado navegador web (Dewey, 2014), y es

mundialmente reconocido por las tres letras “www.” al inicio de la mayoría de los vínculos que circulan por Internet, los cuales hacen referencia a esta gran plataforma de intercambio, más comúnmente abreviada como Web. Son parte de la Web todas páginas con la que la mayoría de los usuarios interactúan diariamente, desde las redes sociales hasta los periódicos en línea, los servicios financieros y las plataformas de consumo de entretenimiento.

Uno de los servicios que vuelve más dinámica a la Web, y que propició su rápida expansión, es la *indexación*, un proceso que utiliza diversos métodos y técnicas para crear un gran índice de páginas web, lo que permite que la gran cantidad de documentos que existen en la web sean fácilmente encontrados. De este modo, los *buscadores web* (*Google, Yahoo, Bing*) rastrean las páginas web, ven cómo se vinculan con otras páginas web, y van creando así un índice ordenado en el cual se pueden localizar las páginas de manera eficiente. Sin embargo, la mayor parte de la información de la Web está oculta en sitios generados de manera dinámica, para los cuales los motores de búsqueda estándares no han desarrollado técnicas de rastreo (*web crawling*), o bien la cualidad de la información de estas páginas hace que sea muy difícil encontrarlas y sumarlas a sus índices.

Esta parte de la Web se denomina *Internet profunda*, o *deep web*, y son todas aquellas páginas que no pueden ser indexadas y ordenadas por los buscadores, sea porque el contenido es dinámico y cambia constantemente, o porque se requieren contraseñas para acceder a la información que contienen, o bien porque no se encuentran enlazadas con otras páginas. De hecho, una analogía útil para entender cómo funciona la indexación es la de un iceberg, o también comparándola con arrastrar una red por la superficie del mar: se pueden extraer muchos peces (páginas indexadas), pero en realidad hay una gran cantidad de peces a los que la red nunca va a alcanzar por estar más alejados, o en otros niveles (Internet profunda) (Bergman, 2001).

La omisión de la Internet profunda por parte de los motores de búsqueda es, lejos de ser un hecho sospechoso, lo que otorga una capa de seguridad a gran parte de los servicios que conforman la infraestructura de la Web: se manejan allí servicios bancarios, intercambio de archivos secretos usando protocolos seguros, bases de datos privadas, servidores de correos electrónicos, intercambios entre centros de investigación académicos, y todo tipo de información que utiliza la tecnología web, pero que está disponible solo para los usuarios que tengan permisos para accederla. De hecho, se

estima que la información en la Internet profunda es actualmente de 400 a 550 veces más grande que la encontrada en la Web indexada (Bergman, 2001).

Las particularidades que adquieren las técnicas requeridas para acceder a la información almacenada en la Internet profunda difieren de las utilizadas por la mayoría de los usuarios de Internet. Esto hace que las actividades se vuelvan más difíciles de rastrear, y controlar. Esta característica, si bien representa una oportunidad de comunicación para grupos minoritarios perseguidos, o proscriptos políticos; también da lugar al surgimiento de actividades ilícitas, que se benefician de la cualidad aislada e ilocalizable de la Internet profunda.

Esta introducción de la composición de los diferentes sectores del ciberespacio tiene como objetivo presentar a la *dark web* (Web oscura), la cual se conforma como una reducida parte de la Internet profunda, que usualmente requiere programas, configuraciones o autorizaciones mucho más complejos y específicos para su acceso, motivo por el cual se crea un ambiente fértil para el desarrollo de actividades delictivas: tráfico de drogas y armas, fraude, documentos falsos, *botnets*. Este lugar es por lo general confundido con la Internet profunda, por lo que es imperioso aclarar que es sólo una reducida parte de esta Web no indexada. Sin embargo, existe, y es una variable importante para este análisis, ya que se constituye como un “mercado negro”, o una plataforma en la cual muchos *crackers* pueden hacer negocios, en un sector de Internet casi imposible de controlar.

De esta manera, el ciberespacio se vuelve un terreno muy complejo de analizar, donde no sólo hay una multiplicidad de actores interactuantes, sino que también existen una gran cantidad de facetas o niveles (Internet indexada, Internet profunda, *dark web*). Además de la descentralización, comienza a visualizarse otro pilar esencial de Internet, que es la carencia de un control o gobierno centralizado. Este factor no solo es relevante para la conformación del ciberespacio, sino también porque permitirá establecer los principales lazos con la teoría de las relaciones internacionales.

4. La anarquía de Internet

Una estrategia relevante a la hora de evaluar cómo se aborda la protección de la información circulante en Internet, es preguntarse si existe un gobierno o un dueño de Internet, es decir si existe algún ente que tenga la capacidad de controlar el tráfico, y de permitir o denegar la utilización de la infraestructura.

En la encuesta previamente citada, realizada por Code.org (2016), se les pregunta a los peatones estadounidenses “¿quién es dueño de Internet?”. Dentro del rango de respuestas, predominan “el gobierno [estadounidense]”, y “Bill Gates”. Si bien no existen datos para negar estas respuestas terminantemente, en términos académicos y técnicos, Internet no posee un dueño o gobernante formal. Su estructura descentralizada hace que los agentes principales sean los Proveedores de Servicio de Internet (mayormente conocidos como ISP, por las siglas en inglés de Int*ernet Service Providers*), es decir aquellas empresas que se encargan de conectar a los clientes (empresas, hogares, particulares) a Internet. Más allá de estas empresas que proveen el servicio de conexión, no existe un “gobierno” de Internet.

También existen organizaciones que se encargan de regular y coordinar cuestiones organizacionales y estructurales específicas de Internet. Una de las más conocidas es la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés de In*ternet Corporation for Assigned Names and Numbers*). La función de la ICANN es difícil de abordar sin entrar en definiciones técnicas, pero básicamente se encarga de garantizar que cada vez que un usuario quiera acceder a determinado servicio o página web, se pueda conectar de manera rápida y eficiente al servidor que contiene ese servicio. A pesar de ser un ente regulador a nivel mundial, la ICANN es una organización sin fines de lucro que provee un servicio a Internet, y no es —ni pretender ser— gobernante de Internet.

Si bien Internet se identifica por tener esta naturaleza anárquica, no implica un caos o desorden permanente. Al igual que en el sistema internacional, existen determinados estándares y acuerdos globales que coordinan su correcto funcionamiento. Inclusive, al no existir monopolio del servicio, se vuelve un sistema colaborativo donde los actores se encargan de mantener las conexiones activas para que el sistema de comunicación se vuelva eficiente.

Entonces, el escenario resultante de Internet es el de una gran red distribuida a nivel global, con muchos usuarios interconectados, que usan servicios privados llamados ISP para comunicarse dentro del ciberespacio, pero que no están sujetos a leyes internacionales ni a un gobierno centralizado. Esta anarquía puede ser análoga a la encontrada en la teoría neorrealista del sistema internacional planteada por Waltz.

De hecho, Internet encuentra aún más paralelos con el sistema internacional anárquico realista cuando se observan, por ejemplo, las particularidades del Sistema de Nombres de Dominio (DNS, por sus siglas en inglés de *Domain Name System*). El DNS

es parte de la familia de protocolos de Internet (un sistema de estándares que permite el funcionamiento de Internet), y es un sistema de nomenclatura jerárquico y descentralizado para los dispositivos que hagan uso de una red. Su función más importante es asociar nombres comprensibles para las personas con números que identifican los equipos conectados a la red, para lograr conectar y direccionar equipos a nivel global.

Una forma más sencilla de entender al sistema de nombres de dominio es a través de las direcciones físicas: si una persona decide ir a un cine en una ciudad que no conoce, posiblemente se dirija a las páginas amarillas de esa ciudad para averiguar la dirección física de las salas de cine. De manera similar, si una persona trata de acceder a los servicios de YouTube mediante su navegador web escribiendo "www.youtube.com", mandará una solicitud a un servidor DNS que, al igual que las páginas amarillas, indicarán la dirección de IP (número identificador) exacta del servidor que contiene todos los datos de YouTube (en este caso el número es 172.217.30.142, difícil de recordar para las personas cada vez que requieran los servicios de esta plataforma).

Una parte principal del sistema de nombres de dominios son los denominados "dominios de nivel superior", de los cuales los más conocidos y utilizados son ".com", ".org", ".edu" y ".gov" (comercial, organización, educativo y gubernamental, respectivamente). Estos ejemplos mencionados forman parte de la categoría de "dominios de nivel superior genéricos" establecidas por la ICANN. Una segunda categoría establecida por esta organización es la de "dominio de nivel superior geográfico" (ccTLD, por sus siglas en inglés de *Country Code Top Level Domain*), que establece una segmentación de los dominios por países (ICANN, 2012). Haciendo uso del estándar de códigos de países ISO 3166-1 (International Organization for Standarization, 2018), la ICANN colabora con la coordinación de los dominios geográficos con cada país o territorio independiente, permitiendo que ".at" esté bajo el control de Austria, ".es" de España, ".br" de Brasil, y así sucesivamente.

Si bien el sistema de ccTLD parece una cuestión exclusivamente técnica, trasluce un factor central para el análisis de las relaciones internacionales en el ciberespacio. Al dividir los dominios por países, la ICANN provocó una sectorización *de facto* de Internet en diferentes zonas geográficas, reforzando la idea de Singer y Friedman (2014, p. 13-15) de que, si bien Internet es global, no está desnacionalizado. Estos autores sostienen que, así como la infraestructura física de Internet está vinculada a la geografía, las estructuras nacionales se extienden al ciberespacio; y así como los

seres humanos son los usuarios de esta infraestructura, también nociones humanas como la soberanía, la nacionalidad y la propiedad son parte del ciberespacio. De hecho, los autores sostienen que la particularidad que tiene Internet es que los recursos digitales no son escasos, a diferencia de los recursos tradicionales, por lo que las cuestiones principales de la gobernanza de Internet son la interoperabilidad (cómo se intercambia la información) y la comunicación, más que el clásico problema de la distribución de recursos. Sin embargo, a pesar de esta aparente infinitud de los recursos digitales, sostienen que las cuestiones tradicionales de gobernanza del mundo material también tienen lugar en el ciberespacio, incluidas la representación, el poder y la legitimidad (Singer y Friedman, 2014, p. 25-26).

De esta manera, el ciberespacio se configura de manera muy similar al sistema internacional: múltiples actores con diferentes capacidades, en una búsqueda de equilibrio constante provocado por un estado generalizado de anarquía. Un caso significativo para ilustrar la puja por representación y legitimidad en el ciberespacio se puede observar con el dominio de nivel superior geográfico ".eh", correspondiente al territorio de Sahara Occidental. Este territorio es disputado hace más de cuarenta años por Marruecos, por un lado, y por la República Árabe Saharaui Democrática por el otro. En este momento, la administración del dominio ".eh" corresponde a la República Árabe Saharaui Democrática, pero, ¿qué pasaría si Marruecos, que entiende a Sahara Occidental como una continuación de su territorio, reclama la administración del dominio? La línea se vuelve muy delgada, y comienza a tomar pertinencia en las relaciones internacionales como un conflicto diplomático convencional.

Estados Unidos es uno de los países que más énfasis ha puesto en la definición y el abordaje estratégico del ciberespacio, y que más fomenta la segmentación territorial del ciberespacio. De hecho, el Departamento de Seguridad Nacional de los Estados Unidos (encargado de la esfera civil y nacional) emitió una "Estrategia Nacional para Asegurar el Ciberespacio", mientras que el Pentágono (es decir el Departamento de Defensa Estadounidense, encargado de acciones militares e internacionales), tiene su "Estrategia para Operar en el Ciberespacio", en la cual lo define como un elemento estratégico:

> "El ciberespacio es una característica definitoria de la vida moderna. Las personas y las comunidades de todo el mundo se conectan, socializan y se organizan a través del ciberespacio. Entre 2000 y 2010, el uso mundial de Internet aumentó de 360 millones a más

> de 2 mil millones de personas. A medida que el uso de Internet continúa expandiéndose, el ciberespacio se irá insertando cada vez más en el tejido de la vida cotidiana en todo el mundo" (Departamento de Defensa de los Estados Unidos, 2011, p. 1).

Por otro lado, la República Popular China posee una "Administración del Ciberespacio de China", una agencia gubernamental encargada exclusivamente de regular, controlar y hasta censurar el tráfico del ciberespacio chino. Estas definiciones y acciones emprendidas tanto por Estados Unidos como por China reflejan la relevancia que tiene el ciberespacio para las principales potencias económicas y geopolíticas del siglo XXI.

De este modo, el ciberespacio se alza como un nuevo y complejo terreno para analizar las relaciones intergubernamentales, en las cuales —como se observó con los ccTLD— cada Estado tiene su zona de control y soberanía, pero que se rige bajo un régimen puro de anarquía y de puja constante de poderes e intereses, fiel reflejo del sistema internacional realista.

III. Ofensivas y defensivas en el ciberespacio: ataques informáticos y Seguridad Informática

El poder ejecutivo estadounidense redacta de manera periódica un documento denominado "Estrategia de Seguridad Nacional", en el cual expresa al Congreso estadounidense las mayores preocupaciones en términos de seguridad nacional, y cómo cada administración planea lidiar con ellas. Durante la administración del expresidente Barack Obama, su *Estrategia de Seguridad Nacional* sostuvo que: "las amenazas de seguridad cibernética representan uno de los desafíos más serios de seguridad nacional, seguridad pública y economía que enfrentamos como nación" (Gobierno de Estados Unidos, 2010, p. 27). Esta noción no solo le otorga un lugar preponderante a la seguridad informática en la agenda estadounidense, sino que también es vista como una constante, al ser inclusive continuada por la administración de Donald Trump, un gobierno republicano cualitativamente disímil a la administración demócrata de Obama. En la Estrategia de Seguridad Nacional del 2017, la administración Trump también enfatizó el peligro de las "actividades cibernéticas maliciosas" para las infraestructuras comerciales, gubernamentales y militares (Gobierno de Estados Unidos, 2017, p. 13).

Del otro lado del globo, el gobierno chino elaboró en 2017 la *Ley de Seguridad Informática de la República Popular de China*, la cual establece estrategias a nivel Estatal referidas a la seguridad informática. Si bien la administración que China realiza de su ciberespacio, con un férreo control sobre el tráfico de datos, será analizada más adelante, es interesante observar cuáles son las prioridades que establece en su agenda de seguridad. En la Ley mencionada, se sostiene que "la seguridad informática se ha convertido en un problema importante que afecta la seguridad nacional y el desarrollo, y tiene relación con los intereses vitales de las personas". De este modo, enfatiza la necesidad de profundizar las estrategias de seguridad informática para evitar que "actividades ilegales como la intrusión de redes y ataques cibernéticos amenacen seriamente la seguridad de la infraestructura de la información en campos importantes como las telecomunicaciones, la energía, el transporte, las finanzas y la defensa" (Comité Permanente de la Asamblea Popular Nacional, 2017).

Las principales potencias del sistema internacional, que consiguientemente son las pioneras en desarrollos tecnológicos, están enfatizando cada vez más la relevancia de la seguridad informática en la agenda geopolítica, por lo que es un tema cada vez más presente en las relaciones internacionales. Es muy importante entonces definir con precisión qué es la seguridad informática, cuál es su rol, y cuáles son los principales ataques informáticos que existen.

1. La definición de Seguridad Informática

La seguridad informática, también referida como ciberseguridad, es el área de la informática que se enfoca en la protección de las infraestructuras computacionales de ataques digitales, y su rol es proteger especialmente la información almacenada en una computadora, o circulante a través de una red de computadoras. Para lograr este objetivo, hace uso de una serie de métodos, reglas y protocolos concebidos para minimizar los posibles riesgos a la infraestructura o a la información contenida en ella.

Previamente se sostuvo que la seguridad informática es, en el siglo XXI, una prioridad en las agendas de seguridad globales, y que al ser una disciplina tan alejada de los estudios clásicos de Defensa y de relaciones internacionales, requiere de una gran precisión conceptual para hacer un abordaje interdisciplinario serio de la temática. Uno de los puntos principales en referencia a esto es lograr una definición integral de la seguridad informática, y poder establecer las diferencias con disciplinas similares.

Respecto a la precisión de los conceptos utilizados, Schatz, Bashroush y Wall sostienen que la terminología utilizada para analizar los aspectos de seguridad de los dispositivos digitales y la información ha cambiado considerablemente en los últimos años. A principio de siglo, “seguridad de la información”, “seguridad informática” y “ciberseguridad” se usaban de manera intercambiable. Sin embargo, los avances técnicos que acontecieron hasta la actualidad requieren una precisión conceptual mayor al momento de abordar estas temáticas, sobre todo cuando su uso profundiza ambigüedades en los tribunales de justicia, las estrategias nacionales de seguridad informática, o los tratados internacionales (Schatz et al., 2017, p. 53-55). Con este fin, y lejos de recaer en meras discusiones semánticas, la principal distinción a establecer es la que existe entre *Seguridad Informática* y *Seguridad de la Información*.

La “Seguridad de la Información” se refiere a la práctica de proteger la información en general, independientemente de su cualidad analógica o digital, y tradicionalmente gira en torno a garantizar la *confidencialidad*, la *integridad* y la *disponibilidad* de la información. La confidencialidad se refiere a mantener los datos privados, es decir que esa información no esté disponible ni se divulgue a personas, entidades o procesos no autorizados. La integridad de la información es lo que Singer y Friedman (2014, p. 35) entienden como la parte más sutil de la tríada mencionada, ya que implica garantizar que los datos no hayan sido alterados o modificados indebidamente sin autorización. Por último, la disponibilidad implica que la información se encuentre siempre a disposición de quienes deben acceder a ella.

Además de la confidencialidad, integridad y disponibilidad de la información, hay un cuarto concepto que las prácticas de seguridad de la información apuntan a garantizar: la *irrefutabilidad*. Esta variable, si bien no está incluida en las definiciones clásicas de seguridad de la información, se configura como esencial, y refiere a la capacidad de un sistema de información de dar pruebas sobre acciones —u omisiones— de los distintos actores que lo integran. Si bien a simple vista la noción de la irrefutabilidad parecería componer el principio de integridad de la información, tiene una connotación diferente al garantizar el *no repudio*[1] de la información: si un actor con permisos de acceso a determinada información decide, por ejemplo, modificar su contenido, deben existir pruebas y registros que demuestren qué se modificó, cuándo y

1 El *no repudio* en criptología refiere a la incapacidad de cualquier actor de negar la validez de la información, debido a la existencia de pruebas del origen de los datos y su integridad.

por quién; así como, en el caso contrario, pruebas que garanticen que la información contenida no ha sido alterada.

La garantía de la confidencialidad, la integridad y la disponibilidad de la información, también conocidos tradicionalmente como la "tríada de la CIA" (por las siglas en inglés de *Confidentiality, Integrity* y *Availability*), sumado a la irrefutabilidad de los sistemas de información, componen el núcleo de la *Seguridad de la Información*. Sin embargo, esta disciplina tiene una particularidad, ya que no se restringe exclusivamente a la información digital. De este modo, la seguridad de la información es la práctica de garantizar que determinada información, tanto física como digital, esté protegida contra el uso, acceso, interrupción, inspección, modificación, destrucción o grabación no autorizados.

La *Seguridad Informática*, se ubica en un nivel más específico, ya que es la práctica de proteger sistemas, redes y programas informáticos de ataques digitales, mediante la implementación de diversas prácticas, procesos y tecnologías. Un abordaje integral de seguridad informática contiene múltiples estratos de protección, siendo relevantes no solo la defensa técnica de las tecnologías (computadoras, redes), sino también la capacitación de las personas que hacen uso de estas tecnologías, y la existencia de procesos y planes de respuesta ante eventuales ataques informáticos.

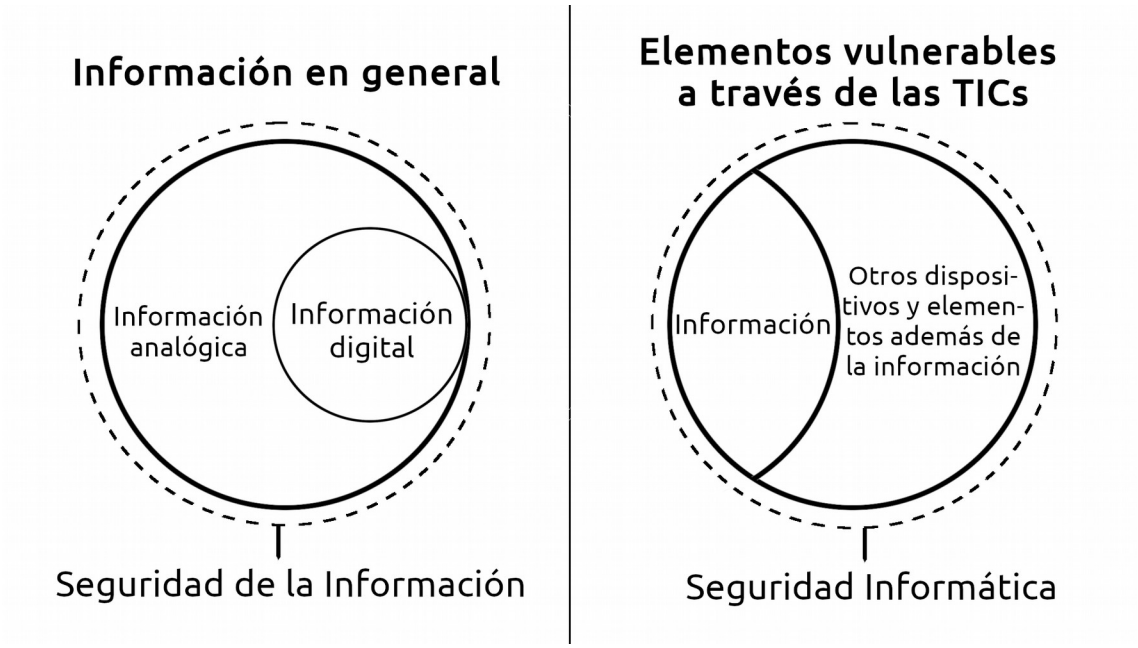

Ilustración 3: Seguridad de la Información vs. Seguridad Informática. Fuente: elaboración propia en base Schatz, Bashroush y Wall (2017, p. 53-55).

Un factor que es importante de resaltar para establecer la distinción con la seguridad de la información, es que la seguridad informática es un conjunto de prácticas

que se restringen exclusivamente a la protección de *información digital*, por lo que la seguridad de la información va más allá de la seguridad informática al abarcar la protección de la información en otros medios no digitales. Si se concibe a la seguridad informática como una disciplina que protege sistemas informáticos que contienen información, se la puede ubicar como una parte de la Seguridad de la Información, pero no se encarga de proteger la información *per se*, sino a los sistemas que la contienen y transportan (ver ilustración 3).

Este trabajo de investigación utilizará la definición de Seguridad Informática propuesta por Schatz, Bashroush y Wall, que pretende ser más abarcadora y representativa que las definiciones tradicionales:

> "La Seguridad Informática se refiere al enfoque y las acciones asociadas con los procesos de gestión de riesgos de seguridad, que son seguidos por organizaciones y Estados para proteger la confidencialidad, la integridad y la disponibilidad de los datos y los activos utilizados en el ciberespacio. El concepto incluye directrices, políticas y conjuntos de salvaguardas, tecnologías, herramientas y capacitación para proporcionar la mejor protección para el estado del entorno cibernético y para sus usuarios" (Schatz et al., 2017, p. 66).

Una característica subyacente y tácita de la seguridad informática es su *proactividad*, ya que como sostienen Singer y Friedman (2014, p. 34) la palabra "seguridad" no solo implica la noción de estar libre de peligro, sino que está asociada a la presencia de un adversario. De este modo, todas las estrategias de seguridad informática, se plantean para combatir o prevenir diferentes tipos de estrategias informáticas ofensivas que tiendan a penetrar un sistema informático. Por consiguiente, antes de plantear las estrategias de seguridad informática, es necesario realizar una introducción de los diferentes avatares que pueden tomar las amenazas y los ataques en el ciberespacio.

2. Los diferentes tipos de ataques informáticos

Cisco, la compañía de redes más grande del mundo, que desarrolla, fabrica y vende dispositivos de redes, equipos de telecomunicaciones y productos de alta tecnología, define un ataque informático como "*un intento malicioso y deliberado de un individuo o una organización de violar un sistema de información*" (Cisco, 2018).

Siguiendo esta definición, un ataque informático es plausible de ser llevado a cabo tanto por una persona individual, como por grupos, organizaciones, o inclusive Estados nacionales. Como si la cantidad posible de actores que pueden perpetrar un ataque informático no fuera suficiente, existe inclusive la posibilidad de que un ataque pueda originarse —al haber diversas herramientas para enmascarar las identidades en línea— de fuentes anónimas, y en diversas ubicaciones geográficas.

El Comité de Sistemas de Seguridad Nacional de los Estados Unidos, una organización intergubernamental de que establece políticas para la protección de los sistemas de seguridad estadounidenses, aporta una definición más elaborada de un ataque informático:

> "[es] un ataque, a través del ciberespacio, dirigido al uso que una empresa[, Estado o individuo] hace del ciberespacio, con el fin de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno o infraestructura informática; o destruir la integridad de los datos o robar información controlada" (Committee on National Security Systems, 2010, p. 22, traducción propia).

Resulta pertinente aclarar que, si bien se refiere a la destrucción o robo de información, lo hace siempre en referencia a información digital, habiendo mencionado que estas acciones se realizan en el ciberespacio, por lo que los ataques informáticos son pertinentes al área de la seguridad informática y no a la seguridad de la información, como podría interpretarse por la referencia a la mención de "protección de información".

Singer y Friedman (2014, p. 68-72) sostienen que el ciberespacio redefine los esquemas preexistentes sobre las cualidades de un ataque, y establecen parámetros para determinar las propiedades de un ataque informático. En primer lugar, sostienen que, por definición, los ataques informáticos se diferencian de un ataque tradicional por los medios que emplea: en lugar de fuerza cinética, se utilizan *medios digitales*. Esto, que parece ser evidente, no debe ser minimizado, ya que da lugar a un nuevo espectro de implicancias:

> "un ataque cibernético no está restringido por la física habitual de los ataques tradicionales, […] un ataque puede moverse literalmente a la velocidad de la luz, ilimitado por geografía

> y límites políticos […] lo que también implica que el mismo ataque puede alcanzar múltiples objetivos a la vez" (Singer y Friedman, 2014, p. 68, traducción propia).

Asimismo, los autores agregan que los costos para realizar un ataque físico fueron históricamente la compra de armas físicas y sus materiales, mientras que en los ataques informáticos los costos se expresan del lado de la investigación y el desarrollo, y una vez que se encuentran desarrollados, no se necesita más que "*copiar y pegar*" su código para reproducirlo (Singer y Friedman, 2014, p. 69).

En segundo lugar, sostienen que, como resultado de esta cualidad virtual de los ataques, los objetivos son también virtuales, motivo por el cual, por lo general, no siempre se puede saber cuál va a ser el resultado de un ataque informático, a qué computadora se va a expandir, ni donde puede terminar. De este modo, afirman que la diferencia entre un ataque tradicional y un ataque informático es que *tanto sus medios como sus objetivos son digitales*, más allá de las implicancias que pueda tener en el mundo material (Singer y Friedman, 2014, p. 69).

Sumado a esta variable inmaterial, la capacidad de algunos ataques informáticos de operar camuflados como programas legítimos, hacen que sea muy difícil su detección. En relación a esto, FireEye, una compañía estadounidense dedicada a proveer servicios de seguridad informática, afirma en su informe anual de amenazas informáticas, que la mediana del tiempo de permanencia de un ataque informático (es decir el número de días que pasa entre la primera evidencia de compromiso de un sistema informático, hasta su detección) en empresas de todo el mundo fue en el 2017 de 101 días. Inclusive demuestran que este valor no se modificó mucho en los últimos años, siendo que la mediana del tiempo de permanencia de un ataque informático fue de 99 días en 2016, y de 146 días en 2015 (FireEye, 2018, p. 4).

Estas cifras, si bien se restringen al sector privado, demuestran de qué manera el desconocimiento generalizado de los ataques informáticos, y la carencia de políticas de seguridad informática se traducen en una exposición de los sistemas informáticos a las amenazas provenientes del ciberespacio. Que un *malware* se encuentre activo durante cien días en los sistemas informáticos de una empresa hasta su detección significa grandes perjuicios económicos, pero si se reproduce una situación en sistemas informáticos de un Estado, los riesgos se extienden a toda su población.

En relación a lo previamente mencionado sobre la necesidad de establecer terminologías acordes y precisas, Singer y Friedman sostienen que intentar hablar sobre un nuevo problema o tema, como el que representa los ataques informáticos, puede ser un poco como viajar a un país extranjero. Las nuevas discusiones requieren nuevos vocabularios y marcos para comprender lo que está sucediendo, y esta situación se puede intensificar y volverse aún más compleja en el ámbito de los problemas en el ciberespacio, ya que los temas mezclan asuntos altamente técnicos con conceptos amplios, en los que incluso los términos más básicos pueden estar cargados de otro significado (Singer y Friedman, 2014, p. 67).

De este modo, al existir la posibilidad de que un ataque informático se convierta en una potencial arma que puede vulnerar la capacidad, no solo de empresas sino también de Estados nacionales, de acceder al ciberespacio y a información estratégica, se vuelve nodal definir con la mayor precisión posible los principales tipos de ataques informáticos. Así, como es necesario para los intereses de Defensa de un Estado distinguir entre una bala de un rifle, un misil intercontinental y un submarino, la definición de las diferentes herramientas que pueden vulnerar las defensas informáticas de un Estado se vuelve crucial para plantear estrategias de seguridad en el ciberespacio.

a) Malwares

La palabra *malware* es el acrónimo de "*malicious software*", *programa informático malicioso* en inglés, y es definido por Microsoft como "un término que se utiliza de manera general para referirse a cualquier programa informático diseñado para causar daños a una computadora, un servidor o una red informática" (Moir, 2003). Típicamente, un *malware* logra realizar daño una vez que fue introducido en un sistema informático, y puede tomar la forma de un código ejecutable, *script,* o un programa más dentro del sistema.

Es importante resaltar, en primer lugar, que si bien las aplicaciones o programas informáticos también pueden crear vulnerabilidades si están mal configuradas, un *malware* es un programa cuyo código está específica e intencionalmente diseñado para causar daños en un sistema informático (Singer y Friedman, 2014, p. 41). En segundo lugar, es necesario aclarar que, dentro de la categoría de *malware,* se han creado muchas tipologías para categorizarlos según su funcionamiento. La realidad es que, en la práctica, la mayoría de estos programas maliciosos terminan volviéndose difíciles de

encapsular en definiciones taxativas, y el hecho de que un *malware* pueda utilizar múltiples técnicas hace que las categorías no sean mutuamente excluyentes.

Los principales tipos de *malware* según su funcionamiento son:

- *Gusano informático:* (usualmente conocido como "*worm*", *gusano* en inglés) tiene la propiedad y el objetivo de multiplicarse a sí mismo de manera constante, usualmente a otras computadoras dentro de la red en la cual la computadora infectada se encuentra. El mayor peligro que recubre este tipo de programa es que una vez que un usuario lo pone en acción, tiene la capacidad de expandirse sin que el resto de los usuarios de la red lo autorice o siquiera lo noten. Es una funcionalidad muy utilizada en un tipo de ataque informático denominado *ransomware* (Barwise, 2010).
- *Virus:* tiene el objetivo de alterar el normal funcionamiento de cualquier tipo de dispositivo informático, modificando los programas instalados. Usualmente, al ejecutarse, el programa malicioso toma control de las funciones principales del sistema operativo, se encarga de infectar el sistema con los archivos necesarios para su funcionamiento, y puede tener objetivos muy variados, desde alterar el normal funcionamiento, hasta eliminar datos.
- *Troyano:* es una de las técnicas más utilizadas, y su nombre es una alegoría a la historia del caballo de Troya mencionado en la *Odisea* de Homero: el programa simula cumplir determinada función específica, engañando al usuario para que lo instale. Sin embargo, una vez que se encuentra instalado en el sistema, ejecuta código malicioso que puede, entre otras cosas adquirir funcionalidades de *virus* o de *gusano informático*. La cualidad diferencial de este tipo de técnica es que oculta las verdaderas intenciones del programa al usuario, el cual no lo ejecutaría si las conociera (Universidad de Indiana, 2018).
- *Spyware:* en español significa "programa espía", y apunta a recolectar información sobre el usuario sin su consentimiento, para luego transmitirla a una entidad o servidor externo.
- *Adware:* muestra publicidad no deseada en el dispositivo infectado, con el fin de generarle lucro a sus autores.
- *Keylogger:* tiene la función de registrar las pulsaciones que se realizan en el teclado, para posteriormente ser enviado al *cracker* que lo creó, usualmente con el objetivo de robar contraseñas e información confidencial.

- *Rootkit:* es una de las técnicas más nocivas, ya que es un programa malicioso que una vez instalado en un dispositivo, se oculta y reserva *permisos de administrador* de manera continua (para cambiar cualquier configuración en el sistema, o alterar el funcionamiento de algún programa), corrompiendo así al sistema operativo y sus funcionalidades.

Si bien esta lista no incluye todos los tipos de *malware* que se pueden encontrar, sí son las funcionalidades más utilizadas por los programas maliciosos. Es significativo volver a remarcar que estas categorías no son mutuamente excluyentes, por lo que un *malware* puede contar con múltiples de las mencionadas funcionalidades. Para ilustrar este hecho, se puede observar uno de los *malware* más famosos de principios de siglo: *ILoveYou*. Este programa malicioso tenía la funcionalidad principal de *gusano informático*, ya que era un correo electrónico cuyo asunto rezaba "ILOVEYOU" (TEAMO en inglés), y que contenía un archivo adjunto: "LOVE-LETTER-FOR-YOU.txt.vbs" (*CARTA-DE-AMOR-PARA-VOS.txt.vbs* en español). Los usuarios, pensando que era un archivo de texto, lo abrían, e inmediatamente se ejecutaba un *script* que activaba funcionalidades de *virus*, ya que dañaba archivos en el sistema; pero también funcionalidades de *gusano informático*, ya que se reenviaba automáticamente a todos los contactos de la agenda de correos electrónicos del usuario (Lemos, 2000).

De este modo, *IloveYou*, haciendo uso de un ataque *phishing* (abordado más adelante), tenía funciones de *virus* y de *gusano informático*, y fue uno de los primeros *gusanos informáticos* en expandirse de manera exponencial y a escala global: llegó a infectar hasta 50 millones de computadoras, y provocó pérdidas por más de 5.500 millones de dólares. Si bien este *malware* fue relativamente inofensivo, en la actualidad existen programas que tienen intenciones mucho más nocivas, y utilizan una combinación mucho más elaborada de las herramientas previamente descritas para lograr su cometido.

Por definición, los *malware* son programas que alteran el funcionamiento de un sistema informático, y no necesariamente son programas desarrollados por *crackers*. En 2005, la compañía *Sony Music*, en aquel momento *Sony BMG*, protagonizó un escándalo al implementar medidas ilegales de protección de copias en alrededor de 22 millones de CDs. Cuando los CDs eran insertados en una computadora con el sistema operativo *Windows*, instalaba sin permiso de los usuarios un programa que proporcionaba gestión de derechos digitales (DRM), y que modificaba al sistema operativo al impedir las funcionalidades de copia de CDs. El problema de esta utilidad

desarrollada por *Sony*, es que no solo se volvía un *rootkit* al alterar las capacidades del sistema operativo, sino que tampoco podía ser desinstalado por el usuario, y también adquirió funcionalidades de *spyware*, al descubrirse posteriormente que enviaba información a los servidores de *Sony* (Schneier, 2005).

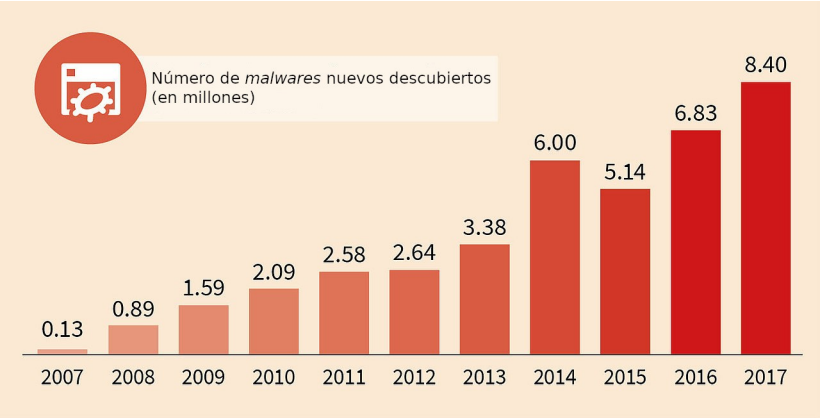

Ilustración 4: Fuente: G Data Software (Benzmüller, 2018)

La incorporación constante de nuevos dispositivos a Internet, desde computadoras a teléfonos móviles, *tablets*, y todos los artefactos comprendidos dentro del paradigma de *Internet of Things*, hace que los *crackers* realicen cada vez más intentos por vulnerar los dispositivos mediante programas maliciosos. De hecho, la empresa alemana de seguridad informática G Data Software sostiene que en 2017 se descubrieron 8.4 millones de *malware* nuevos: un promedio de 959 ejemplares descubiertos por hora, 63 veces más que los descubiertos en 2007 (Benzmüller, 2018).

De hecho, *G DATA Sotware* aclara que, con la inclusión de los dispositivos móviles en la ecuación, se descubre un nuevo *malware* cada 10 segundos (Lueg, 2018). Indudablemente, ante este amplio abanico de estrategias ofensivas, visto desde los intereses de un Estado, se vuelve estratégico el rol de la seguridad informática en la protección de los dispositivos y las redes que contengan información confidencial o sensible frente a los ataques de *malwares*.

b) Phishing

Conocido como *suplantación de identidad*, adquiere ese nombre ya que es un homófono de la palabra *fishing* (*pescar* en inglés), y es una analogía al uso de una carnada o un cebo en el intento de atrapar a una víctima desprevenida. La práctica del *phishing* consiste en enviar comunicaciones digitales fraudulentas, que parecen provenir de una fuente confiable, para adquirir información confidencial de alguna persona u organización (Cisco, 2018). Esta técnica es uno de los ataques informáticos más

extendidos, y generalmente se realizan a través de servicios de mensajería instantánea o de correo electrónico.

Un típico mensaje de *phishing* puede hacerse pasar por el correo electrónico de un banco, un organismo estatal, o una empresa de renombre, que lleva al usuario a ingresar información privada en sitios web que simulan ser legítimos, para obtener datos personales, como números de tarjetas de crédito (conocido típicamente como *pharming*). También, los correos electrónicos de *phishing* son famosos por contener archivos adjuntos maliciosos, o por dirigir a los usuarios a páginas infectadas que distribuyen *malwares*.

La cualidad que tienen los ataques de *phishing* es que son mensajes que se distribuyen de manera generalizada, esperando que un usuario descuidado caiga en la trampa. Como se mencionó, el objetivo primordial de las técnicas de *phishing* suele ser obtener credenciales de acceso a servicios bancarios y a los números de las tarjetas de crédito. De hecho, en el 2007, el 80% de las marcas y empresas falsificadas en ataques de *phishing* fueron del sector financiero. A parte de sitios financieros, también se han visto ataques que falsificaban páginas de proveedores de servicio de Internet, comercios, seguros, y comunidades de Internet (Stamp y Stavroulakis, 2010, p. 437-438). La insistencia de los *crackers* en obtener específicamente este tipo de datos mediante técnicas de *phishing* no es por un rédito personal, sino que se debe también a la existencia de un gran mercado que demanda este tipo de información robada, en la *dark web*.

Más allá del lucro económico que un *cracker* pueda obtener con información robada mediante un ataque *phishing*, es necesario concebir que podría pasar en casos más elaborados. Por ejemplo, es imaginable el peligro que significaría que el empleado de una entidad bancaria infecte sin intención la red local de esa institución financiera, comprometiendo los datos privados de los clientes del banco. Este peligro se multiplica cuanto más sensible es la información a la cual estos ataques pueden tener acceso.

Desde el punto de vista de los intereses estratégicos de Defensa de un Estado, es imperioso contemplar las vulnerabilidades que un ataque de *phishing* podría introducir mediante un simple correo electrónico malicioso, en, por ejemplo, un sistema informático que contenga información digital sensible sobre la identidad de sus ciudadanos, proyectos de infraestructura, o inclusive información confidencial de negociaciones internacionales. Si bien los ataques de *phishing* son cada vez más comunes y hay estrategias para identificarlos, siguen siendo los más extendidos y

usados por su efectividad. Por este motivo, no hay que desestimarlos, ya que pueden servir de puertas de entrada para ataques informáticos más complejos y nocivos, tales como amenazas persistentes avanzadas (APTs) o *ransomwares* (Cisco, 2018).

El *phishing* es una de las prácticas más representativas de lo que en el contexto de la seguridad de la información se conoce como *ingeniería social*, es decir la manipulación psicológica de las personas para realizar acciones o divulgar información confidencial. El uso de la ingeniería social para engañar a los usuarios y explotar las debilidades técnicas de la seguridad de un sistema informático es plausible ser abordada y prevenida con legislaciones, capacitaciones y difusión, pero en última instancia recae en la capacitación técnica en seguridad informática del usuario final que utiliza un servicio.

Si bien existen una gran cantidad de variantes y técnicas para realizar ataques de *phishing*, una de las más relevantes para este análisis es la denominada *spear phishing* (del inglés *pesca con arpón*). A diferencia de los ataques de *phishing* tradicionales, que como se mencionó son enviados de manera masiva en el intento de atrapar víctimas desprevenidas, los ataques de *spear phishing* requieren una un grado mayor de investigación sobre el objetivo antes de ser ejecutados, ya que son ataques de *phishing* cuidadosamente diseñados para atraer a una persona u organización específica a, por ejemplo, descargar un archivo adjunto malicioso o hacer clic en un enlace malicioso (Dimov, 2015).

Uno de los casos más actuales y resonantes de *spear phishing* cobró relevancia en las elecciones presidenciales de 2016 en los Estados Unidos, en la cual se filtraron correos electrónicos de funcionarios de alto rango del Comité Nacional Demócrata, comprometiendo la campaña presidencial de la candidata demócrata Hillary Clinton. El grupo de *crackers* rusos *Fancy Bear*, denominado por Estados Unidos como "*Threat Group-4127*", admitió haber realizado *spear phishing* durante el primer trimestre de 2016 a direcciones de correo electrónico asociadas con el Comité Nacional Demócrata. Realizando una investigación sobre las plataformas de comunicaciones utilizadas por los principales funcionarios del Comité, los *crackers* engañaron a integrantes de alto rango para que ingresaran sus credenciales en páginas maliciosas, que aparentaban ser las páginas de acceso de *Gmail* que utilizaban diariamente (Secureworks, 2016).

El resultado de este ataque de *spear phishing* fue la filtración masiva de más de 30.000 correos electrónicos, los cuales fueron publicado por la organización *WikiLeaks* a lo largo del 2016, y que siguen estando disponibles e indexados públicamente

(WikiLeaks, 2018). Si bien es un caso puntual de *spear phishing* que no parecería tener relación con los intereses de Defensa de un Estado, con estas filtraciones se evidenció la utilización del correo personal de Clinton —Secretaria de Estado de los Estados Unidos en el momento que se enviaban dichos correos— para manejar información clasificada, volviéndose de carácter público negociaciones y secretos de Estado que deterioraron su imagen pública durante la campaña electoral (BBC, 2016).

Este caso es muy relevante para este trabajo de investigación, y será analizado más adelante, ya que un engaño virtual de *spear* phishing se tradujo en un conflicto diplomático que se extendió inclusive hasta luego de las elecciones, ya que los Estados Unidos continúan en el 2018 acusando al gobierno de Rusia de filtrar los correos electrónicos de Hillary Clinton para deteriorar su imagen positiva, y fortalecer la campaña de Donald Trump durante las elecciones de 2016 (Hacquebord, 2017).

c) Ataques de Denegación de Servicio (DoS) y de Denegación de Servicio Distribuido (DDoS)

Usualmente conocido como ataque DoS, por sus siglas en inglés de *Denial of Service*, un ataque de denegación de servicio consiste en enviar a una computadora, servidor o recurso, una cantidad suficiente de solicitudes superfluas, como para que el sistema se sobrecargue y no sea capaz de responder a las solicitudes de los usuarios legítimos del servicio. En general, lo que sucede a nivel técnico es que el servidor atacado no puede dar respuesta a las solicitudes, y deja de funcionar (*crash*), o bien las solicitudes sobrepasan la capacidad del ancho de banda de la red donde se encuentran alojados los servicios, volviéndolos lentos o inclusive inaccesibles (National Cybersecurity and Communications Integration Center, 2009).

Un ataque de denegación de servicio distribuido (DDoS, por sus siglas en inglés de *Distributed Denial of Service*) es un tipo de ataque DoS que ocurre cuando son varias las computadoras que trabajan juntas para atacar un objetivo. En un ataque DoS tradicional, las solicitudes y paquetes que se envían al objetivo provienen de una sola computadora, por lo que al bloquear la fuente de los ataques (usualmente la dirección de IP), se soluciona rápidamente la sobrecarga del servicio. Por el contrario, en un ataque DDoS, el tráfico que inunda al servidor o red víctima proviene de múltiples fuentes, y vuelve muy difícil la tarea de detener el ataque bloqueando la gran cantidad de fuentes individuales (National Cybersecurity and Communications Integration Center, 2009).

Un ejemplo que puede ilustrar el accionar de un ataque DDoS es el siguiente: si se les pide a 1000 personas que llamen de manera constante al número de teléfono de un individuo que usa su teléfono para realizar 10 llamadas por día, podrían suceder dos cosas. En primer lugar, por más que ese individuo tenga la intención, no podrá responder a todas las llamadas por una cuestión de capacidad de respuesta. En segundo lugar, lo que posiblemente sucedería es que ese individuo tampoco pueda utilizar su línea para realizar las 10 llamadas que realiza comúnmente por día, ya que el volumen de llamadas entrante abrumaría su línea telefónica.

Los atacantes que implementan técnicas de DDoS suelen aprovechar el uso de grandes redes de dispositivos infectados que pueden ser controlados remotamente, denominadas *botnets*. Aprovechando las vulnerabilidades de seguridad de muchos dispositivos, algunos atacantes infectan dispositivos mediante *malwares* que luego permiten su uso remoto. La conjunción de muchos de estos dispositivos infectados, controlados remotamente, se denomina *botnet* (red de robots, del inglés, conjunción de "*bot*", abreviatura de "robot", y "net", que significa "red"), y puede ser utilizada por un atacante para realizar un ataque DDoS sobre un objetivo, desde múltiples dispositivos y fuentes geográficas (National Cybersecurity and Communications Integration Center, 2009). Las *botnets*, si bien no son un requisito necesario para realizar este tipo de ataque distribuido, aumentan significativamente la efectividad de un ataque DDoS, y son herramientas que inclusive están disponibles para ser alquiladas por tiempo en la *dark web*.

También existen herramientas de público dominio muy fáciles de descargar, instalar y usar para un usuario promedio, que permiten realizar ataques DoS desde una computadora personal. Una de las herramientas de este tipo más conocidas denomina LOIC (del inglés *Low Orbit Ion Cannon*, que significa *Cañón de Iones de Órbita Baja*), e inclusive cuenta con una *interfaz gráfica de usuario*, lo que proporciona un entorno visual sencillo para su utilización. Esta herramienta no solo tiene particular importancia por su fácil instalación y uso, sino también porque fue utilizada, por ejemplo, por muchos usuarios en una operación de protesta masiva organizada por el grupo *hacktivista "Anonymous"*, contra los sitios web del FBI, el Departamento de Justicia de los Estados Unidos, la Oficina del Derecho de Autor de los Estados Unidos y la Asociación Cinematográfica de Estados Unidos, entre otros. Este ataque no sólo provocó que los sitios web de estas organizaciones estuvieran fuera de servicio durante

la tarde del 19 de enero de 2012, sino que también conformó lo que efectivamente se podría denominar una *botnet voluntaria* (Greenberg, 2012).

Los ataques DDoS han aumentado en magnitud a medida que más y más dispositivos se conectan a Internet a través del nuevo paradigma de *Internet of Things* (*Internet de las Cosas* en inglés, usualmente abreviado IoT). Los dispositivos IoT son computadoras muy pequeñas, alojadas en accesorios hogareños tales como lavarropas, luces, cámaras de vigilancia y vehículos, entre otros, con el objetivo de conectarlos a Internet para ser monitoreados o controlados de manera centralizada y remota. En términos de seguridad informática, el problema que introducen los dispositivos IoT, es que a menudo utilizan contraseñas predeterminadas y no tienen políticas de seguridad sólidas, lo que los hace vulnerables al compromiso y la explotación mediante ataques informáticos. La infección de dispositivos IoT puede pasar desapercibida para los usuarios, y un atacante puede fácilmente comprometer cientos de miles de estos dispositivos para realizar un ataque a gran escala sin el consentimiento de los propietarios del dispositivo (National Cybersecurity and Communications Integration Center, 2009).

De hecho, un *malware* llamado "*Mirai*" aprovechó estas mencionadas vulnerabilidades y creó una *botnet* masiva de millones de dispositivos de IoT. Esta *botnet* fue famosa en 2016 por un famoso ataque DDoS a una compañía estadounidense llamada *Dyn*, encargada de operar servidores DNS, que provocó que millones de usuarios en todo América del Norte tuvieran dificultades para acceder —o directamente imposibilidad de acceder— a servicios como *Amazon*, *BBC*, *CNN* y *Twitter*, e inclusive imposibilitó la utilización de servicios financieros como *PayPal* y *Visa* (Fruhlinger, 2018).

En relación estricta con los Estados, los ataques DDoS han sido noticia, tales como los ataques DDoS contra las páginas web del gobierno tailandés en 2015 (BBC, 2015), o contra los servidores del gobierno de Luxemburgo en 2017 (Millman, 2017). Los ataques DDoS con un Estado como objetivo atentan contra la capacidad de los ciudadanos de acceder a un servicio público, por lo cual —aunque usualmente pueden ser mitigados de manera rápida— pueden afectar la comunicación o el normal desarrollo de las actividades de un Estado en el ciberespacio.

Muchas veces, la intención de un ataque DDoS es también la de enviar un mensaje político: en 2012, fueron lanzadas de manera repentina una serie de ataques DDoS a la Bolsa de Nueva York y a múltiples entidades bancarias de Estados Unidos,

incluida la empresa *JP Morgan Chase*. Más tarde se descubrió que los perpetradores de este ataque habían sido un grupo que se llamó a sí mismo los "combatientes cibernéticos" de las Brigadas de Ezzeldin Al-Qassam, una organización islamista palestina (Perlroth y Hardy, 2013). Este ataque no solo impulsó la utilización de tipologías que se abordarán más adelante, como "*ciberterrorismo*", sino que se constituyó como uno de los ataques DDoS más prolongados de la historia: se denominó "Operación Ababil", y fue entendido por las agencias de inteligencia de los Estados Unidos como un mensaje político de grupos islamitas contra las sanciones comerciales impuestas en el 2012 a Irán por el gobierno de los Estados Unidos y la Unión Europea, frente a su negativa de detener su plan nuclear (Radware, 2018).

En la actualidad, los Estados Unidos están cotejando la posibilidad de retirarse del pacto nuclear que mantienen con Irán, ya que fue una de las promesas de campaña del presidente Donald Trump. Una de las variables que los especialistas señalan como consecuencias inmediatas plausibles de esta acción es el potencial aumento de ataques informáticos hacia los Estados Unidos (Global Risk Insights, 2018). Si bien la disciplina de la seguridad informática provee soluciones para mitigar los efectos de los ataques DDoS, muchas veces este tipo de ataque es muy difícil de detectar y de combatir, por lo que se abre una discusión sobre la posibilidad que tienen los Estados de resistir los ataques DDoS, ya que inclusive el gobierno de Estados Unidos, país creador de Internet y líder en tecnología a nivel global, está preocupado por la posibilidad de ser el objetivo en el corto plazo de este tipo de ataques (National Cybersecurity and Communications Integration Center, 2009).

d) Ataque de Intermediario (MitM)

El ataque de intermediario, conocido por sus siglas en inglés *MitM* (de *Man-in-the-Middle*, literalmente "*Hombre-en-el-Medio"* en español) es un tipo de ataque informático en el cual un *cracker* se posiciona entre dos partes que creen estar comunicándose directamente entre sí, teniendo la capacidad de espiar la comunicación, o inclusive alterar su contenido. Normalmente, las partes no son conscientes de que el atacante está presente en sus comunicaciones o transacciones (Piscitello, 2015).

Uno de los tipos de ataques de intermediario más utilizado por los *crackers* es el denominado *evil twin* (gemelo malvado en inglés): el atacante simula, con una computadora, ser un punto de acceso a una red inalámbrica, al cual un dispositivo *Wi-Fi* se conecta interpretando que es un punto de acceso legítimo. Una vez conectado, el

atacante puede interceptar los datos que los dispositivos conectados ingresan, tales como credenciales de acceso a una compañía o banco, información de tarjetas de crédito, o incluso redirigir a los usuarios a sitios web falsos que roben información personal o descarguen algún tipo de *malware* (Piscitello, 2015).

Sin recaer en ejemplos donde la información privada individual de cada usuario que es objeto de un ataque de intermediario puede resultar robada; es relevante hipotetizar cuál sería el daño que este tipo de ataques podría realizar si logra espiar o modifica, por ejemplo, conversaciones oficiales entre embajadas, mensajes oficiales, o intercepta información sensible o estratégica para un Estado.

Como si la posibilidad de que un *cracker* utilice estos ataques no fuera suficiente, muchas veces los fabricantes de diferentes computadoras o dispositivos hacen uso de estrategias muy similares para introducir funcionalidades en sus productos, pero que como efecto secundario genera una recopilación de los datos personales de los usuarios. En 2015, por ejemplo, *Comcast*, una de las empresas proveedoras de servicios de Internet más grandes de los Estados Unidos, realizaba, por definición, ataques de intermediario para advertir a los usuarios que podían estar descargando contenido con permisos de autor (Knight, 2015). Si bien las empresas siempre argumentan su utilización con medios comerciales y sin malas intenciones, es casi incomprobable la utilización que puedan hacer con este tipo de datos recolectados (Leyden, 2003; Meyer, 2013; Williams, 2015).

Las formas que adquieren los ataques de intermediario pueden ser muy variadas, e inclusive existen rumores y sospechas hacia la Agencia de Seguridad Nacional de los Estados Unidos, la cual es acusada de utilizar un ataque de intermediario para simular ser uno de los buscadores web más ampliamente utilizados en todo el mundo, *Google*, y lograr así una recolección masiva de inteligencia sobre sus ciudadanos (Moyer, 2013).

Las diferentes alternativas que tienen a su disposición los usuarios para mitigar un ataque MitM dan lugar a la introducción de una disciplina central para la seguridad informática: la *criptografía*. La Real Academia Española (2018) define a la criptografía como el “arte de escribir con clave secreta o de un modo enigmático”, y es entendido como una disciplina dentro de la criptología que se ocupa de elaborar técnicas de cifrado para alterar las representaciones lingüísticas de un mensaje, con el fin de hacerlo irreconocible a lectores no autorizados. Si bien las técnicas de la criptografía han sido utilizadas históricamente en campos que van desde el arte hasta la guerra, en la actualidad los sistemas informáticos hacen uso de técnicas criptográficas que sirven,

mediante la implementación de diversos *algoritmos*, para cifrar la información digital almacenada o transmitida por Internet.

Hoy en día, muchos programas informáticos hacen uso de protocolos criptográficos para cifrar la información intercambiada mediante Internet, dentro de los cuales uno de los más utilizados es el protocolo TLS/SSL (del inglés *Transport Layer Security/Secure Sockets Layer*, *Seguridad de la Capa de Transporte/Capa de Puertos Seguros* en español). Mediante un complejo sistema de *intercambio asimétrico de certificados únicos*, esta tecnología asegura al usuario que la información está siendo enviada desde o recibida de una fuente confiable, desestimando la posibilidad de un ataque de intermediario.

Si bien la utilización de estos protocolos criptográficos se encuentra generalizada para asegurar las comunicaciones a través de Internet, no es un método infalible. Barak, académico especialista en criptografía, argumenta que es cierto que los sistemas criptográficos adquieren una gran capacidad de complejización con el uso del poder computacional moderno, pero la utilización masiva y generalizada de estas técnicas criptográficas también aumenta de manera proporcional la información y los métodos que los *crackers* tienen a su disposición, para burlar o romper este tipo de códigos (Barak, 2018, p. 460).

Para ilustrar este hipotético caso, Barak remite al *Proyecto Venona*, un programa de contraespionaje que llevaron a cabo durante la Guerra Fría los Estados Unidos en conjunto con el Reino Unido, para descifrar los mensajes intercambiados por las principales agencias de inteligencia de la Unión Soviética. El autor explica que la causa principal por la cual se pudieron descifrar los mensajes en código fue que los soviéticos, por la molestia que implicaba fabricar tantas claves de cifrado para todos los comunicados, comenzaron a reutilizar las claves. Este descubrimiento en el patrón de utilización de claves secretas fue lo que permitió que el *Proyecto Venona* resultara en la exposición de cientos de agentes y espías rusos en los Estados Unidos y otros países occidentales (Barak, 2018, p. 468).

De la misma manera, se vuelve relevante concebir la posibilidad de que la generalización del uso de los protocolos de cifrado modernos, hoy en día implementados en la mayoría de los servicios que operan en Internet para evitar ataques MitM, pueda generar algún tipo de patrón que termine vulnerando el sistema. Si bien con esto no se intenta afirmar que no exista posibilidad de defenderse de ataques de intermediarios, sí sugiere que los sistemas no son infalibles, y la capacidad de defensa

que los usuarios tienen para asegurar la veracidad de sus comunicaciones por Internet se sintetiza en la capacidad de combinar los aspectos técnicos, con la capacitación y la precaución de los usuarios finales a la hora de utilizar los servicios (Piscitello, 2015).

e) Ransomware

Un *ransomware* (acrónimo del inglés "*ransom*", *rescate*, y "*ware*", acortamiento de "*software*", *programa informático*), es un tipo de ataque informático que amenaza a la víctima con revelar sus datos personales, o con bloquear su acceso de manera permanente, a no ser que se pague un rescate por la información afectada. Los *ransomware* más simples realizan un bloqueo reversible del dispositivo afectado; pero aquellos que son programados con mayor detalle, utilizan métodos de cifrado criptográfico para volver los archivos y la información contenida en una computadora inaccesibles, lo cual es virtualmente imposible de revertir, sólo siendo posible su descifrado mediante el pago del rescate (FBI, 2012). Si bien este tipo de funcionalidad califica técnicamente dentro de los parámetros de un *malware*, sus implicancias y su uso difundido hacen que se configure como un tipo de ataque informático de alto riesgo.

Si bien son ataques que representan un potencial peligro para cualquier tipo de sistema informático que almacene información sensible, desde la perspectiva de Defensa de un Estado, es especialmente importante la protección de dispositivos que integren la infraestructura crítica, ya que puede robar o cifrar información vital para el funcionamiento estructural de una sociedad. Uno de los ejemplos que mejor ilustra la prioridad de protección de las computadoras encargadas de sostener la infraestructura crítica aconteció en mayo de 2017, cuando se desataron a nivel global una serie de ataques *ransomware* bajo el nombre de *WannaCry*, que infectó más de 230.000 computadoras en más de 150 países. Este ataque, que estaba dirigido a computadoras con el sistema operativo *Microsoft Windows*, cifró los datos de cientos de usuarios y exigía pagos de rescate en la criptomoneda *Bitcoin*.

Los primeros reportes del ataque resonaron en múltiples empresas en todo el mundo, desde *LATAM* en Chile (Neira, 2017), hasta *Hitachi* y *Honda* en Japón (Reuters, 2017). Sin embargo, además del sector industrial privado, comenzaron a ser afectadas por este *ransomware* empresas ligadas a la infraestructura crítica: la empresa española de telecomunicaciones *Telefónica* se vio forzada a directamente apagar sus computadoras y desconectarlas de la red (Jané, 2017), la empresa petrolera brasileña

Petrobrás también se vio afectada (Cavalcante, 2017), así como estaciones de policía y las empresas petroleras en China (Lau, 2017).

Uno de los sectores estratégicos que se vio más perjudicado por el *ransomware* WannaCry fue el Servicio Nacional de Salud de Reino Unido (en inglés *National Health Service – NHS*), el cual reportó más de 70.000 dispositivos infectados, incluyendo computadoras, tomógrafos de resonancia magnética y heladeras de almacenamiento de sangre (Graham, 2017). El caso del sistema de salud del Reino Unido ilustra de manera absoluta la importancia de la protección de los sistemas informáticos encargados del mantenimiento de sistemas de infraestructura crítica, y el rol preponderante de la seguridad informática para garantizar el correcto funcionamiento de los servicios de los Estados que estén conectadas a Internet.

Este tipo de *malware* está en pleno ascenso en su uso desde 2012, y se configura como una efectiva extorsión del usuario para permitirle recuperar toda la información afectada. La importancia en la actualización de los sistemas operativos y sus funcionalidades de seguridad se vuelve especialmente relevante en los casos de *ransomwares*, ya que, en el caso de continuar encontrándose una computadora vulnerable, es capaz de seguir expandiéndose e infectando otras computadoras en la red. De hecho, en agosto de 2018, y una vez que se habían distribuido las actualizaciones de Windows, el mismo *ransomware WannaCry* forzó a la empresa de fundición de semiconductores más grande del mundo, *Taiwan Semiconductor Manufacturing Company* (TSMC), a cerrar temporalmente varias de sus fábricas de chips debido a la infección de más de 10.000 computadoras en las instalaciones más avanzadas de la empresa (Kumar, 2018).

f) Amenazas Persistentes Avanzadas (APT)

Así como se estableció que los *malwares,* o programas maliciosos, tienen la capacidad de implementar diversas técnicas para lograr sus cometidos, los ataques informáticos se han vuelto progresivamente más sofisticados, serios y extensivos. En la actualidad, en el zenit de esta escalada de complejización de los ataques informáticos se materializa en un tipo de ataques sigilosos y continuos, dirigidos a organizaciones o instituciones específicas, que se denominan “Amenazas Persistentes Avanzadas”, usualmente abreviado APT, por sus siglas en inglés de *Advanced Persistent Threat*.

Si bien las definiciones de una Amenaza Persistente Avanzada pueden variar, su nombre realiza una buena definición: son ataques que son considerados *amenazas* ya

que tienen la capacidad y la intención de causar daño a un sistema informático, al ser ejecutadas de manera deliberada por humanos contra un objetivo específico. A su vez, es *persistente* porque prioriza una tarea específica, y no cesa en su accionar hasta lograrlo, al contrario de los ataques más convencionales que buscan penetrar sistemas informáticos de manera más oportunista. Por último, son *avanzadas* porque sus operadores cuentan con un espectro completo de inteligencia y conocimiento del objetivo del ataque, y van adaptando sus técnicas y herramientas para conseguir su cometido.

De esta manera, podemos definir a una APT como un tipo de ataque informático dirigido, que combina el uso de diversos tipos de ataques informáticos convencionales (DoS, *phishing*, *malwares*), para burlar las defensas de un sistema informático específico, con el fin de extraer información del mismo, o disrumpir su normal funcionamiento. La cualidad que distingue a un APT es que, a diferencia de los ataques convencionales, los cuales cesan en su accionar una vez que cumplieron su función, ocurren durante largos períodos de tiempo de manera sigilosa, con el objetivo de afectar lo más posible un sistema informático (Symantec, 2011, p. 1).

Un gobierno de un Estado puede estar acostmbrado a ataques políticos, guarras comerciales, o financieros, sostenidos en el tiempo, realizados por diferentes adversarios. El *modus operandi* de las APT es muy similar, pero la novedad que introducen es que los medios que se utilizan para ejecutar estos ataques se han movido al terreno de las redes y las aplicaciones informáticas (Sullivan, 2011, p. 3).

Las cualidades y la complejidad previamente descritas hacen que sea virtualmente imposible que un *cracker* individual pueda llevar adelante una APT, ya que sería descomunal que un individuo cuente con los medios necesarios para realizarla, y lograr que se desarrolle de manera *avanzada* y *persistente*. De esta manera, las APT tienen la particularidad de sólo poder ser orquestadas por grandes grupos que tengan los medios y los recursos para realizarlas, y usualmente son gobiernos nacionales o grandes empresas las que reúnen las capacidades para llevar a cabo una APT.

Si bien no es un hecho menor que una empresa realice ataques contra otras empresas por razones de rivalidad comercial, lo cual se constituye en un acto de competencia desleal, para el alcance de este trabajo de investigación es mucho más relevante que sea un Estado nacional quien lleve a cabo una APT. Como sostienen Singer y Friedman (2014, p. 59), si un Estado implementa una APT con el objetivo de robar datos o alterar los archivos de otro Estado nacional, las APT pueden ser

desplazadas de la figura de espionaje o crimen, y pueden llegar convertirse directamente en un acto de sabotaje, o incluso de guerra.

La capacidad de penetrar en un sistema informático que tiene una APT realizada con recursos, y de manera eficiente, es muy alta. Debido a esto, lo que muchas veces es muy difícil, en primer lugar, descubrir cuándo un Estado u organización está siendo objeto de este tipo de ataque; y, en segundo lugar, una vez que se fue descubierta, es mucho más difícil de asegurarse de su erradicación total del sistema o red infectado. Por ejemplo, una empresa estadounidense que había sido objeto de una APT, contrató a una firma de seguridad altamente calificada por el Pentágono para limpiar su red infectada. A pesar de haber sido asistida por esta empresa de renombre, unos meses más tarde, un termostato y una impresora en su edificio fueron encontrados enviando mensajes a un servidor ubicado en China, de donde se sospechaba que había provenido la APT inicialmente (Singer y Friedman, 2014, p. 59).

El concepto de las APT, y ejemplos concretos serán abordados de manera específica en el tercer capítulo de este trabajo de investigación, donde se analizarán diversos casos de ataques que se sospecha tuvieron origen en las principales potencias del sistema internacional, y alteraron el equilibrio de poder a escala global. Una de ellas, que muestra la complejidad y la escala que puede adquirir una APT, fue *Stuxnet*, un ataque que se deduce originado de un trabajo conjunto entre los Estados Unidos e Israel, apuntado a las instalaciones nucleares de Irán. Para detener el avance en materia de investigación nuclear, este ataque estaba dirigido específicamente a los sistemas de control industrial utilizados por esas instalaciones para controlar las turbinas de refinamiento de uranio, y logró retrasar los avances iraníes al hacer rotar las turbinas fuera de secuencia, provocando inclusive la destrucción de los dispositivos.

El caso de Stuxnet muestra que los recursos necesarios para realizar una APT no radican simplemente en lograr penetrar un sistema o una red, sino que también requieren esfuerzos para saber qué hacer una vez que se ingresó: en el caso de Stuxnet, además de *crackers* se requirieron expertos nucleares e ingenieros que conocieran el funcionamiento de los dispositivos que se buscaban alterar, y la utilización de vulnerabilidades recientemente descubiertas (o de *día cero*) para perpetrar sistemas informáticos específicos (Singer y Friedman, 2014, p. 98).

En relación a las APT y al resto de los ataques informáticos simples, hay dos cuestiones que son centrales para su análisis integral: en primer lugar, es necesario interpretar la forma en que logran explotar con alta eficiencia las vulnerabilidades en la

seguridad de los sistemas informáticos para lograr su cometido; y en segundo lugar, la cuestión de cómo se establece una atribución, ya que en un ciberespacio repleto de actores estatales y no estatales, es muy difícil determinar con certeza la procedencia de los ataques informáticos.

3. Vulnerabilidades en los programas informáticos. Día Cero y *backdoors*.

Los ataques informáticos se aprovechan de *vulnerabilidades* en los sistemas y programas informáticos para poder llevar a cabo sus acciones. La compañía japonesa de seguridad informática *Micro Trend* (2017) descubrió un total de 382 nuevas vulnerabilidades, sólo en el primer semestre de 2017, un número preocupante de posibilidades para un *cracker* de vulnerar diversos sistemas informáticos. Una de las preguntas principales que surgen entonces es por qué existen en primer lugar esas vulnerabilidades, y por qué, con los avances tecnológicos, no se logra reducir su número.

Para abordar estas cuestiones, es necesario resumir la manera en que se desarrolla un programa informático. Para que una computadora pueda realizar una tarea, ésta debe ser redactada en un proceso denominado *programación.* El único lenguaje en el cual se le pueden enviar instrucciones a una computadora se denomina *código binario*, y es un sistema numérico compuesto por combinaciones de unos y ceros (ver ilustración 5). Si bien es técnicamente posible para una persona escribir un código binario, su complejidad e ininteligibilidad implicaría una tediosa tarea que llevaría mucho tiempo, por lo que un programador utiliza *lenguajes de programación* mucho más entendibles para las personas, creando lo que se denomina un *código fuente* (ver ilustración 6). Los códigos fuente son la esencia de un programa informático, ya que es lo que permite entender cómo éste funciona y cuáles son sus resultados al ejecutarlo, y son escritos en diversos lenguajes de programación que utilizan diferentes herramientas, con múltiples utilidades (por ejemplo, hay lenguajes de programación específicos para diseñar páginas web, para manejar bases de datos, o para para analizar estadísticas, entre otros).

Una vez que el código fuente de un programa informático se encuentra finalizado, y todas sus funcionalidades están probadas y cumplen con el comportamiento esperado, el o los programadores que lo diseñaron escribieron utilizan programas específicos para *compilar* (traducir) su código fuente a código binario, y permitir así que el programa sea ejecutado por una computadora.

Por más que un grupo de programadores trabaje activamente para perfeccionar un programa informático, al igual que toda creación humana puede contener errores de programación, conocidos como *bugs*, que pueden llegar a desencadenar algún tipo de resultado inesperado. Es en este momento, en el proceso de creación de un programa informático, en el cual se pueden producir el primer tipo de vulnerabilidades, denominadas *vulnerabilidades involuntarias*. Ya sea que se produzcan durante la creación inicial del código fuente, por la inclusión posterior de nuevas funcionalidades, o por eventuales cambios imprevistos, cuando un programador descubre un fallo en su código que puede generar vulnerabilidades de seguridad, procede a corregirlo y a distribuir esa corrección a las personas que utilizan ese programa, mediante actualizaciones.

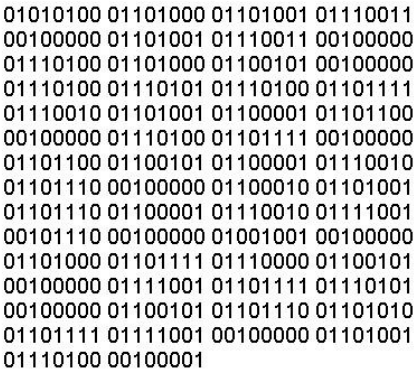

Ilustración 5: Ejemplo de código binario. Fuente: elaboración propia.

```
int main ()
{
        string name; //Nombre del estudiante
        cout<< "Ingrese su nombre";
        cin>>name;
        /*Ahora muestra Hola, y el nombre del estudiante*/
        cout<< "Hello " << name;
        return 0;
}
```

Ilustración 6: Ejemplo de un código fuente en el lenguaje de programación C++. Fuente: elaboración propia.

También existen otro tipo de vulnerabilidades, denominadas *deliberadas*, y que son incluidas intencionalmente en el código fuente de un programa por sus desarrolladores. Las vulnerabilidades deliberadas se alzan como las más peligrosas, y para explicarlas se deben introducir una serie de nuevos conceptos, los cuales serán funcionales para el análisis de los casos analizados más adelante, y que refieren a la forma en que se desarrollan los programas y sistemas informáticos, y las estrategias adoptadas para garantizar su seguridad.

En grandes rasgos, existen dos grandes formas de desarrollar programas informáticos. La primera forma se denomina *privativa*, y es aquella en la cual una empresa o individuo se vuelve dueño de ese programa, convirtiéndolo en un bien transable, y vende copias del mismo para obtener un rédito económico (en general mediante licencias pagas). Usualmente, los productores de programas privativos ocultan su código fuente, y utilizan diversas técnicas de protección de derechos de autor, para

garantizar que los usuarios no puedan observar el código que se ejecuta en sus computadoras, volviendo casi imposible alterar o reproducir el código fuente.

La segunda forma de producir programas informáticos se denomina de *código abierto*, y como su nombre lo indica, es la distribución de los programas informáticos sin ningún tipo de licencia restrictiva de acceso a su código fuente. Es aquí donde se erige el primer argumento respecto a las vulnerabilidades deliberadas en los programas informáticos: si un programa mantiene oculto su código fuente, no es posible corroborar que realice acciones no deseadas, o contenga funciones adicionales, que se puedan convertir en vulnerabilidades.

Estas dos maneras de crear programas informáticos dan lugar a un debate dentro de la disciplina de la seguridad informática, que —aunque es una dicotomía que proviene de la criptografía, y no solo se aplica a la informática— refiere a la forma en que se garantiza la seguridad de un programa o sistema informático. La primera postura se denomina *paradigma de seguridad por oscuridad*, y sostiene que el método para proporcionar seguridad debe residir en el secreto de su diseño (en el caso de un programa informático, ocultando su código fuente) o de su implementación (Miessler, 2009). Este paradigma ha sido rechazado por muchos expertos en seguridad, e inclusive dio lugar al surgimiento de un reconocido principio en criptografía, denominado *Principio de Kerckhoffs*, el cual sostiene que la seguridad de un sistema nunca debe depender de que su diseño permanezca en secreto, sugiriendo a los implementadores de sistemas de cifrado que hay que logar garantizar la seguridad, inclusive si todos los parámetros de su sistema criptográfico son de público conocimiento.

Las críticas al paradigma de seguridad por ocultamiento dan lugar a la segunda postura, denominada *paradigma de seguridad por exposición*, conocido en inglés como *Open Security*. Este paradigma sostiene que al hacer público el código fuente de los programas, los problemas de seguridad y las vulnerabilidades se pueden prevenir o mejorar ya que un número mayor de programadores pueden ver y modificar el diseño del programa, mejorando la seguridad mediante la colaboración, y otorgando a los sistemas una mayor auditabilidad (Wheeler, 2013).

En relación a este debate, la *Fundación por el Software Libre* es una organización que realiza un abordaje técnico y filosófico sobre la relación entre los usuarios y los programas informáticos, y argumentan que los programas informáticos *deben* ser *libres*. Esta libertad, heredada de la cualidad libre de los primeros programas informáticos y la cultura *hacker* previamente abordada, no concibe a los programas

como bienes sino como servicios, e implica la posibilidad del usuario de utilizar el programa como lo desee, estudiar su funcionamiento sin restricciones, poder adaptarlo a sus necesidades, y poder mejorarlo, copiarlo y distribuirlo sin ningún tipo de límite. Para lograr este cometido, la Fundación por el Software Libre argumenta que una cualidad *sine qua non* de los programas informáticos es que su código fuente esté disponible sin licencias restrictivas. Su argumento principal es que los programas privativos, al ocultar su código fuente, tienen la posibilidad de incluir funciones que no son deseadas por los usuarios, tales como funcionalidades de espionaje, modificación de datos, y creación de vulnerabilidades de seguridad, y que hacen que los programas privativos se puedan convertir efectivamente en *malwares* (Sistema Operativo GNU, 2018b).

El argumento técnico para ponderar la apertura del código fuente frente a su ocultamiento, que se enmarca en el debate de paradigmas de seguridad por oscuridad y seguridad por exposición, es que, al estar disponible, la cantidad de ojos críticos que se encuentran examinando la estructura del código hacen que pueda ser evaluado, mejorado y mantenido por un gran número de programadores, resultando en programas y aplicaciones mucho más robustas y seguras (Sridhar et al., 2005, p. 944). De este modo, el planteo de la Fundación de Software Libre sobre la maliciosidad que pueden contener los programas informáticos privativos se vuelve auténtico, específicamente si se considera que, como se argumenta con casos específicos, los desarrolladores pueden inclusive ocultar *backdoors* en su código cerrado.

Un *backdoor*, o *puerta trasera*, es un método de sobrepasar los procedimientos convencionales de autenticación o cifrado de un sistema informático, para proveer a su creador de acceso remoto al dispositivo en el cual el programa informático afectado fue instalado. Este método puede encontrarse en sistemas operativos o diversos programas, y estar configurados de manera intencional o no, pero se constituyen como una clara vulnerabilidad del sistema en el cual el programa esté instalado. En el caso de que un *backdoor* se encuentre encapsulado en un código fuente cerrado por licencias, es muy difícil de descubrir y sólo el programador que lo desarrolló puede crear una actualización para solucionarlo. El problema es que hasta que eso ocurra, ese *backdoor* se vuelve una vulnerabilidad aprovechable por un *cracker* para llevar a cabo un ataque informático.

Esta dinámica da lugar a un tipo de vulnerabilidad que se denomina de "*día cero*", la cual es considerada una de las más peligrosas en informática. Este tipo de

vulnerabilidad es muy codiciada por su imprevisibilidad, y su nombre proviene de la noción de que el ataque que la utiliza tiene lugar en el *día cero* desde su descubrimiento: los interesados en mitigarla recién descubren la vulnerabilidad recién cuando están siendo víctimas de un ataque que la explota. De este modo, un *cracker* puede hacer uso de una vulnerabilidad de *día cero* para realizar un ataque informático de manera sorpresiva e inédita, antes de que una actualización para arreglarlo pueda ser implementada (Singer y Friedman, 2014, p. 42). El gran problema con las vulnerabilidades de día cero es que no solo pueden provocar un daño grave, sino que usualmente se concentran en programas o sistemas operativos privativos ampliamente utilizados, y esta cualidad estratégica hace que también exista en la *dark web* un sistema de ventas y subastas de vulnerabilidades *días cero*, las cuales pueden ser compradas y utilizadas por el mayor postor.

Como se puede apreciar con estas conceptualizaciones, son múltiples las razones por las cuales un sistema informático puede poseer vulnerabilidades que son pasibles de ser aprovechadas por un atacante. Todas las herramientas ofensivas en el ciberespacio que hagan uso de estas vulnerabilidades, se alzan como potenciales peligros, tanto para actores individuales como para los Estados. De esta manera, es necesario definir cómo afectan las vulnerabilidades informáticas específicamente a los Estados, y cuáles son las estrategias que éstos pueden adoptar para incrementar su seguridad y defensa informática. Antes de proceder a esto, es necesario introducir una última variable de análisis, que es fundamental ya que condiciona el análisis de los ataques informáticos: la determinación de la procedencia de los ataques en el ciberespacio.

4. El problema de la atribución en el ciberespacio

Luego de haber introducido las principales herramientas informáticas que pueden ser utilizadas para disrumpir el normal funcionamiento, o corromper un sistema informático, es interesante cotejar los motivos por los cuales no existe una correlación entre el acelerado desarrollo de estas herramientas de penetración de sistemas, con la capacidad que las entidades u organismos tienen para responder y defenderse de estos ataques.

Si bien esto es una cuestión que refiere, en parte, a la capacidad constante de re-adaptarse de los *crackers*, los cuales están constantemente elaborando nuevas estrategias para abordar sistemas informáticos nuevos y cambiantes, también tiene que ver con variables estructurales de Internet y el ciberespacio, las cuales condicionan las

estrategias defensivas que una entidad puede tomar para defenderse de un ataque informático. Las razones estructurales más enraizadas en la estructura de Internet refieren a la *identidad* y la *atribución* en el ciberespacio.

a) La identidad en el ciberespacio

La identidad refiere a la capacidad de identificar físicamente a la persona que está realizando acciones en el ciberespacio, independientemente de que sean delitos o no. El primer impedimento que existe respecto a la identidad en línea es que, como sostiene Kabay (1998), el anonimato en el ciberespacio es una cualidad intrínseca de la estructura de Internet, la cual está orientada a proteger el derecho a la privacidad de las personas. Sin embargo, la contracara del anonimato en línea implica el uso generalizado de fraudes, evasión impositiva, extorsión, chantaje, entre otros (Kabay, 1998).

En 1993, la revista estadounidense *The New Yorker* publicó una ilustración de Peter Steiner en la cual se mofa de esta característica de Internet: son dos perros sentados cerca de una computadora, y uno le dice a otro “en Internet, nadie sabe que eres un perro”. Frente a este anonimato generalizado que plantea Internet, es interesante suponer qué capacidad tiene, por ejemplo, un Estado nacional, para identificar a un atacante, o un perpetrador de un delito informático, que afecte sus intereses estratégicos. Post y Johnson (1997, citado en Kabay, 1998) argumentan, desde una visión más globalista, que los Estados nacionales geográficamente definidos no pueden lidiar razonablemente con un medio de comunicación virtual sin fronteras como lo es Internet. Sin embargo, en la práctica, las estructuras geográficas se combinan con el ejercicio del poder, para brindar a los Estados cierto nivel de control sobre las conexiones de sus ciudadanos, y poder enmarcarlos en sus reglamentaciones tradicionales (Kabay, 1998).

A pesar de la potestad legal, el impedimento que puede tener un Estado para obtener la identidad de un atacante informático en Internet se reduce en gran medida a cuestiones técnicas. En primer lugar, la definición de la identidad en línea está estrechamente ligada un proceso de autenticación. Identidad y autenticación son nociones similares, pero que no significan lo mismo, por lo cual es necesario establecer la distinción. La autenticación se refiere exclusivamente a la *prueba de identificación* que un usuario realiza frente a un sistema informático, usualmente definida como “algo que alguien sabe, algo que alguien tiene, o algo que alguien es o representa” (Singer y Friedman, 2014, p. 31-33).

“Algo que alguien sabe” simboliza uno de los métodos de autenticación más utilizados en los sistemas informáticos, es decir el de una *contraseña* o clave de seguridad (un secreto idealmente sólo conocido por la persona adecuada). Por otro lado, “algo que alguien tiene” refiere a un componente físico al cual solo la persona adecuada tiene acceso, como por ejemplo una tarjeta para un cajero de banco, una llave magnética para desbloquear una cerradura electrónica, entre otras. En último lugar, “algo que alguien es, o representa” refiere a técnicas de autenticación biométricas, como una huella dactilar (The Economist, 2017).

Para un sistema informático, un proceso de autenticación exitoso implica la prueba de identificación. Usualmente, la prueba de identificación en un programa informático trae aparejado la consecuente autoridad para hacer uso del sistema o de un servicio que éste provee, o inclusive obtener permisos para modificar su funcionamiento. El problema con los procesos de autenticación desde la perspectiva de la seguridad informática, es que existen debilidades referidas a las pruebas necesarias para validar estos procesos de autenticación. El caso que mejor ilustra estas debilidades es que el proceso de autenticación más utilizado, las contraseñas o claves de seguridad, tienen que ser recordadas por el usuario, por lo cual contienen un límite cognitivo que se configura como una debilidad de partida: las claves no pueden ser ni aleatorias, ni extremadamente largas. En palabras sencillas, las contraseñas pueden ser robadas o adivinadas (sea por humanos o por programas informáticos específicamente diseñados para adivinar contraseñas), y también las “cosas que alguien tiene” para acceder a un sistema informático pueden ser robadas o falsificadas.

Cualquier persona puede acceder a la cuenta bancaria de otra persona con su tarjeta magnética y su código de seguridad, así como cualquier persona puede hacer uso de las redes sociales de otra persona, conociendo las contraseñas para autenticarse. Inclusive son conocidos los casos en los que usuarios se han podido autenticar en lectores de huellas dactilares, con una réplica de un dedo autorizado hecha en golosinas de gelatina (Leyden, 2002). Para un sistema informático, la autenticación es la prueba suficiente de la veracidad de la identidad del usuario, pero por las debilidades mencionadas anteriormente, esto puede no ser cierto en la totalidad de los casos. Uno de los acercamientos que se han tomado desde la seguridad informática para mitigar estas vulnerabilidades en los procesos de autenticación ha sido la de la *autenticación de múltiples factores*, es decir la autenticación exitosa una vez que el usuario presenta dos

o más pruebas de identidad. Sin embargo, a pesar de ser mejores, estas estrategias han probado no ser infalibles (The Economist, 2017).

Que el proceso de autenticación no garantice la identidad en línea de los usuarios no es un hecho menor, ya que, desde la perspectiva de un Estado, no se puede saber con certeza si la persona detrás de un usuario es realmente quien dice ser. Esto puede dar lugar a situaciones simples, como perfiles falsos en las redes sociales, pero también a cuestiones más complejas, como atacantes sofisticados que se camuflan, al identificarse con la identidad de ciudadanos aleatorios. De esta manera, la combinación de variables técnicas, y de variables intrínsecas de Internet, hacen que la identidad en línea sea muy difícil de comprobar, y complejiza cualquier tipo de identificación que un Estado o entidad pueda hacer sobre un usuario que realice ataques informáticos.

b) La atribución en el ciberespacio

Como sostiene Schneier (2015), cuando un Estado es atacado por un misil, es muy simple seguir su trayectoria para encontrar desde dónde fue lanzado. El problema es que cuando un Estado es atacado mediante un ataque informático proveniente del ciberespacio, no sólo es difícil descubrir de dónde provino, sino que es aún más difícil atribuir con certeza quién lo hizo, y más difícil todavía determinar si fue perpetrado por el gobierno de otro Estado. Esta realidad de la agresión internacional es, para el autor, un factor que obliga a cambiar la forma en que se abordan las temáticas de Defensa en la actualidad.

Dentro de todos los datos que una computadora comparte al conectarse a Internet, uno de los más utilizados para conocer la procedencia de las conexiones es la dirección IP, un identificador único de los dispositivos que se conectan a Internet. Sin embargo, como sostienen Singer y Friedman (2014, p. 33), no es sensato confiar exclusivamente en la dirección IP para asegurar la procedencia de un ataque, y mucho menos para determinar la identidad del atacante: sería igual que confiar en las patentes de los autos para identificar a los conductores.

Como si este nivel de complejidad no fuese suficiente, también existen métodos que muchos atacantes pueden utilizar para enmascarar su verdadera dirección IP. Para continuar con la analogía del conductor del automóvil, esto significa que el mismo puede ser prestado, alquilado o robado. Inclusive, un ataque informático puede provenir de un dispositivo que sea parte de una *botnet*, donde siquiera el usuario y dueño

legítimo del dispositivo es consciente que, usualmente en segundo plano, su computadora está realizando un ataque informático comandado remotamente.

Estas variables añaden un nivel de complejidad cada vez mayor a la hora de determinar la procedencia y la identidad de los ataques informáticos, haciendo que la atribución de los ataques en el ciberespacio sea una tarea extremadamente difícil. Muchas veces los paquetes enviados por un atacante no arriban con direcciones de devolución, pero en el caso de ser así, es muy difícil distinguir entre *crackers* individuales, y ataques llevados a cabo por un Estado nacional, ya que ambos pueden usar las mismas herramientas informáticas para realizar los ataques (Schneier, 2015).

Usualmente, los programas de seguridad informática suelen prestar especial atención a determinados indicadores de compromiso (IOC, de sus siglas en inglés de Ind*icator Of Compromise*). Los IOC son indicadores que señalan, en general con alta confianza, una intrusión en un sistema o red, y también pueden ayudar a determinar la procedencia de los mismos, haciendo uso de diferentes elementos técnicos, como las ya mencionadas direcciones de IP, firmas digitales, páginas web, nombres de dominio, entre otros elementos. Sin embargo, como sostiene Maloney (2017), los ataques han evolucionado de tal manera, que inclusive hacen un uso adverso de los IOC estandarizados en los protocolos de seguridad informática, para burlar las capacidades de detección, y hacer el proceso de atribución más difícil. Esto llega al uso de lo que la autora denomina “banderas falsas”, lo cual se traduce en una situación insólita en el sistema internacional: un atacante impostor dirige un ataque informático hacia un Estado víctima, y disfraza los ataques con IOC pertenecientes a un tercer Estado, lo que usualmente lleva a aumentar las tensiones entre el Estado víctima y el presunto Estado atacante (Maloney, 2017).

El caso más emblemático para ilustrar la complejidad de la atribución en el ciberespacio es el de las *botnets*. Como se describió previamente, muchas formas de *malware* toman el control de las computadoras de sus víctimas y las vinculan a una gran red de computadoras que luego puede ser operada de manera remota y masiva por un atacante. En 2010, por ejemplo, tres españoles crearon una *botnet* de escala global que incluía más de 12 millones de computadoras, solamente usando un programa que adquirieron en la *dark web* (Larraz, 2010).

Como sostienen Singer y Friedman (2014, p. 73-74) son tres las características claves que hacen importantes a las *botnets* en este contexto. En primer lugar, no cuentan con límites geográficos: alguien en Holanda puede comprometer computadoras en Chile

para lanzar ataques informáticos contra sistemas informáticos localizados en España. En segundo lugar, el propietario de una computadora que es parte de una *botnet*, usualmente no tiene noción de que está siendo utilizada por un actor remoto para realizar un ataque informático. Y tercero, cuando se realiza un ataque, un análisis sofisticado puede, a lo sumo, identificar la computadora que se utiliza para lanzar el ataque, pero es muy difícil lograr determinar si esa computadora está a su vez siendo operada remotamente, por lo que es virtualmente imposible determinar quién es el usuario detrás del ataque.

Más allá de las cuestiones exclusivamente técnicas, no es muy difícil imaginar las potenciales implicancias que tienen para las relaciones internacionales estas falencias para establecer la atribución de los ataques informáticos. Un caso emblemático, que sigue aún vigente en el momento de redacción de este trabajo de investigación, es el de la supuesta intromisión rusa en las elecciones presidenciales en los Estados Unidos en 2016.

Como se abordó previamente, luego de la conclusión de las elecciones comenzaron a circular informes públicos que apuntaban a agentes rusos por utilizar técnicas de *phishing* para comprometer los sistemas de información del Comité Nacional Demócrata, filtrando sus informes internos y correos electrónicos al público. Inclusive el Departamento de Seguridad Nacional y el Director de Inteligencia Nacional anunciaron el 7 de octubre de 2016 que la comunidad de inteligencia de los Estados Unidos estaba “segura de que el gobierno ruso dirigió los compromisos recientes" (DHS Press Office, 2016, traducción propia).

Aunque diecisiete agencias estadounidenses estaban de acuerdo en que Rusia era responsable de piratear la campaña de DNC y Clinton, el entonces presidente electo Trump siguió negando el hecho de la interferencia rusa, y solo reconoció esa posibilidad por primera vez el 11 de enero de 2017 (Nakamura y Phillip, 2017). Si bien la Oficina del Director de Inteligencia Nacional de los Estados Unidos publicó un informe detallado en el que concluye que Rusia fue responsable del *crack* de DNC, el informe de veinticinco páginas dice poco sobre la evidencia que las agencias tienen para sostener la participación del Estado ruso en los ataques (Universidad de Yale, 2017).

Este ejemplo demuestra de manera fehaciente que el problema de la atribución puede generar tensiones diplomáticas entre Estados, y también deja claro que establecer la atribución no es lo mismo que establecer complicidad. Por más que sea posible rastrear los esfuerzos de un actor a un determinado lugar geográfico, es mucho más

complejo establecer un papel formal del gobierno de ese lugar como autor o sancionador de la operación (Singer y Friedman, p. 76).

Estas variables hacen que, como sostienen Singer y Friedman (2014, p. 76), en seguridad informática la atribución se vuelva un verdadero dilema. A la hora de señalar a un grupo o persona como el responsable o cómplice de determinado ataque informático, es necesario sopesar las ganancias y las pérdidas potenciales de realizarlo sin pruebas contundentes, y aún mucho más si el acusado es un Estado nacional. Así, como se ve en el caso de la supuesta interferencia rusa en las elecciones presidenciales estadounidenses de 2016, la atribución en el ciberespacio se vuelve muchas veces una cuestión política, en la cual los objetivos del mundo material importan más que el suceso que aconteció en el ámbito cibernético, y pasa a ser jurisprudencia de las relaciones internacionales.

IV. Conclusiones parciales

Internet, la gran red de redes de escala global a la cual un creciente número de dispositivos se conectan, inicialmente concebida como una plataforma de comunicaciones, cada vez tiene más funcionalidades. Estas funcionalidades combinadas dan lugar a un nuevo espacio virtual, en el cual múltiples actores interactúan, denominado ciberespacio. El ciberespacio es un terreno de acción muy novedoso, pero que en su configuración puede ser idealizado como un espejo del sistema internacional, gracias a un elemento en común que define a ambos: la anarquía.

La multiplicidad de actores con la que cuentan, tanto el sistema internacional como el ciberespacio, no da lugar a la existencia de un gobierno centralizado, y las capacidades de acción de los actores individuales son las que moldean las interacciones. Los Estados se distinguen en ambos, como aquellos actores con mayores recursos y capacidades para influenciar al resto. Sin embargo, como se observó, el ciberespacio reserva algunas particularidades que complejizan aún más el análisis de las relaciones virtuales entre Estados.

Que el ciberespacio pueda ser considerado un espejo del sistema internacional en términos conceptuales, no implica que se configure como un espacio completamente análogo. Si bien se podría afirmar que traslada de manera casi inalterada las relaciones de poder y las capacidades de acción de los actores que componen al sistema internacional, el ciberespacio presenta características muy distintivas: se constituye en la herramienta principal de comunicación entre Estados, pero también en el lugar en el

que se almacenan más de dos millones de videos de gatos sólo en *YouTube*, una de las plataformas de video más extendidas (Dahl, 2015).

Desde la perspectiva de las relaciones internacionales, el ciberespacio se configura como un escenario complejo, que, al trasladar las pujas y los equilibrios de poder ya existentes en el sistema internacional, puede ser considerado como una extensión de éste. Las capacidades ofensivas y defensivas en el ciberespacio siguen concentrándose en los poderes centrales del sistema internacional, pero adquieren formas cambiantes y variables, con alcances aún más impredecibles.

Factores como la dificultad para confirmar la identidad de los usuarios en línea, y las diferentes estrategias que existen para ocultar o camuflar la procedencia de los ataques en el ciberespacio hacen que cuestiones clave, como la atribución de un ataque, sean muy difíciles de definir en el ciberespacio. Naturalmente, estas situaciones crean nuevas capacidades ofensivas y defensivas, y cuestiones esenciales en las relaciones internacionales, como la guerra, empiezan a reconceptualizarse al verse atravesadas por la virtualidad.

Habiendo precisado conceptualmente las estrategias ofensivas en el ciberespacio, y las particularidades que éstas adquieren, se procederá a analizar su influencia específica en los Estados y en las relaciones intergubernamentales. Con ataques informáticos cada vez más variados, que adquieren diversas morfologías, cobra relevancia estratégica la seguridad informática, es decir la forma en que se hace frente a las ofensivas en el ciberespacio. Es menester, de esta manera, analizar si el ciberespacio se puede convertir, además de un terreno de acción, en un campo de batalla, y en el caso de así serlo, definir cuáles son las estrategias que los Estados pueden adoptar en su posicionamiento en el ciberespacio.

Capítulo II. La Seguridad Informática en las Relaciones Internacionales

I. Introducción

En 2013, Edward Snowden, un contratista informático de bajo nivel, se encargaba de administrar sistemas informáticos en la Agencia de Seguridad Nacional de los Estados Unidos. Por negligencias en los controles de acceso, tuvo a su disposición una gran cantidad de programas informáticos, altamente secretos y controversiales, que posteriormente filtró a la prensa (Singer y Friedman, 2014, p. 50). Si bien fueron masivas y abarcaron diferentes áreas, estas filtraciones se concentran en el rol de los Estados Unidos en el espionaje digital, en el cual es la Agencia Nacional de Seguridad estadounidense el organismo principal que ejecutaba acciones de espionaje. Esta agencia pertenece al Departamento de Defensa, y es responsable de monitorear, recopilar y procesar información con propósitos de inteligencia y contraespionaje extranjero. En relación a este tipo de instituciones, Petallides (2012b) asevera que:

> "desde el nacimiento de la civilización, los líderes y sus gobiernos han tratado de proteger sus secretos, mientras aprenden todo lo que pueden sobre los secretos de sus enemigos. El espionaje, la interceptación de mensajes, y la inteligencia han sido tradiciones para obtener una ventaja sobre un oponente durante milenios".

Las filtraciones de Snowden reafirman lo sugerido por el autor, y muestran las diferentes morfologías que estas estrategias adoptan en el ciberespacio: se dieron a conocer una gran variedad de programas informáticos con la capacidad espiar diversos tipos de actividades, haciendo uso de vulnerabilidades en muchos sistemas informáticos. En un principio, la abrumadora cantidad filtraciones apuntaron específicamente a estrategias de espionaje dentro de los Estados Unidos. Se revelaron programas informáticos con la capacidad de intervenir comunicaciones de correos electrónicos, llamadas y mensajes de texto (tanto de teléfonos celulares como de líneas telefónicas), e inclusive algunos de los programas tenían la capacidad de interceptar comunicaciones satelitales en todo el mundo.

Las capacidades de los programas informáticos desarrollados por la Agencia de Seguridad Nacional estadounidense sirven como punto de partida para evidenciar de qué manera el ciberespacio reconfigura y potencia las estrategias que un Estado, con las intenciones y capacidades suficientes, puede adoptar para perseguir sus objetivos. Es fundamental resaltar que la capacidad de montar una estructura que permita generar este tipo de programas informáticos de espionaje, requiere no solo de un gran conocimiento técnico, sino de un gran presupuesto que posibilite un trabajo constante para la generación de nuevos desarrollos. Esto explica por qué son los Estados Unidos, el país con mayor presupuesto de Defensa en el mundo, el país que cuenta con las posibilidades de implementar este tipo de estrategias de espionaje a escala global.

Hasta el momento, se evidenció la multiplicidad de variables que Internet y el ciberespacio introducen, configurando un escenario complejo para las relaciones entre los actores del sistema internacional, sean privados o estatales. El objetivo de este capítulo es restringir el foco de estudio, realizando un análisis más específico sobre las potenciales consecuencias e implicancias que el ciberespacio puede tener en los Estados, de qué manera modifica las relaciones internacionales, y qué estrategias de seguridad informática existen para hacer frente a las hostilidades virtuales.

II. Enfrentamientos en el ciberespacio

Previamente se describió a un programa informático como una serie estricta y ordenada de instrucciones que se le da al procesador de una computadora, para que realice determinada acción. Siguiendo con esta línea, se definió como *malware* a todo tipo de programa informático diseñado específicamente para causar daños a una computadora, un servidor, o una red informática. El hecho de que una computadora logre ejecutar una serie de órdenes que tenga la capacidad de dañar otra computadora y la información que ésta contenga, da lugar a un gran debate dentro de las ciencias exactas referido a la neutralidad de la tecnología.

Existen dos escuelas principales de pensamiento que abordan esta temática (Nolan, 1999). La primera sostiene que la tecnología posee una cualidad intrínsecamente pasiva, y que esto hace que la tecnología *per se* no sea le foco del análisis sobre su neutralidad, sino la utilización que los actores hacen de ella, en los diferentes sistemas sociales y económicos en los que está inserta (MacKenzie y Wajcman, 1999). La segunda cosmovisión niega las cualidades pasivas en las tecnologías, y sostiene que toda tecnología es diseñada con un fin. Además, afirma que

algunas tecnologías contienen ciertas propiedades que no permiten la neutralidad, condicionando el uso final que su usuario le puede dar (Chandler, 1995).

Si bien este dilema está ligado a interpretaciones y concepciones subjetivas, la evolución de los avances tecnológicos hasta la actualidad, hace que se obtengan diferentes conclusiones al analizar distintos tipos de tecnologías, pero el recrudecimiento más intenso de estas discusiones tiene lugar cuando los nuevos desarrollos adquieren carácter ofensivo. Se podría argüir que, por ejemplo, una pistola es inherentemente pasiva, porque requiere intervención humana para apretar el gatillo, pero esto no implica que sea neutral, ya que fue diseñada para disparar una bala. La misma conclusión se podría extraer, por ejemplo, si se discute la neutralidad de la energía nuclear, o de los organismos genéticamente modificados (Nolan, 1999).

Sin embargo, cuando el foco se pone sobre una computadora, que se constituye como una tecnología diseñada para ejecutar órdenes redactadas en un programa informático, la neutralidad de este tipo de herramienta se vuelve mucho más difícil de determinar. Un caso representativo sobre esta complejidad lo puede demostrar uno de los principales lenguajes de programación utilizados para escribir las órdenes de un programa informático, denominado "*C*". Las cualidades de este lenguaje hacen que sea considerado uno de los lenguajes de programación más simples, portables y eficientes para desarrollar programas informáticos (Sistema Operativo GNU, 2018c). Así, la flexibilidad de esta herramienta hace que en *C* se pueda desarrollar un programa que controle un monitor de ritmo cardíaco. Sin embargo, también en *C* se escribió el ransomware *WannaCry*, que volvió inutilizable en 2017 a la mayor parte del Servicio Nacional de Salud del Reino Unido.

De este modo, se puede plantear como punto de partida algo que ha estado implícito a lo largo de este trabajo de investigación, y es que, si bien las computadoras se constituyen como tecnologías neutrales, el empleo que un usuario hace de ellas, no lo es. De este modo, lo que no es neutral son las instrucciones que se le dan a una computadora, es decir los programas informáticos, y que son siempre producto de la intención humana. Esta cualidad hace que un programa informático pueda tener usos positivos y negativos, lo cual va a estar siempre determinado por la perspectiva subjetiva que se le imprima a la interpretación de las funciones que cumpla un programa.

Independientemente de la cualidad subjetiva que determina si, por ejemplo, un programa informático es "bueno" o es "malo", la capacidad que han adquirido las

computadoras para procesar de manera simultánea una gran cantidad de órdenes, se traduce en que puedan ser desarrollados programas cada vez más complejos. De esta manera, un *malware* puede adquirir un nivel sin precedentes de capacidades de acción, que hace que, por ejemplo, como sucedió en diciembre de 2017, un solo ataque informático pueda generar un corte en el suministro de la energía eléctrica en toda la capital de Ucrania durante una hora (Greenberg, 2017). Así, los programas informáticos adquieren capacidades de acción cada vez mayores, y tienen la potencialidad de ser convertidos, por diferentes intereses, en verdaderas *armas informáticas*, cuyas implicancias están aún por ser descubiertas.

Las posibilidades que presentan este empleo ofensivo de las herramientas informáticas en el ciberespacio, ameritan nuevas definiciones de conceptos clásicos para las relaciones internacionales, pero también requiere un análisis objetivo sobre las verdaderas capacidades de acción que pueden tener, y su alcance en el mundo material. Esta situación ha engendrado conceptos como “ciberguerra”, “ciberterrorismo” y “armas cibernéticas”, y es crucial para este análisis detenerse en ellos, y entender sus implicancias para el sistema internacional.

1. ¿Ciberterrorismo?

Como toda construcción conceptual que comience con el prefijo “ciber”, es menester definir el concepto que sucede al prefijo, antes de analizar las cualidades que el ciberespacio le pueda otorgar. Por ende, antes de cotejar la posibilidad del terrorismo en el ciberespacio, es prioritario definir qué es el terrorismo. En relación a esto, Flabián Nievas, sociólogo y doctor en Ciencias Sociales, afirma que el icónico ataque a las torres gemelas del World Trade Center de septiembre de 2001 dio lugar a que el “terrorismo” pase a ocupar un lugar predominante en las agendas de seguridad de gran parte de las naciones del mundo, pero sostiene que, a pesar de esta importancia empírica, no existen definiciones formales que expliquen qué es el *terrorismo*. El autor afirma que esta ausencia de una definición común hace que el terrorismo se vuelva un adjetivo calificativo de diversos tipos de actos, y que “terroristas” sean aquellas acciones nominados como tales (Nievas, 2015, p. 174-175).

Nievas sugiere que la carencia de definición no es por inexistencia de vocación entre los académicos, sino que responde a intereses políticos, lo que da lugar a un gran debate sobre la temática. Y es esta cualidad política del concepto lo que crea dificultades técnicas a la hora de definir al terrorismo, dentro de las cuales el autor

considera como principal que su utilización como concepto aparece indisociablemente ligado a la moral: los actos terroristas son morales para quienes los ejecutan, e inmorales para quienes los padecen (Nievas, 2015, p. 175-176).

Saint Pierre (2003, p. 53) convalida esta postura, y mantiene una posición muy similar al afirmar que el *terror* tiene una cualidad intrínsecamente subjetiva, entendiéndola como una de las causas que generan dificultades a la hora crear definiciones, y resalta cómo el fenómeno del terrorismo se convirtió en el "criterio para distinguir amigos de enemigos, y el orientador principal de las decisiones en materia de seguridad internacional" (Saint Pierre, 2003, p. 43). La propiedad subjetiva del terror, y la cualidad nominal del terrorismo, provocan que la morfología que puede adquirir un perpetrador de actos terroristas sea múltiple. Saint Pierre señala, en relación a esto, que:

> "Las tácticas terroristas son frecuentemente usadas por grupos del crimen organizado, por traficantes, por gobiernos y en muchos casos por ejércitos regulares, inclusive en Colombia, por ejemplo, pero esos actos terroristas por sí solos no tornan terroristas a aquellos que los realizan, así como no torna terrorista a George Bush su frase claramente terrorista "quien no está del lado de los EE.UU. estará en contra y será aniquilado" (Saint Pierre, 2003, p. 52).

Esta insistencia sobre la inexistencia de definiciones sobre el terrorismo no es aleatoria, sino que, como se sostuvo previamente, el ciberespacio es considerado, a los fines de este trabajo de investigación, como una extensión del sistema internacional, sujeto a las mismas normas y regulaciones del mundo material. Consecuentemente, el vacío conceptual que existe a la hora de definir al terrorismo, se traslada a los actos que puedan ser nominados como tales, y que tomen lugar en el ciberespacio. Se vuelve fundamental, entonces, comprender si el ciberespacio define efectivamente nuevas formas de accionar terrorista, y de ser así identificar de qué manera lo hace.

Sin ignorar las mencionadas diversidades, a los fines prácticos de este análisis, se delimitará el actor terrorista a los grupos subnacionales que hagan uso del terrorismo, y se adoptará la definición que propone Saint Pierre (2003, p. 58), en la que entiende al terrorismo como una forma de violencia que tiene como fin producir una reacción psicológica de terror en el objetivo, sea un individuo, un grupo o un Estado; y que como resultado de este efecto psicológico provoca una conmoción social. De este modo, en palabras del autor, "el fundamento del terror no es la muerte, sino la inseguridad que

provoca, la certeza de la vulnerabilidad ante el accionar terrorista" (Saint Pierre, 2003, p. 61).

El FBI, principal servicio doméstico de inteligencia y seguridad de los Estados Unidos, afirma en su página web que "así como el departamento se transformó para abordar mejor la amenaza terrorista después de los ataques del 11 de septiembre de 2001, está emprendiendo una transformación similar para hacer frente a la amenaza cibernética generalizada y en evolución" (FBI, 2018). Mediante esta afirmación, el FBI reconoce que el terrorismo puede hacer uso del ciberespacio para operar, y define al *ciberterrorismo* como un "ataque premeditado y políticamente motivado contra la información, los programas y sistemas informáticos, y datos, que resultan en la violencia contra objetivos no combatientes, por parte de grupos subnacionales o agentes clandestinos".

La definición que el departamento de inteligencia estadounidense realiza sobre el ciberterrorismo se limita a actores subnacionales, se asemeja a la definición de terrorismo que propone Saint Pierre, y pone en evidencia la necesidad de determinar los riesgos y posibles consecuencias de un ataque terrorista en el ciberespacio. En relación a esto, Singer y Friedman (2014, p. 96) sostienen que para que cualquier análisis sea efectivo, más allá de hipotetizar sobre potencialidades, se debe propender hacia un análisis más objetivo y empírico sobre las capacidades y consecuencias reales de estos ataques. De este modo, argumentan que a pesar de que hasta el 2014 se habían escrito 31.000 artículos discutiendo el fenómeno del ciberterrorismo, no existían hasta el momento personas heridas físicamente o asesinadas por un acto de terrorismo en el ciberespacio.

La inexistencia de consecuencias materiales por ataques terroristas llevados a cabo en el ciberespacio no implica la inexistencia de ataques informáticos con el fin de causar terror, pero a la escasez conceptual del ciberterrorismo se le suman las cuestiones previamente abordadas sobre la atribución en el ciberespacio, lo cual hace que la tarea de determinar los actos terroristas en el ciberespacio sea una tarea mucho más compleja. En un reporte destinado al Congreso de los Estados Unidos, Clay Wilson, especialista estadounidense en tecnología y seguridad nacional, señala esta complejidad para detectar planes de ataques terroristas en el ciberespacio. De hecho, sostiene que no existen evidencias reales de organizaciones terroristas que planeen ataques coordinados contra computadoras o redes, y se limita meramente a señalar la existencia de *botnets* como herramientas que representan un peligro potencial contra los objetivos digitales de

un Estado, dentro de los cuales los principales son los que conforman la infraestructura crítica (Clay, 2005, p. 7-10).

Esta mención de la infraestructura crítica no es menor, ya que un ataque a este tipo de servicios de los cuales depende el funcionamiento de una sociedad, se traduce en una forma muy efectiva de lograr el objetivo del terrorismo, es decir causar terror en una sociedad. En relación a esto, la Oficina de Lucha contra el Terrorismo de las Naciones Unidas (CTC, por sus siglas en inglés de *Counter-Terrorism Committee*), emitió en 2017 un reporte que pone en relevancia este hecho, titulado "Protección Física de la Infraestructura Crítica contra los Ataques Terroristas". En este documento, la oficina realiza una revisión de la situación, y advierte:

> "[la Oficina] alienta a todos los Estados a realizar esfuerzos concertados y coordinados, incluso a través de cooperación, para crear conciencia, para ampliar el conocimiento y la comprensión de los desafíos planteados mediante ataques terroristas, a fin de mejorar la preparación para tales ataques contra infraestructura crítica" (CTED, 2017, p. 11, traducción propia).

En el mismo documento, la CTC presenta a la infraestructura crítica como vulnerable no solo a todo tipo de ataques físicos, sino que cada vez más a ataques realizados a través de Internet (CTED, 2017, p. 9-10). Si se analiza la composición de los sistemas de las industrias pertenecientes a la infraestructura crítica, uno de los elementos más vulnerables ante los ataques informáticos son los denominados sistemas SCADA, los cuales se componen por un conjunto de computadoras y dispositivos encargados de realizar los controles de cada proceso industrial (Clay, 2005, p. 10). Irónicamente, mientras los análisis estadounidenses reconocen a los sistemas SCADA como una vulnerabilidad, más adelante se analizará cómo fueron los Estados Unidos quienes aprovecharon vulnerabilidades en sistemas de control industrial para ralentizar el programa nuclear iraní, en una APT denominada *Stuxnet*.

Hasta el momento, todos los análisis se ocupan de señalar la existencia de vulnerabilidades y amenazas, pero no hablan de casos empíricos, lo que evidencia las dificultades existentes a la hora de determinar los riesgos reales que los ataques informáticos terroristas representan para las estructuras principales de un Estado. Las conclusiones del reporte de Clay al Congreso estadounidense (2005), en la misma línea de lo sostenido por Singer y Friedman (2014, p. 96), aseveran que, a pesar de estas

evidentes vulnerabilidades, la complejidad para perpetrar este tipo de ataques es tan elevada, que se deben considerar los riesgos reales que las herramientas informáticas pueden generar en manos de grupos terroristas. A pesar de la paranoia o el temor que pudieron generar, por ejemplo, en 2010 las amenazas explícitas de ciberataques que *Al Qaeda* propinó a los Estados Unidos, los efectos reales de los mismos terminaron siendo muy menores (Kingsman, 2010).

La razón por la que los efectos de los ataques *ciberterroristas* terminan relativizándose respecto de su intención inicial radica, una vez más, en la capacidad de acción de estos grupos: los recursos necesarios para lograr un ataque informático violento y de gran escala contra, por ejemplo, infraestructura crítica, requiere no solo conocer sobre informática para penetrar un sistema informático, sino también conocer los sistemas industriales que controlan la infraestructura una vez que las defensas informáticas fueron penetradas.

Entonces, ¿qué capacidad tienen los grupos subnacionales terroristas para realizar ataques informáticos con consecuencias materiales o virtuales, y que cumplan con el objetivo de causar una reacción psicológica de terror? En el caso de querer lograr daños materiales, la barrera está determinada por la complejidad técnica que implica alcanzarlos, motivo por el cual los analistas sostienen que es una estrategia rápidamente desestimada por los mismos grupos terroristas (Clay, 2005, p. 18). En el caso de querer lograr daños en recursos virtuales sin lograr explosiones o daños materiales, si bien la complejidad es relativamente menor, Singer y Friedman (2014, p. 98) sostienen que también es menor el efecto psicológico logrado, por lo que también es desestimado por los grupos terroristas, en pos de estrategias mucho más sencillas y efectivas para lograr el fin de provocar terror. Con estas afirmaciones no se busca relativizar la capacidad de acción de grupos terroristas en Internet, pero sí se busca lograr un análisis comprensivo y objetivo del uso *real* que éstos hacen del ciberespacio.

Singer y Friedman (2014, p. 99-101) sostienen que el uso más significativo de Internet que los terroristas han realizado es el de una plataforma de comunicación segura, de bajo presupuesto, y confidencial. La elaboración progresiva de protocolos y medidas de cifrado para proteger la privacidad de las comunicaciones es también aprovechada por los grupos terroristas para proteger sus comunicaciones. Este hecho refleja, una vez más, la neutralidad previamente aludida de los sistemas informáticos: si es una carta de amor, o los planos de un rifle de guerra, una computadora realiza el proceso de cifrado de la misma manera, y los protocolos de transmisión de datos tratan

de la misma manera los paquetes que transportan la información. De esta manera, la creciente cantidad de herramientas informáticas que permiten comunicaciones seguras e indescifrables, sumada a la mencionada existencia de partes de Internet que escapan a formas convencionales de indexación y vigilancia, convierten al ciberespacio en un terreno fértil para la comunicación y la organización de grupos terroristas. Internet le es también funcional a este tipo de grupos al configurarse como una plataforma de difusión sin precedentes para técnicas y procedimientos terroristas (diseños de artefactos explosivos, composiciones para bombas), por lo que el peligro real del ciberterrorismo se traduce en un incremento efectivo en la capacidad de acción de los terroristas, al tener un acceso irrestricto a este tipo de conocimiento.

Una vez más, esta conclusión no tiene como intención relativizar el poder potencial que puede tener un ataque informático para generar terror, sino analizar el uso real que grupos terroristas han hecho hasta la actualidad de Internet y el ciberespacio, y proveer un contexto académico para todas las discusiones que refieran al "ciberterrorismo". La inexistencia, hasta el momento en que se redacta este trabajo de investigación, de ataques informáticos que se puedan caracterizar como *terroristas*, hace que el *ciberterrorismo* se restrinja a la utilización del ciberespacio como un lugar de bajo costo y bajo riesgo para recopilar inteligencia, compartir información y comunicarse. En relación a esta situación empírica, es más que relevante analizar las estrategias adoptadas por los Estados para prevenir el ciberterrorismo, y cuán acordes son en relación a la capacidad de acción de los grupos terroristas en el ciberespacio.

Las medidas contra el ciberterrorismo encuentran parangón en las medidas adoptadas para combatir el terrorismo. Menos de 12 horas después de los ataques del 11 de septiembre en Estados Unidos, el ex presidente George W. Bush proclamó el comienzo de una "Guerra Mundial contra el Terrorismo", una campaña militar de escala global con el objetivo de acabar con el terrorismo internacional, que fue apoyada por miembros de la OTAN y otros aliados (Gordon, 2007). Para lograr este fin, se llevaron a cabo operaciones militares para perseguir y eliminar de manera sistemática a los grupos considerados terroristas, lo cual se tradujo en la invasión militar conjunta de diversos Estados (Saint Pierre, 2003, p. 53). En el ciberespacio, esta Guerra contra el Terrorismo implicó un aumento en la cantidad de programas de inteligencia y espionaje internacional por parte de Estados Unidos y sus aliados.

El mencionado bagaje conceptual subjetivo que implica la definición de un acto terrorista es fruto de grandes conflictos internacionales, en los cuales los Estados toman

diversas posturas respecto a la definición de límites en el accionar de las fuerzas antiterroristas, y esta situación complejiza aún más en el ciberespacio. El aumento de medidas de vigilancia masiva, como las reveladas con las filtraciones de Snowden, realizadas por la Agencia Nacional de Inteligencia de los Estados Unidos, demostraron que estos límites de acción para el combate contra el ciberterrorismo se vuelven mucho más difusos. Mediante las filtraciones se pudo observar que las estrategias se reducían a una recolección indiscriminada de datos por parte de las agencias de inteligencia, para su posterior procesamiento, siendo objeto de espionaje un gran grupo de individuos que pueden o no ser terroristas. Así, como sostienen Singer y Friedman (2014, p. 104), este tipo de accionar es "tratar de encontrar una aguja en un pajar, pero recogiendo todo el pajar en el intento", volviéndose no solo una forma ineficiente de encontrar actividades terroristas en el ciberespacio, sino también una vulneración de la privacidad de los recursos virtuales de individuos y de otros Estados.

Esta relación desproporcionada en las medidas para prevenir el ciberterrorismo, se asimilan a las reacciones desmedidas que Nievas señala que los Estados utilizan para prevenir los efectos del terrorismo en el mundo material. El autor considera que no es razonable que se destine una cantidad tan grande de recursos al combate contra el terrorismo, cuando hay otros problemas que generan más muertes, y reciben menos asignación presupuestaria. De esta manera, Nievas pondera la función política del terrorismo tanto en el mundo material como en el ciberespacio, el cual se vuelve funcional para los gobiernos que quieren o necesitan ampliar la vigilancia de su población, y se convierte en lo que él denomina una "llave" que habilita la excepcionalidad de las medidas antiterroristas (Nievas, 2015, p. 192-196).

Singer y Friedman, sobre la misma línea argumental, sostienen que de la misma manera que el miedo al terrorismo permitió la instalación masiva de mecanismos físicos de control de la población en el mundo material, el ciberterrorismo es la amenaza que habilita medidas de vigilancia masiva en el ciberespacio. Los autores sostienen que el nivel de recolección de datos realizados por la Agencia Nacional de Seguridad de Estados Unidos no tiene correspondencia con la capacidad de acción real que tienen en la actualidad los ataques informáticos organizados por grupos terroristas: si bien, como el mencionado caso de los cortes en los suministros de energía eléctrica del 2017 en Ucrania, un ataque informático complejo con fines terroristas podría interrumpir temporalmente el suministro de energía, otros ataques más sencillos en el mundo

material tienen mayor capacidad de generar terror y daño (Singer y Friedman, 2014, p. 98).

Como se evidenció a lo largo de este análisis, los debates conceptuales del terrorismo y las estrategias antiterroristas adoptadas por los Estados se trasladan sin mayores alteraciones al ciberespacio. Consecuentemente, las capacidades de un Estado para emprender medidas antiterroristas —tanto materiales como virtuales— dependen también de sus capacidades materiales, y varían dependiendo de los recursos asignados para estas estrategias. Independientemente de las individualidades, en el caso de las estrategias adoptadas en el ciberespacio, la función de las medidas antiterroristas se asemeja más, en la actualidad, a la sugerida por Nievas: el *ciberterrorismo* funciona como una "llave" que permite controles virtuales masivos a la población —tanto propia como ajena—, que si bien tiene el objetivo oficial de encontrar terroristas en el ciberespacio, permite la recopilación de una cantidad muy grande de información y datos no relacionados con el terrorismo virtual.

2. Guerras en el ciberespacio

Habiendo realizado un análisis sobre los potenciales peligros que puede implicar la utilización maliciosa de herramientas informáticas, y considerando que los sistemas informáticos de los Estados, utilizados para almacenar y transmitir información, están cada vez más interconectados en Internet, es oportuno analizar qué categorización tendría un ataque informático originado en un Estado, y que tenga como objetivo comprometer los recursos informáticos de otro Estado. Que ambos extremos del conflicto estén ocupados por Estados lo vuelve un tema pertinente a las relaciones internacionales, e inclusive se puede transformar en un enfrentamiento bélico, pero el hecho de que las variables se encuentren atravesadas por la virtualidad, complejiza mucho su definición. De esta manera, es necesario establecer de base hasta qué punto pueden dos Estados desarrollar un enfrentamiento en el ciberespacio.

Como primera medida, es menester definir las concepciones de guerra y de enfrentamientos bélicos en el mundo material, las cuales sirven como punto de partida para la definición de los enfrentamientos en el ciberespacio. Dinstein, especialista en derecho internacional y en leyes de la guerra, aporta una definición elaborada de la guerra:

> "es una interacción hostil entre dos o más Estados, ya sea en un sentido técnico o material. La guerra en el sentido técnico es un estado formal producido por una *declaración de guerra*. La guerra en el sentido material se genera mediante el *uso real de la fuerza armada*, que debe ser integral por parte de al menos una de las partes en conflicto" (Dinstein, 2005, p. 15).

La definición de *guerra* propuesta por Dinstein es funcional en este análisis por dos motivos. En primer lugar, es útil a fines prácticos, ya que circunscribe el estado de guerra a los Estados, excluyendo a los ataques terroristas o cualquier tipo de ataque aislado del análisis, los cuales serían pertinentes a las esferas de seguridad interna de cada Estado. En segundo lugar, formaliza el enfrentamiento bélico a un estado particular, y no a un desorden generalizado de intercambio de ataques. De esta manera se restringen las capacidades de acción de los Estados a los principios de las *leyes de la guerra*, primordialmente al *principio de distinción* (el cual requiere que los ataques se limiten a objetivos militares y que los civiles u objetos civiles no sean objeto del ataque), y al *principio de proporcionalidad* (el cual "prohíbe los ataques que pueden causar pérdida accidental de vida civil, lesiones a civiles, daños a bienes civiles, o una combinación de ambos, que serían excesivos en relación con la ventaja militar concreta y directa") (Koh, 2010).

El estado de guerra puede ser alcanzado, como define Dinstein, tanto por la declaración técnica de guerra emitida por medio de una comunicación oficial, como por una agresión material que inicie las hostilidades. En relación a este último desencadenante, la Organización de las Naciones Unidas define una *agresión* como "el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas" (Asamblea General de las Naciones Unidas, 1967), y establece que los Estados pueden ejercer su derecho a la legítima defensa en caso de ser objeto de tales agresiones a su integridad (Naciones Unidas, 1946, art. 51).

Si se considera al ciberespacio como una extensión del campo de acción de un Estado, en el cual se expresan de manera idéntica las relaciones de fuerza existentes en el sistema internacional, estas definiciones de *estado de guerra* y de *agresión internacional* deberían aplicar a conflictos que se puedan desarrollar en el terreno virtual. Sin embargo, es específicamente la cualidad virtual lo que condiciona el modo

en el que se pueden desarrollar las hostilidades. La definición de agresión que propone la ONU plantea un dilema, ya que fue redactada en un momento histórico en el cual una agresión solo se podía dar en el plano material, en un mundo físico con fronteras Estatales demarcadas, y con posibilidades de probar la procedencia de un ataque. Si bien no es una definición anacrónica, sí se podría calificar de incompleta frente a las posibilidades de ataques informáticos que existen en el mundo contemporáneo.

En 2016, un grupo de *crackers* rusos realizó un ataque de *spear phishing* correos electrónicos de funcionarios de alto rango del Comité Nacional Demócrata, comprometiendo información confidencial, que posteriormente fue filtrada a la prensa y difundida por WikiLeaks. Si bien ya se hizo mención a la dificultad de establecer la atribución en línea, ¿qué pasaría en el hipotético caso de que el gobierno ruso admitiera que fue éste quien promovió el ataque, el cual comprometió la campaña presidencial y generó un detrimento de la imagen pública de la candidata demócrata Hillary Clinton? ¿Sería considerada esta agresión suficiente como para evocar el derecho a ejercer legítima defensa e iniciar un estado de guerra?

Desde el punto de vista del derecho internacional, no hay hasta el momento avances sustanciales como para responder a estos cuestionamientos. Como sostiene Reed (2013) en la revista *Foreign Policy*, "el proceso de formalizar las reglas para el ciberespacio probablemente demorará décadas debido a las diferentes prioridades entre varios gobiernos". De este modo, una de las formas más eficaces para responder estas preguntas es observar cual es la postura individual adoptada por los Estados, y ver cuál es la norma que se manifiesta en su accionar empírico. Los Estados Unidos, por ejemplo, cuentan con una "Estrategia Internacional para el Ciberespacio", en la cual advierten que "responderán a actos hostiles en el ciberespacio como lo harían con cualquier otra amenaza para su país", y que "se reservan el derecho de utilizar todos los medios necesarios (diplomáticos, informativos, militares y económicos) según corresponda y de conformidad con el derecho internacional aplicable, a fin de defender la nación, sus aliados, sus socios y sus intereses" (The White House, 2014, p. 14, traducción propia).

Entonces, bajo la doctrina de la *Estrategia Internacional para el Ciberespacio* de los Estados Unidos, en el hipotético caso de que el gobierno de Rusia admitiese la responsabilidad en los ataques de *crackers* rusos al Comité Nacional Demócrata del 2016, ¿qué tipo de ataques se configurarían como "proporcionales" en el caso de entrar en un estado de guerra? ¿Es suficiente una agresión virtual como ésta para justificar, por

ejemplo, una invasión militar en el mundo material? En el caso de que se restringiera al ciberespacio, si un contraataque informático originado desde los Estados Unidos, enmarcado en este estado de guerra, compromete los servicios de provisión de energía eléctrica de Rusia, ¿se está respetando el principio de distinción, o se está realizando también un ataque generalizado sobre objetivos civiles?

Sin dudas la posibilidad de una *ciberguerra* reconfigura las concepciones tradicionales sobre la guerra, y genera más incertidumbres que certezas. La carencia, hasta el momento de redacción de este trabajo de investigación, de ejemplos empíricos de ataques informáticos entre Estados que se enmarquen en un estado de guerra, hace aún más difícil dilucidar las características intrínsecas que adquieren conflictos bélicos en el ciberespacio. Singer y Friedman (2014, p. 131) sostienen que esta situación de incertidumbre puede generar mucha inquietud, no solo en los individuos sino también en los mismos Estados, por lo que proponen establecer diferencias teóricas entre las guerras tradicionales y las *ciberguerras*.

En primer lugar, sostienen que es poco probable que el ciberespacio multiplique inmediatamente el poder destructivo de las armas, en formas que sí lo hicieron innovaciones tecnológicas previas: si bien un apagón generalizado o la imposibilidad de contar con localización satelital tendrían efectos devastadores, no se acercan a los niveles de destrucción de, por ejemplo, una bomba nuclear. Y, en segundo lugar, sostienen que, a diferencia de las armas convencionales, los ataques informáticos son mucho menos predecibles en su alcance real: *Stuxnet*, por ejemplo, fue un ataque informático que se expandió utilizando técnicas de *gusano informático*, pero a pesar de haber estado diseñado para expandirse en un conjunto específico de computadoras de las centrales nucleares iraníes, terminó infectando, además, a más de 25.000 computadoras en todo el mundo (Singer y Friedman, 2014, p. 132).

De esta manera, los autores sostienen que el ciberespacio sin duda añadirá mucha más complejidad a los ya caóticos escenarios bélicos, pero que su aplicación puede variar, y sus implicancias reales están aún por ser descubiertas. Variables como la desterritorialización, y las problemáticas para establecer las atribuciones de los ataques en el ciberespacio, hacen que las *ciberguerras* tengan más posibilidad de ser estrategias que se realicen sin declaraciones de guerra formales, y sin necesidad de comprometer la imagen de un Estado. Así, sostienen que las ciberguerras, más que un estado de guerra tradicional, posiblemente se constituirían en un intercambio constante e informal de ataques, y este estado se adaptaría mejor a la histórica definición de Carl von

Clausewitz, en la cual afirma que "la guerra no es un fenómeno independiente, sino la continuación de la política por diferentes medios" (Singer y Friedman, 2014, p. 125-132).

Stephen Walt, profesor de relaciones internacionales en la Universidad de Harvard y referente teórico en neorrealismo estructural, reconoce la existencia de varias formas de ataques informáticos que tienen potencial militar, pero invita a revisar, en la línea argumental de Singer y Friedman, los usos reales y efectivos que se les pueden llegar a dar, para evitar que se caiga en lo que denomina una "*inflación de la amenaza*". El autor sostiene que la temática se trata con un alto nivel de esoterismo, lo que produce dos efectos. En primer lugar, se traduce en una incomprensión de las consecuencias concretas de los ataques informáticos por parte de los analistas que no tengan una inmersión técnica en la informática. En segundo lugar, y derivado de este hecho, sostiene que es una oportunidad que permite, al generar incertidumbre, destinar una cantidad de recursos cada vez mayor para prevenir una situación hipotética de la cual no se ha establecido el peligro real (situación análoga a la mencionada con las estrategias para combatir el *ciberterrorismo*), por lo que es necesario un análisis íntegro de costos y beneficios (Walt, 2010).

Para sintetizar este análisis de los conflictos entre Estados en el ciberespacio, se tomará la postura de Singer y Friedman (2014, p. 132), quienes advierten que los ataques informáticos son sin dudas factores que añaden muchas capas de complejidad a los conflictos entre Estados, algunas que inclusive están aún por ser descubiertas. Sin embargo, afirman que el estado actual de la situación resulta en que los enfrentamientos entre Estados en el ciberespacio pueden adquirir dos formas principales. La primera, es la de una guerra sigilosa y sin declaraciones formales, que atenten contra objetivos específicos, y que sean muy difíciles de probar de manera fehaciente, como lo son las Amenazas Persistentes Avanzadas, las cuales serán analizadas en detalle en el último capítulo de este trabajo de investigación.

La segunda forma no excluye a la primera, y está exclusivamente ligada a las cualidades ofensivas que pueden adquirir los ataques en el ciberespacio: sería una situación en el cual los Estados desarrollarían herramientas informáticas con capacidades tanto ofensivas como defensivas, y que la incertidumbre por sus consecuencias, causaría un estado de estabilidad generado por la disuasión resultante.

Stuxnet demostró que las herramientas informáticas tienen la capacidad de causar daños en el mundo material, y las filtraciones en las elecciones estadounidenses

de 2016 demostraron que la información robada de sistemas informáticos puede alterar inclusive el resultado de las elecciones en Estados Unidos. Sin embargo, se sostuvo que una particularidad que tienen las herramientas informáticas es que su costo se concentra en su desarrollo, ya que luego pueden ser reproducidas muy rápidamente. El peligro evidente que demuestra la utilización empírica de los ataques informáticos hace que se desaliente su uso, y se reivindique su capacidad de disuasión: al igual que las armas nucleares, su uso implicaría un perjuicio tan grande, que el efecto disuasivo prevalece por sobre la capacidad real de acción (Singer y Friedman, 2014, p. 145).

Una vez más, en ambas de las formas que pueden tomar los conflictos internacionales en el ciberespacio, las capacidades ofensivas y defensivas dependerán de la asignación de recursos económicos y técnicos que realicen los actores interesados en desarrollarlas. Consecuentemente, frente a otro tipo de actor, los Estados se configuran como los actores con mayor capacidad de acción para el desarrollo de este tipo de aplicaciones informáticas. De esta manera, y al igual que en la configuración de poderes del sistema internacional, serán las grandes potencias quienes marquen el paso y determinen la escala y las potencialidades de las estrategias ofensivas y defensivas en el ciberespacio (Breene, 2016).

3. Posibilidad de una carrera armamentista digital

La mencionada capacidad exponencial que pueden adquirir los ataques informáticos para realizar daños llama a revisar, desde un punto de vista estratégico, hasta qué punto su utilización en una sucesión de ataques y contraataques, no puede derivar en un perjuicio para el actor que inicie las hostilidades. De este modo, al igual que con las armas nucleares o las biológicas, el valor de disuasión que adquieren los ataques informáticos se vuelve una estrategia mucho más llamativa que su utilización.

Al pensar en estrategias de disuasión, el ejemplo histórico más cercano y significativo es sin dudas el modelo de la Guerra Fría de “destrucción mutua asegurada”, conocido por sus siglas en inglés “*MAD*” (de *Mutual Assured Destruction*, las siglas conforman “*loco*” en inglés). Esta premisa implicaba que cualquier tipo de ataque nuclear, sería respondido con un contraataque de igual o mayor magnitud, lo cual derivaría en una destrucción asegurada no solo de ambos bandos, sino también, por la capacidad de destrucción masiva de las armas nucleares, de la mayoría de la vida en el planeta. Afortunadamente, esta situación nunca llegó a ser un hecho empíricamente comprobable, ya que este potencial teórico desalentó durante cuatro décadas la

utilización de armas de tal calibre, y derivó posteriormente en tratados internacionales para evitar la proliferación de este tipo de capacidades ofensivas. Singer y Friedman (2014, p. 144-145) sugieren que, al igual que sucedió durante la Guerra Fría, los programas informáticos con capacidades ofensivas tienen la potencialidad de adquirir un valor disuasivo, que es mejor para alterar las acciones de un adversario sin causarle daños directos.

Si se toma el caso actual de los actores principales del período de la Guerra Fría, Estados Unidos y Rusia (comprendido como Estado principal de la Unión Soviética), ambas se posicionan en el sistema internacional del siglo XXI como potencias militares, tanto en el mundo material como en el ciberespacio. Realizando un análisis costo-beneficio, por ejemplo, ¿le convendría a Rusia realizar un ataque informático contra los Estados Unidos, quienes tienen una capacidad igual o mayor de respuesta? ¿O es más útil para Rusia exhibir sus desarrollos informáticos para desalentar cualquier tipo de ataque por parte de otros Estados, convirtiendo así a las herramientas informáticas en elementos de disuasión?

Joseph Nye (2011), teórico de las relaciones internacionales y principal impulsor del concepto de *poder blando*, se pregunta si existe alguna lección que el período nuclear le pueda dar a estos debates que comprenden a las capacidades ofensivas y defensivas de las herramientas informáticas. Como punto de partida, sostiene que las capacidades destructivas de los ataques informáticos no se comparan con las armas del mundo material, y para argumentarlo cita a Martin Libicki, profesor en el MIT:

> "al contrario que las armas nucleares, los ataques informáticos no representan un peligro existencial […], como mucho, la destrucción o la desconexión de los sistemas informáticos podrían retornarnos a la economía de 1990, mientras que una guerra nuclear nos podría retornar a la Edad de Piedra" (Libicki, 2011, citado en Nye, 2011, p. 22).

A pesar de esta capacidad de acción menor, Nye sostiene que no se deben desmerecer las potencialidades tácticas o estrategias de las herramientas informáticas. De esta manera, sostiene que el estado de "destrucción mutua asegurada" de la Guerra Fría, que derivó en una carrera armamentista nuclear, es uno de los elementos principales a los que se le debe prestar atención, por su plausibilidad de reproducción en el ciberespacio (Nye, 2011, p. 34). Afirma que, si bien los Estados Unidos y la Unión Soviética desarrollaron algunas reglas tácitas sobre el comportamiento prudente

respecto a las armas nucleares desde el principio de la Guerra Fría, el período se caracterizó por una sucesión de avances técnicos en las capacidades destructivas de las armas, las cuales sólo aumentaban su valor por su capacidad disuasiva.

Al igual que en el caso nuclear, las capacidades de los Estados son determinantes clave a la hora de entrar en una carrera armamentista en el ciberespacio, donde las herramientas informáticas se constituyen como el capital principal. Como sostienen Singer y Friedman, “al igual que en la influencia militar tradicional, el poder cibernético de Burundi palidece en comparación con el de los Estados Unidos o China” (Singer y Friedman, 2014, p. 156). En relación a esto, McAfee, una empresa de seguridad informática estadounidense, estima que sólo hay una veintena de países que realmente tienen programas avanzados de ciberguerra, con la capacidad de generar ataques informáticos con una capacidad ofensiva compleja.

Independientemente de la sectorización que se pueda generar en el sistema internacional debido a la exclusividad requerida para realizar avances significativos en las capacidades de los ataques informáticos, es útil revisar, nuevamente, cual es la concepción de las grandes potencias al respecto. Singer y Friedman revelan que un ex Subsecretario de Defensa para Asuntos Estratégicos Globales del gobierno estadounidense, admitió que “los Estados Unidos consideran que existe una carrera de armamentos en el ciberespacio, y que es muy intensa” (Singer y Friedman, 2014, p. 156).

Nye (2011, p. 34) sugiere que, si es efectiva la existencia de una carrera armamentista digital, es necesario revisar de qué manera se puede evitar la proliferación de herramientas informáticas con capacidades militares. Y aquí es donde se complejiza una vez más el campo de acción, debido a la mencionada cualidad virtual de los recursos. A diferencia de una bomba atómica, la cual requiere no solo materiales escasos y costosos, sino también el conocimiento necesario para saber qué hacer con ellos, la proliferación en el caso de ataques informáticos se limitaría a copiar y pegar el código de un programa, e intentar reproducirlo contra un nuevo objetivo. Si bien lo verdaderamente valioso es contar con los recursos para desarrollar de manera efectiva y constante este tipo de herramientas informáticas, es irónico el caso de que pocas semanas después de que se descubriera *Stuxnet*, ya existían guías en línea para reconstruir el ataque (Zetter, 2011).

La complejidad que introduce el ciberespacio para contener la proliferación de las herramientas informáticas modifica las condiciones dentro de las cuales se puede

desarrollar una carrera armamentista digital. Como se sostuvo, en la práctica, se ha demostrado que el peligro real reside en quién posee el conocimiento para generar los ataques informáticos, y es por eso que las potencias que poseen mayores recursos para invertir en estos desarrollos, conservan la mayor capacidad de acción. Si bien, como confirman Singer y Friedman (2014, p. 147), se puede afirmar que una carrera armamentista digital ya está en curso, una competencia para lograr mayores capacidades de acción debería estar acompañada de estrategias que desalienten la proliferación, ya que podría derivar en una situación de empoderamiento de Estados o grupos que no necesiten una dinámica disuasiva, y hagan uso de herramientas informáticas altamente dañinas.

4. Del complejo industrial-militar al complejo *ciber-militar*

Durante el discurso que culminó su mandato en 1961, el ex presidente estadounidense Eisenhower advirtió sobre las capacidades de lo que él consideraba un creciente riesgo para las libertades y las democracias: el *complejo industrial-militar*. Este complejo hace referencia a un grupo de intereses de la industria militar, que utiliza su poder económico para realizar *lobby* a favor de medidas que propendan a la inversión en desarrollos militares y en defensa (Turley, 2014). Uno de los pilares que promovió la aceptación generalizada de la inversión en defensa durante la Guerra Fría, fue la existencia de un polo antitético en el sistema internacional: la Unión Soviética. En el mundo de post-Guerra Fría, a pesar del creciente número de conflictos, uno de los elementos principales que justifica estas inversiones, es la amenaza terrorista. El complejo industrial-militar ha sido el foco en diversos análisis que abordan las políticas armamentistas de los Estados, y resulta pertinente en este trabajo revisar qué tipo de variaciones puede introducir el ciberespacio en los intereses de los sectores industriales militares.

Singer y Friedman advierten que el potencial para el desarrollo de un complejo es real, y es abonado por diversas iniciativas y eventos, dentro de las cuales destacan una invitación que los autores recibieron para asistir a una conferencia, con el siguiente mensaje:

> "A diferencia de la mayoría de las guerras, la guerra cibernética no tendrá fin, ya que Internet, junto con la continua globalización de industrias fundamentales, creará nuevos campos de batalla para proteger. La inversión necesaria para proteger a las empresas

> estadounidenses y al gobierno de los Estados Unidos crecerá a tasas exponenciales, las asociaciones públicas y privadas tendrán que florecer, cada vez más empresas de defensa existentes tendrán que pivotar y aumentarán las oportunidades de fusiones y adquisiciones y de inversión. Si desea invertir en esta carrera de armas informáticas, entonces esta es la conferencia para usted" (Singer y Friedman, 2014, p. 162).

Este mensaje promocional invita a considerar las posibles consecuencias del crecimiento de este sector industrial, dedicado al desarrollo de herramientas informáticas con capacidades ofensivas y defensivas, y que se caracteriza no solo por el surgimiento de nuevas empresas, sino también por la reconversión de empresas que históricamente proveyeron recursos a los sectores de Defensa de los Estados. De hecho, fue noticia el reposicionamiento de grandes conglomerados de defensa como *Boeing* y *Northrop Grumman*, los cuales han comenzado a desarrollar herramientas para servir al mercado de seguridad informática (Deibert y Rohozinski, 2011).

Cybersecurity Ventures, una revista estadounidense de seguridad informática, sostiene que, en el año 2004, el mercado global de seguridad informática tenía un valor de 3.500 millones de dólares, y en 2017 escaló a más de 120.000 millones de dólares. Este crecimiento de 35 veces su valor de mercado en 13 años, habla de la potencialidad económica que tiene la seguridad informática, y el desglose de las principales empresas de seguridad informática muestra que existe una gran concentración en las principales potencias: 79 de las 100 empresas de seguridad informática más importantes del mundo son originarias y tienen sede en los Estados Unidos (Cybersecurity Ventures, 2018).

Si bien este complejo ciber-industrial se encuentra liderado por los Estados Unidos, la revista Forbes señala que es una tendencia generalizada de crecimiento en todo el mundo, y afirma que hubo un millón de aperturas de puestos de trabajo en ciberseguridad sólo en 2016, cifra que se espera que crezca a seis millones de puestos de trabajo demandados a nivel global en 2019 (Morgan, 2016). De esta manera, Singer y Friedman (2014, p. 164) sostienen que, al igual que lo sucedido con el complejo industrial-militar originado en la Guerra Fría, cuando un Estado tiene un gran presupuesto de defensa atendido por el sector privado, se crean potenciales circunscripciones por parte de las grandes empresas: si bien adquieren un valor estratégico significativo, esta importancia puede derivar en una influencia deliberada sobre las políticas, percepciones de amenazas y estrategias de los Estados.

Para no sobredimensionar el poder que adquieren este tipo de empresas, es menester lograr análisis objetivos, que despojen las amenazas del ciberespacio de posibles intereses corporativos, y que contextualicen de manera efectiva el alcance y los peligros de los ataques en el ciberespacio. Como se sostuvo previamente, los peligros en el ciberespacio existen y tienen grandes potencialidades, pero deben ser analizados objetivamente para evitar distorsiones en las decisiones adoptadas por los Estados, o las "inflaciones de las amenazas" sugeridas por Nye. La forma en que los Estados se posicionen frente a este mundo atravesado por la tecnología, y su comprensión objetiva de las amenazas en el ciberespacio es muy importante, ya que condicionará el futuro de Internet, la posibilidad de enfrentamientos en el ciberespacio, e inclusive *ciberguerras* de escala global (Singer y Friedman, 2014, p. 165). Como en el resto de las esferas gubernamentales, las capacidades ofensivas y defensivas de los Estados en el ciberespacio se encuentran ligadas a la asignación de recursos en Defensa, por lo que serán las grandes potencias militares del sistema internacional serán las que marcarán el camino.

Independientemente de la capacidad de acción individual de cada actor, se analizarán las diferentes estrategias que los Estados pueden implementar para insertarse en el ciberespacio. Desde la perspectiva tradicional de las relaciones internacionales, la búsqueda de acuerdos internacionales es una de los caminos hacia los que se apunta. Desde la perspectiva de la seguridad informática, existen diversas estrategias técnicas que los Estados pueden utilizar para mejorar su posicionamiento en el ciberespacio.

III. Políticas de Defensa en el ciberespacio

Si el ciberespacio se conforma como una extensión del sistema internacional, en el cual los Estados también son los actores principales encargados de establecer las reglas de juego, es primordial analizar cuáles son las políticas de Defensa en el ciberespacio, es decir de qué manera se posicionan los Estados para defender sus recursos frente a las amenazas virtuales provenientes de Internet. Algunas posturas sostienen que el ciberespacio ha llegado a un punto tal de extensión, que no puede ser considerado propio de ningún Estado, y que, por consiguiente, las estrategias de Defensa deben ser producto de acuerdos internacionales que regulen el uso que se le da al ciberespacio, entendiéndolo como un espacio común. Por el contrario, otras posturas sostienen que el estado de anarquía que se configura en el ciberespacio deriva en que, si

bien no existen fronteras en el ciberespacio, cada computadora y red que permiten que Internet y el ciberespacio existan, sí están dentro de las fronteras soberanas de un Estado, motivo por el cual la forma en que se administra y se defienden los recursos depende de las políticas de defensa individuales adoptadas por cada Estado (Singer y Friedman, 2014, p. 182).

Algunas de las cosmovisiones planteadas por la teoría de las relaciones internacionales son funcionales en términos metodológicos para explicar las diferentes posturas que existen a la hora de determinar las estrategias de Defensa en el ciberespacio. Joseph Nye (2011, p. 34), desde la postura de la interdependencia compleja, sostiene que es absolutamente necesario lograr una cooperación internacional temprana, para efectivizar controles en los desarrollos armamentísticos digitales, y para regular las asimetrías en las capacidades de acción de diferentes Estados. A pesar de señalar la importancia de acuerdos que propendan al control conjunto del ciberespacio como estrategia de Defensa colectiva, Nye es consciente de que existen dos grandes impedimentos que no se han podido sortear hasta la actualidad. El primero refiere a las diferencias en normas culturales entre los diversos Estados interesados en regular el ciberespacio; y el segundo impedimento refiere la cualidad técnica de un acuerdo internacional de estas características, ya que la naturaleza descentralizada de Internet se traduciría en una dificultad muy grande, no solo para negociar condiciones, sino aún más para comprobar que éstas sean respetadas.

Desde una postura teórica mucho más realista en términos de la teoría de las relaciones internacionales, Rex Hughes, asesor de la OTAN, plantea una realidad muy diferente respecto a las intenciones que los países líderes del sistema internacional tienen sobre el ciberespacio, específicamente de países pertenecientes a la OTAN: afirma que si bien la respuesta oficial es que sí se busca que haya reglas que contribuyan a regular al ciberespacio, y que apliquen las leyes del conflicto armado a eventuales enfrentamientos, la respuesta extraoficial siempre será que no conviene que se lleguen a acuerdos de estas características, ya que “los países que tienen capacidades avanzadas desean preservarlas” (Menn, 2011).

Estas posturas dispares en relación a las estrategias de Defensa en el ciberespacio se ven enmarcadas en debates muy contemporáneos, dentro de los cuales uno de los que puede considerarse como más significativo es el de la *gobernanza de Internet*. En 2005, la Cumbre Mundial sobre la Sociedad de la Información, evento

patrocinado por las Naciones Unidas, definió la gobernanza de Internet como "el desarrollo y la aplicación por parte de los gobiernos, el sector privado y la sociedad civil, en sus respectivos roles, de principios, normas, reglas y procedimientos de toma de decisiones compartidos, y programas que dan forma a la evolución y uso de Internet" (WSIS, 2005, art. 34, traducción propia). Esta definición de gobernanza de Internet deja en claro que los organismos internacionales reconocen que Internet y el ciberespacio no tienen un gobierno jerárquico e institucional, y que la coordinación entre las decenas de miles de entidades (en su mayoría del sector privado) que mantienen la infraestructura de Internet, deben ser ayudadas por los Estados en su tarea (Masters, 2014).

La mencionada definición de gobernanza de Internet es importante para este análisis, ya que explica la posición que asumen los Estados en el ciberespacio. Si bien son capaces de implementar políticas para el control de los dispositivos físicos que controlan la infraestructura de Internet dentro de sus fronteras, los Estados se insertan en el ciberespacio como un actor más. Un tipo de actor muy particular e importante, con una capacidad de acción mucho mayor que el resto de los actores, pero, en fin, como un usuario más. Este hecho da como resultado que ningún Estado, en el caso de tener la intención, pueda contar ni con el poder ni con la autoridad como para modificar sustancialmente al ciberespacio, ya que la naturaleza descentralizada de Internet no lo permitiría. De esta manera, los Estados adoptan posturas que tienden a la promoción de políticas para regular las acciones en el ciberespacio, y políticas de Defensa individuales para proteger sus recursos frente a la amenaza que puedan representar otros actores (Masters, 2014).

Un caso paradigmático que evidencia esta realidad sucedió 2011, durante las revueltas de la Primavera Árabe, cuando el gobierno egipcio intentó cerrar el acceso a Internet durante las protestas masivas. Frente a esta iniciativa gubernamental, grandes conglomerados tecnológicos como *Google*, *Twitter* y *Skype* brindaron apoyo técnico a los manifestantes, y les proveyeron de diversas soluciones para evitar la censura gubernamental en Internet. La más icónica se denominó "*Speak to Tweet*" (Habla para *twitear*), mediante el cual los mensajes de voz enviados por teléfono por los manifestantes se convertían en *tweets* de texto y audios descargables, permitiéndoles así a los manifestantes censurados el envío de noticias en tiempo real (Singh y Mardini, 2011). Este caso demuestra que, si bien un Estado podría propender en casos extremos a

denegar el acceso a Internet de sus ciudadanos, la naturaleza descentralizada del ciberespacio generaría medios alternativos de acceso.

De este modo, si bien los Estados tienen una gran capacidad de acción, por contar con mayores recursos económicos y técnicos, se ven condicionados por el ciberespacio y su dinámica, al igual que lo hacen en la *estructura* definida por el neorrealismo estructural. Se procederá a analizar cuáles son las acciones que los Estados pueden tener en el ciberespacio, como propuestas de política de cooperación que tiendan a la regulación del uso de Internet, y el diseño de estrategias de Defensa de sus recursos frente al resto de los actores del ciberespacio. A pesar de que las capacidades de acción están determinadas por los recursos que se puedan invertir en los desarrollos de programas informáticos, motivo por el cual las grandes potencias se destacan como las más poderosas en el ciberespacio, también existen una serie de estrategias que se analizarán, las cuales propenden a la ecualización generalizada de las posibilidades de Defensa de los Estados, independientemente de las capacidades individuales.

1. Abordaje desde el derecho internacional. ¿Un tratado que regule al ciberespacio?

El ciberespacio, comprendido como un área más en la que se desarrollan las relaciones interestatales, no difiere conceptualmente de diversas zonas comunes para los Estados, como pueden ser el océano o el continente antártico. De esta manera, se vuelve relevante analizar la capacidad de respuesta que puede brindar el Derecho Internacional para regir sobre el ciberespacio, y si sería posible que exista algún tipo de tratado internacional que lo regule, así como existen, por ejemplo, el Tratado Antártico y la Convención de las Naciones Unidas sobre el Derecho del Mar.

Una de las posibles estrategias ha sido propuesta por Brad Smith, el presidente y Director Jurídico de la empresa de tecnología *Microsoft.* Reconociendo la hostilidad de muchos actores en el ciberespacio, y su potencialidad de convertirse en un campo de batalla virtual entre Estados, Smith propuso en la Conferencia *RSA*, una de las conferencias más grandes de seguridad informática del mundo, lograr algún acuerdo internacional que se asemeje a unas “Convenciones de Ginebra Digitales” (Guay y Rudnick, 2017). Haciendo alusión a los convenios que regulan el derecho internacional humanitario desde 1864 con el propósito de proteger a las víctimas de los conflictos

armados, la empresa de tecnología sostiene que en la medida en que los Estados desarrollen mayores capacidades ofensivas en el ciberespacio, deben existir acuerdos internacionales que sirvan para regular los alcances de este tipo de herramientas (Microsoft, 2018).

Singer y Friedman (2014, p. 186) señalan que, en la misión de regular el ciberespacio mediante acuerdos internacionales, también se han propuesto como modelo diversos acuerdos vigentes, como el tratado de 1967 sobre el espacio ultraterrestre, o el Tratado Antártico, al ser éstos territorios que plantean una naturaleza análoga: son ámbitos abiertos por la tecnología, utilizados para múltiples propósitos, y que ningún Estado puede pretender poseer. De este modo, los autores sugieren que de la misma manera en que acuerdos internacionales de esta naturaleza fueron funcionales en la prevención de la militarización de zonas comunes a todos los Estados, se podría lograr de la misma manera un tratado que regule el ciberespacio.

Sin embargo, a la hora de acordar cuáles serían los alcances de este tipo de tratados en el ciberespacio, a pesar de las similitudes conceptuales con otros acuerdos, la virtualidad es un factor que indudablemente distorsiona los análisis, y agrega un grado más de dificultad a entendimientos internacionales que de por sí ya son extremadamente complejos. Además, como si la complejidad en la delimitación de los alcances no fuera suficiente, la virtualidad también introduciría impedimentos técnicos para comprobar su aplicación: identificar un submarino nuclear que cruza los 60 grados de latitud en un mapa es una violación de tratados internacionales mucho más tangible y detectable que, por ejemplo, la posesión por parte de un Estado de un programa informático con capacidades ofensivas (Singer y Friedman, 2014, p. 186).

Una de las convenciones más desarrolladas hasta el momento de redacción de este trabajo de investigación que intenta regular algunos aspectos de Internet y el ciberespacio, sólo ha prosperado ya que gira en torno a los intereses compartidos por los Estados que la firmaron: asegurarse que Internet funcione bien y sin criminales. La *Convención sobre el Delito Cibernético* del Consejo de Europa se encuentra vigente desde el 2001, y establece pautas para compartir datos e inteligencia entre los gobiernos parte, en casos transfronterizos de fraude bancario, robo de identidad, pornografía infantil, *phishing* y otras manifestaciones en línea del crimen organizado (Moore, 2010). Si bien esta convención cuenta con 57 estados parte, tanto europeos como de otras partes del mundo, la forma en que plantea el tratamiento de la información hace que

muchos Estados duden de su utilización, y se traduce que hasta la actualidad no haya podido adquirir una escala mayor que el treinta por ciento de los países que conforman el sistema internacional.

De esta manera, no solo es complejo lograr acuerdos que regulen un escenario virtual, sino que a esta tarea se le suman dificultades más convencionales, tales como las percepciones que cada Estado tiene sobre lo que se conforma como un acto ofensivo en el ciberespacio, que puede ser diferente de Estado en Estado, y complejiza aún más la tarea de crear regulaciones comunes (Singer y Friedman, 2014, p. 190). En relación a esto, Markoff y Kramer (2009) sostienen que los Estados Unidos y Rusia, los actores que pueden considerarse —junto a China— con mayor capacidad de acción en el ciberespacio, difieren sustancialmente sobre la forma en que se puede llegar a un tratado internacional. Los autores afirman que, si bien ambas naciones coinciden en que el ciberespacio se está configurando como un campo de batalla emergente, Rusia está a favor de un tratado internacional en la línea de los negociados para armas químicas, que implicaría un control y una prohibición de los ataques informáticos; mientras que los Estados Unidos argumentan que un tratado es innecesario, y que la solución reside en la cooperación de grupos internacionales de aplicación de la ley ya existentes.

Indudablemente existen múltiples aristas que dificultan la concreción, hasta la actualidad, de acuerdos internacionales que regulen el ciberespacio. Esto no significa que sea imposible, pero sí evidencia que los esfuerzos que se han realizado han sido estériles, o han tenido consecuencias menores a las pretendidas, y que habrá que esperar más tiempo para la concreción de acuerdos de base, que permitan avances sustanciales en tratados internacionales. Es necesario aclarar, sin embargo, que la carencia de acuerdos no significa que la anarquía en el ciberespacio llegue a un estado de descontrol generalizado, por lo que se deben contextualizar las proposiciones como las planteadas por *The Economist* (2012), donde sugieren que esta falta de acuerdos puede derivar en una “guerra fría digital”.

Hasta el momento, la carencia de acuerdos internacionales unánimes lleva a que cada Estado determine individualmente lo que considera como un ataque informático, una agresión informática, o un delito cibernético (Clough, 2015, p. 736). De este modo, si bien no se deben desestimar categóricamente los desarrollos que el Derecho Internacional ha aportado para regular las hostilidades en el ciberespacio, en la actualidad prevalecen las políticas de defensa individuales de cada Estado en el

ciberespacio, y las maneras en que éstos plantean sus estrategias de seguridad informática. Para este análisis, entonces, se vuelve más relevante analizar cuáles son estas posturas, y cuáles son las posibles posiciones y estrategias que pueden adoptar los Estados para realizar una defensa eficiente de sus recursos informáticos.

2. Políticas estatales de Defensa en el ciberespacio

Un análisis pormenorizado de todas las políticas individuales de Defensa que los Estados adoptan en el ciberespacio, sería de tal escala y complejidad que escaparía a los límites de este trabajo de investigación. Si se realiza un abordaje heurístico, se puede sostener que la mayoría de los Estados adoptan estrategias activas y preventivas frente a las amenazas en el ciberespacio, y estas estrategias siempre dependen de las percepciones y la capacidad de acción de los Estados (Clough, 2015, p. 736).

En relación a esto, el director de la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) de los Estados Unidos, organismo que contribuyó a crear la infraestructura base del Internet moderno, sostuvo que las estrategias de seguridad informática en el ciberespacio "han crecido exponencialmente en esfuerzo y complejidad, pero continúan siendo derrotadas por ataques informáticos que requieren mucha menos inversión por parte de los atacantes" (Singer y Friedman, 2014, p. 154). Esta declaración es importante ya que demuestra la naturaleza que deben tomar las estrategias defensivas en el ciberespacio: las nuevas amenazas surgen constantemente, motivo por el cual las estrategias de Defensa no pueden ser estáticas, sino que deben estar siempre listas para responder ante nuevos riesgos.

Las consultorías de seguridad informática en empresas, conocidas como *penetration testing* (pruebas de penetración), se han multiplicado exponencialmente, y son útiles para determinar, antes que un atacante, cuáles son las vulnerabilidades de un sistema informático, y cuáles deberían las estrategias que se necesitan adoptar para minimizar los riesgos y proteger los recursos virtuales de una empresa. En comparación, la escala, la complejidad, y la cantidad de usuarios que tienen los sistemas informáticos de un Estado son mucho mayores, y se podría argüir que almacenan y transmiten datos mucho más estratégicos: si bien una empresa puede almacenar, por ejemplo, los datos de las tarjetas de crédito de sus usuarios, los sistemas informáticos estatales contienen la identidad de sus ciudadanos, comunicaciones oficiales, planes de gobierno, y un sinfín de información sensible y estratégica para los intereses y la soberanía de un Estado.

Las estrategias genéricas de seguridad informática que se recomiendan a las empresas también aplican a las medidas que los Estados pueden tomar para crear sistemas más robustos, y son medidas técnicas como, por ejemplo, el uso de contraseñas más seguras, la implementación de firmas digitales, controles de acceso a las redes, entre otras (Alton, 2018). Sin embargo, la protección de una infraestructura informática como la que poseen los Estados, de tal escala y complejidad, y sobre todo por la cualidad estratégica de la información que contiene, amerita la aplicación de estrategias de seguridad informática verdaderamente integrales, que no dependan exclusivamente de variables técnicas, y que tomen en consideración los factores necesarios para evitar que se comprometan los recursos virtuales.

Si bien no existen soluciones ubicuas que puedan ser aplicadas en todos los casos específicos, sí existen estrategias de base que pueden ser adoptadas por todos los Estados para incrementar los niveles de protección en el ciberespacio y minimizar los *vectores de ataque*, es decir los puntos vulnerables por los cuales un atacante puede penetrar un sistema informático. Las dos estrategias que se detallarán a continuación, una de índole técnica y otra no técnica, de ser aplicadas por los Estados en combinación, no solo implicarían una mejora en términos teóricos, sino que estas mejoras se encuentran documentadas por evidencias empíricas. La aplicación conjunta de estas estrategias daría como resultado un aumento cualitativo en las defensas virtuales de los Estados, al permitir reducir las potenciales vulnerabilidades en sus sistemas informáticos.

a) Los programas informáticos libres de código abierto

Como se sostuvo previamente, existen dos formas para desarrollar programas informáticos, y la distinción gira en torno al tratamiento que recibe el código fuente (las instrucciones escritas que se le dan a la computadora) de un programa informático. La primera forma se denomina *privativa*, y es aquella en la que el código fuente se encuentra intencionalmente oculto, y las instrucciones pueden ser interpretadas por una computadora, pero no leídas por otra persona más que su desarrollador; y la segunda forma se denomina de *código abierto*, y es aquella en la que el código fuente se encuentra disponible para su escrutinio y modificación por cualquier interesado.

Desde la seguridad informática, estas dos maneras de producir programas informáticos se fundamentan en dos perspectivas diferentes sobre la forma de garantizar

la seguridad de los programas. La primera perspectiva, denominada *paradigma de seguridad por oscuridad*, tiene su origen en el paradigma privativo, y sostiene que ocultar el código fuente se constituye en una manera de resguardar los derechos de autor del dueño del programa (Miessler, 2009). La *seguridad por oscuridad* se constituye, entonces, en una consecuencia inevitable de este paradigma, el cual se ha cuestionado en diversos trabajos teóricos que evidencian que tarde o temprano los secretos en el código se revelan y derivan en problemas de seguridad informática.

Uno de los desarrollos teóricos más importantes que refutan la efectividad a largo plazo del paradigma de *seguridad por oscuridad,* es el mencionado Principio de Kerckhoffs, el cual sostiene específicamente que la seguridad de un sistema nunca debe depender de que su diseño permanezca en secreto. El Principio va inclusive un paso más allá que desestimarlo, alentando a los implementadores de sistemas de seguridad a lograr garantizar la seguridad de un programa informático, inclusive si todos los parámetros de su sistema criptográfico son de público conocimiento. Hoepman y Jacobs (2005, p. 2), del grupo de Seguridad de Sistemas del Instituto de Informática y Ciencias de la Información de la Universidad de Nimega, intentan —a pesar de las dificultades que esto implica— poner en perspectiva esta crítica al paradigma de seguridad por ocultamiento, llevándolo a un ejemplo menos técnico: “Si una persona viajara lejos de su casa y se enfermase, ¿tomaría medicamentos de una marca totalmente desconocida, proveídos por un médico cuya formación profesional desconocen, y por lo tanto sin una garantía —más que la brindada por el mismo médico— sobre la naturaleza del medicamento?”. De forma análoga, los desarrolladores de programas privativos proponen un concepto de programa informático igual que una *caja negra*: el usuario introduce información en un programa, y según su criterio no tiene por qué saber cuál es el proceso que éste realiza, siempre y cuando el resultado sea el esperado.

El desconocimiento del código fuente de los programas informáticos privativos deriva en que la seguridad quede a cargo exclusivamente del desarrollador, y si existiese algún tipo de vulnerabilidad, la imposibilidad de ser visto públicamente se constituye como el factor principal que otorga la seguridad. Sin embargo, el problema reside en que este paradigma asume que no existe nadie más con la capacidad de descubrir vulnerabilidades, y eso no es algo que se pueda garantizar en ningún desarrollo informático, ya que existen diversas técnicas, como la *ingeniería inversa*, que permiten descubrir vulnerabilidades incluso en programas privativos. Usualmente, los actores que

buscan de manera activa fallas en un sistema informático, no se caracterizan por tener buena fe en su accionar, motivo por el cual hay mayor probabilidad de una utilización criminal del eventual descubrimiento de una vulnerabilidad. De esta manera, de darse esta situación, no existe una protección real para evitar que ésta sea aprovechada con fines maliciosos, mucho menos si los dispositivos vulnerables están conectados a Internet.

Estas críticas al modelo privativo, sin embargo, no son sólo teóricas, y se demuestran en casos empíricos: el caso de *spear phishing* contra el Comité Nacional Demócrata estadounidense durante la campaña presidencial estadounidense hizo uso de vulnerabilidades en Microsoft *Windows 10, Adobe Flash* y *Java*, todas herramientas informáticas privativas (Edwards, 2017). El *ransomware* WannaCry, que infectó y cifró en 2017 más de 230.000 computadoras en más de 150 países, hizo uso de una vulnerabilidad en un protocolo privativo de *Windows* que afectaba específicamente a este sistema operativo (Goodin, 2017). *Stuxnet*, la APT que logró ralentizar el desarrollo nuclear en las instalaciones nucleares iraníes, hizo uso de cuatro vulnerabilidades *día cero* diferentes, encontradas en el sistema operativo privativo *Microsoft Windows* (Naraine, 2010).

Estos tres ejemplos, con graves consecuencias institucionales, demuestran el peligro en el que deriva la dependencia del ocultamiento para garantizar la seguridad de un programa informático. De esta manera, muchos llegan a entender que el modelo privativo se reduce a una relación de poder, en la cual el desarrollador del programa informático es el único garante de la seguridad de su programa, y el usuario debe confiar en la capacidad del desarrollador para garantizar la seguridad (Sistema Operativo GNU, 2018a). Sin embargo, si algo demuestran los ejemplos previamente mencionados, es que ni siquiera los conglomerados más grandes de tecnología pueden garantizar una certeza absoluta sobre la seguridad de sus programas. Sumado a esto, los únicos capaces de actualizar el programa informático con las correcciones en el código para solucionar vulnerabilidades son los mismos desarrolladores. Esto deriva en que de la capacidad de respuesta de los desarrolladores dependa la extensión temporal de la "ventana de vulnerabilidad", es decir el tiempo entre que se lanza un ataque que hace uso de una vulnerabilidad previamente desconocida, hasta que el programa es actualizado por el usuario final (Edwards, 2017).

Si bien este debate sobre la relación de poder entre desarrollador y usuario da lugar a diferentes posturas, se podría argüir que, en última instancia, la decisión de utilizar programas privativos, cuando éstos pretenden ser utilizados con fines privados o empresariales, reside en el usuario final. Por ende, las posibles consecuencias relacionadas con potenciales vulnerabilidades en los programas, son causadas por la decisión de los actores particulares que eligen utilizar programas informáticos privativos. Sin embargo, cuando el usuario de un programa informático no es un particular, sino un empleado público que utiliza herramientas informáticas para almacenar y transmitir información estratégica para los intereses de un Estado, o un funcionario público que lo usa para comunicaciones confidenciales, es apremiante la implementación de sistemas que planteen un tratamiento seguro y confidencial de la información.

El paradigma que se alza como contraposición al de seguridad por ocultamiento es el *paradigma de seguridad por exposición*, conocido en inglés como *Open Security*. Esta postura sostiene que, al desarrollar programas informáticos de *código abierto*, el código fuente de los programas se encuentra públicamente disponible, por lo que los problemas y las vulnerabilidades de seguridad se pueden prevenir ya que un número mayor de programadores pueden ver y modificar el diseño del programa, mejorando la seguridad mediante la colaboración (Wheeler, 2013). Los principales impulsores de los programas de código abierto ponderan esta estrategia como una de las maneras más eficientes de lograr la seguridad de las implementaciones informáticas, ya que no solo previene la inclusión de vulnerabilidades por errores no intencionados, sino que elimina la potencialidad de peligros aún mayores, como la inclusión intencional de funciones maliciosas en un programa informático. La estructura privativa permite este tipo de accionar, dando lugar a la posibilidad de incluir funcionalidades de, por ejemplo, espionaje o robo de datos, mientras que la apertura del código las evidenciaría de manera inmediata, haciendo que sea muy difícil de ocultarlas.

La *Fundación por el Software Libre* (FSF, por sus siglas en inglés de *Free Software Foundation*), es una organización sin fines de lucro fundada en los años ochenta, que realiza un abordaje integral sobre las capacidades informáticas de los programas modernos, y reivindica los ideales de apertura y colaboración originarios de la *cultura hacker* descritos por Castells (2000). De esta manera, la FSF sostiene que, al igual que los primeros programas informáticos, la libertad debe ser el principio que rija

la creación de los programas informáticos, y esta libertad se expresa en un frente técnico, y en uno humano. Desde la perspectiva técnica, requiere que el código fuente del programa informático se encuentre abierto y libre para su observación; y desde la perspectiva humana, sostiene que, gracias a esta apertura, el usuario debe contar con la libertad de poder utilizar el programa como lo desee, estudiar su funcionamiento sin restricciones, poder adaptarlo a sus necesidades, y poder mejorarlo, copiarlo y distribuirlo sin ningún tipo de límite (Sistema Operativo GNU, 2018a).

Una vez más, si el uso es particular, la decisión de usar programas informáticos privativos o de código abierto reside en el usuario. Pero si se utilizan programas privativos para, por ejemplo, crear bases de datos con la identidad de los ciudadanos de un país, no existen garantías de que ese programa no esté, por ejemplo, enviando paralelamente la información a un servidor localizado en otro país. Esto no quiere decir que todos los programas informáticos privativos contengan funciones maliciosas, pero la imposibilidad de comprobar que no las contengan es una razón suficiente para buscar soluciones informáticas que propendan a niveles mayores de seguridad de almacenamiento y transferencia de información, sobre todo cuando esta información en manos equivocadas puede significar perjuicio para un Estado o sus ciudadanos.

El argumento técnico para ponderar la apertura del código fuente de un programa informático es la *auditabilidad*. Esta cualidad implica que, al estar disponible para el que lo requiera, la cantidad de ojos críticos que se encuentran examinando la estructura del código fuente de un programa hacen que pueda ser evaluado, mejorado y mantenido por un gran número de desarrolladores, resultando en programas y aplicaciones mucho más robustas y seguras (Sridhar et al., 2005, p. 944). Si las implementaciones están bien realizadas, la información se mantiene secreta en ambos extremos de un programa informático, y los ojos críticos sólo auditan específicamente el tratamiento que se hace de la información, reduciendo, o inclusive anulando, la posibilidad de inclusión de funciones maliciosas intencionales o *backdoors* en el código de un programa informático.

Además de descartar la inclusión de funciones maliciosas intencionales, la apertura del código fuente contribuye a minimizar la mencionada “ventana de vulnerabilidad” de un ataque: si se descubre una vulnerabilidad en el programa, puede ser actualizado y solucionado por cualquier individuo capacitado para hacerlo, o inclusive de forma colaborativa, sin depender de los tiempos de ninguna empresa

privada. De esta manera, la utilización de programas informáticos libres y de código abierto se constituye en una estrategia que reduce significativamente los vectores de ataque de un sistema informático, derivando en implementaciones seguras, resilientes y actualizadas (Watercutter, 2013).

El incremento sustancial en términos de seguridad informática que representa la utilización de programas de código abierto no solo está ampliamente respaldado en términos teóricos por profesionales y académicos, sino que inclusive se traduce en implementaciones privadas y públicas en muchos aparatos administrativos gubernamentales en todo el mundo. El Departamento de Defensa de los Estados Unidos pondera explícitamente las capacidades que otorga la apertura del código fuente de un programa para los intereses de los Estados, sosteniendo que, para lograr su misión de Defensa, es prioritario desarrollar y actualizar sus capacidades basadas en programas informáticos de código abierto, los cuales afirman que pueden proveer ventajas significativas (Department of Defense, 2009, p. 1). El Departamento argumenta que la disponibilidad pública del código fuente no solo contribuye con la seguridad y la confiabilidad de un programa informático, sino que permite la modificación del mismo para adaptarse a las situaciones cambiantes propias de la Defensa de los Estados (Department of Defense, 2009, p. 4).

Evidenciada la ventaja estratégica en términos de seguridad informática que proveen los programas libres de código abierto, es relevante analizar por qué no son tan conocidos, y por qué son aisladas las grandes implementaciones gubernamentales de estos sistemas en la actualidad. La causa que se puede señalar como principal remite a una cuestión puramente económica, y reside en los intereses empresariales que se sustentan en los programas informáticos privativos. Los grandes conglomerados de tecnología tienen la capacidad de acordar con los fabricantes de dispositivos físicos para imponer sus programas informáticos privativos, los cuales por lo general no son modificados por los usuarios finales. Las implementaciones informáticas de programas libres de código abierto, por el contrario, no están representadas por empresas tan grandes y poderosas, por lo que su implementación en, por ejemplo, infraestructuras gubernamentales, requiere de políticas específicas que promuevan su utilización.

Una de las preguntas principales es, entonces, si existe la posibilidad de generar transiciones ordenadas desde las estructuras administrativas gubernamentales actuales, mayoritariamente basadas en sistemas informáticos privativos, hacia sistemas de código

abierto que otorguen a los Estados mayor control sobre la seguridad de sus implementaciones informáticas. Hoepman y Jacobs (2005, p. 13-14) sostienen que, si bien abrir el código fuente de sistemas ya existentes podría, en un principio, visibilizar públicamente las vulnerabilidades que puedan existir, en el largo plazo se traduciría en beneficios de seguridad. De este modo, sostienen que la apertura de los sistemas derivaría en una evaluación mayor y una búsqueda proactiva de errores, lo cual terminaría aumentando la seguridad del sistema, y permitiría inclusive el desarrollo de herramientas mucho más sofisticadas. Además, afirman que las soluciones de seguridad estarían disponibles rápidamente, por lo que el período de mayor exposición es corto.

Uno de los baluartes del *Movimiento por el Software Libre* en la promoción de las implementaciones informáticas que hagan uso de programas libres de código abierto, es el sistema operativo *GNU/Linux*, el cual se alza como alternativa ante las plataformas más utilizadas, siendo las principales *Windows* de Microsoft y *macOS* de Apple. *GNU/Linux* prueba ser un sistema operativo eficiente y seguro gracias a la apertura del código fuente de todos sus programas, y esto se expresa en que, por ejemplo, sea utilizado en las 500 mejores supercomputadoras del mundo (Vaughan-Nichols, 2017).

Desde la perspectiva de los Estados, como se sostuvo, existen casos que demuestran cómo la implementación de soluciones informáticas con programas libres de código abierto y del sistema operativo GNU/Linux se puede traducir en un aumento en la seguridad informática, minimizando los riesgos al reducir los vectores de ataque mediante los cuales un atacante puede vulnerar los sistemas de los organismos públicos. En 2013, por ejemplo, la Gendarmería Nacional de Francia instaló *GNU/Linux* en un total de 37.000 computadoras que se encontraban usando el sistema operativo *Windows* (Finley, 2013). El Gobierno alemán, por su parte, hace uso de tecnologías de nube de código abierto para almacenar y transmitir datos privados, argumentando que son mucho más seguras que las tecnologías ofrecidas por los programas privativos (Thornett, 2018). Y para desestimar cualquier tipo de dudas de la efectividad de las implementaciones libres de código abierto en sistemas de gran escala, un estudio del 2018 demuestra que el 78 por ciento de los organismos estatales de Brasil utilizan programas informáticos de código abierto (Mari, 2018).

El evidente beneficio que genera la adopción de este tipo de programas libres, y de sistemas operativos abiertos, ha dado lugar a la creación del Observatorio y Repositorio de Código Abierto, un proyecto de la Comisión Europea para estudiar y

promover el uso de soluciones de código abierto en los servicios públicos de la Unión Europea. Estos ejemplos institucionales demuestran que, independientemente de las asperezas que puedan generar los intereses empresariales de los grandes conglomerados de tecnología, los Estados están tendiendo a mudar sus sistemas a este tipo de programas abiertos, para aumentar la seguridad de sus recursos virtuales. Sin embargo, aún queda un largo trayecto hasta la implementación mayoritaria de este tipo de tecnologías, por lo que es necesaria su difusión, ya que es una variable técnica que, en combinación con la capacitación proactiva de los usuarios, tiene la potencialidad de incrementar significativamente los niveles de Defensa estatales en el ciberespacio (Hoepman y Jacobs, 2005, p. 13-14).

b) Capacitación proactiva

Como se sostuvo previamente, no existen soluciones ubicuas para que los Estados puedan obtener una defensa férrea de todas las amenazas a las que se enfrenta en el ciberespacio, pero sí existen una serie de medidas que pueden aplicar para mejorar radicalmente su posición. La primera de las variables desarrolladas implica la implementación de programas informáticos libres de código abierto. Si bien se encuentra probada la capacidad que este tipo de programas tienen para reducir los vectores de ataque, es necesario resaltar que ninguna implementación técnica por sí sola puede representar un aumento de la seguridad informática, si no es acompañada por una capacitación constante y proactiva de los usuarios de los programas informáticos.

Por más que un sistema informático se instale con las mayores precauciones en términos técnicos, si un empleado público en sus funciones, por ejemplo, envía de forma descuidada información confidencial a un servidor que no corresponde, cualquier estrategia de seguridad informática se nulifica, ya que el usuario es la vulnerabilidad mayor dentro del sistema. Si bien hay muchas posturas que sostienen que para evitar este tipo de casos, es mejor restringir la capacidad de acción del usuario a las funciones necesarias para desempeñar su trabajo, en términos prácticos estos abordajes representan dos impedimentos: en primer lugar, el trabajo técnico necesario para contener al usuario termina siendo mucho más exhaustivo que su capacitación; y en segundo lugar, cualquier mínima funcionalidad adicional que se le otorgue al usuario se convertiría en una vulnerabilidad, al desconocer éste sus implicancias y alcances.

El caso de *spear phishing* del Comité Nacional Demócrata estadounidense, que derivó en las filtraciones masivas de correos electrónicos de la candidata Hillary Clinton en 2016, es útil para ilustrar esta situación. Si bien existieron una serie de ataques informáticos previos que allanaron el terreno y recopilaron la inteligencia para que se pudiera realizar, es altamente probable que la capacitación proactiva de los usuarios de Comité hubiese resultado en que éstos observaran más detenidamente el vínculo de la página web a la que estaban accediendo, y hubiesen reconocido que estaban conectándose con un servicio de correo electrónico tergiversado. Sin embargo, no lo hicieron, y se filtraron más de 30.000 correos electrónicos privados que comprometieron la imagen pública de la candidata demócrata.

Diversos análisis han señalado que dentro de la denominada "cadena de seguridad informática", el eslabón potencialmente más débil es el usuario humano (Miller, 2018). Corey Nachreiner, especialista en seguridad informática y Director de Tecnología de la empresa estadounidense de seguridad de redes *WatchGuard Technologies*, enfatiza este factor, y sostiene que la capacitación y la concientización del usuario final debe ser la parte fundamental de las estrategias de seguridad. Advierte que, si esta capacitación se logra convertir en una prioridad, los usuarios adquirirían herramientas para reconocer y evitar, por ejemplo, correos electrónicos maliciosos; y también asevera que la carencia de este tipo de capacitación, se puede traducir en que un simple error de usuario pueda burlar todo el programa y la infraestructura técnica de seguridad informática previamente construida (Levy, 2016).

En la escala estatal, este factor se vuelve aún más relevante, ya que un usuario capacitado es un funcionario que hace un tratamiento prudente de información estratégica para un Estado. La falta de capacitaciones de este tipo en usuarios gubernamentales se evidencia en diversos casos, y cuanto más importante sea la información a la que un usuario accede, más peligrosa es la carencia de capacitación en medidas de seguridad informática. En el 2008, por ejemplo, un soldado estadunidense encontró un dispositivo de almacenamiento USB (*pendrive*) tirado fuera de una base del Departamento de Defensa estadounidense en Medio Oriente, y decidió conectarlo a una computadora dentro de la red del Comando Central. El problema fue que esta unidad USB había sido depositada intencionalmente por agencias de inteligencia extranjeras en la zona donde fue encontrada, en una estrategia conocida como "*caída de dulces*". Esta acción por parte del soldado se tradujo en la introducción de un *gusano informático* llamado "*agent.btz*" en los sistemas del Departamento de Defensa, que escaneó las

computadoras de la red robando datos, creando puertas traseras y comprometiendo los servidores del Comando Central, haciendo que el pentágono pasara más de catorce meses tratando de limpiar todos los rastros del ataque informático (Prince, 2010).

Tanto el ejemplo del *spear phishing* del Comité Nacional Demócrata estadounidense, como el ataque informático de *agent.btz* ilustran las potenciales vulnerabilidades que representa la falta de capacitación de los usuarios de sistemas informáticos públicos. Es por esta razón que muchos expertos en tecnología arguyen que, si una red tiene algún tipo de información sensible, todos los usuarios deben estar regularmente certificados en aspectos básicos de seguridad informática. Singer y Friedman (2014, p. 176) llegan a sugerir que, al igual que existen anuncios constantes sobre el uso de profilácticos para prevenir la propagación de enfermedades de transmisión sexual, o recordatorios en los lugares de trabajo sobre lavarse las manos para evitar la propagación de gripes, deben crearse políticas que fomenten buenas prácticas en los protocolos básicos de seguridad informática para todos los usuarios finales. Estas consideraciones han dado lugar a concepciones tales como las de "*ciber higiene*", las cuales sugieren prácticas y pasos que los usuarios de computadoras y otros dispositivos deben tomar para preservar el estado de los sistemas informáticos, y prevenir la propagación de amenazas y *malwares* (Aldorisio, 2018).

Si bien se constituiría en una afirmación contrafáctica, por lo que metodológicamente no es válida, se podría afirmar que, de haberse aplicado esta combinación de estrategias, muchos de los ataques informáticos previamente mencionados, y la gran mayoría de los APT que se abordarán en el siguiente capítulo, no hubiesen tenido lugar, o sus consecuencias hubiesen sido sustancialmente menores. ¿En qué se sustenta esta afirmación? Muchos de los casos tuvieron lugar gracias a dos factores: el aprovechamiento de vulnerabilidades en programas privativos, o la negligencia de usuarios sin conocimientos en seguridad informática (cuando no fue por una combinación de ambas).

Si bien las amenazas con las cuales un Estado se puede enfrentar a la hora de ingresar en el ciberespacio son múltiples y adquieren diversas morfologías, la utilización de instrumentos técnicos libres, auditables, seguros y robustos, combinada con una capacitación constante de los usuarios finales en buenas prácticas para mantener la seguridad de los sistemas informáticos, se constituye como una estrategia que elimina vulnerabilidades de base, y es una postura mucho más estable que los Estados pueden adoptar para posicionarse en el ciberespacio.

IV. Conclusiones parciales

El ciberespacio introduce una interesante dinámica a las relaciones internacionales. En una especie de retroalimentación, los Estados hacen uso del ciberespacio como un terreno en el cual pueden desplegar estrategias para perseguir sus intereses, pero el ciberespacio y los sucesos en él acontecidos influyen en la forma en que los Estados llevan a cabo sus políticas y determinan sus prioridades.

Las capacidades de acción que el ciberespacio otorgará a los Estados evidencian en el día a día, pero se puede afirmar que es un proceso que recién está comenzando. Un caso interesante para demostrar cómo se pueden configurar las nuevas estrategias intergubernamentales en el ciberespacio lo demostraron, una vez más, las filtraciones de Snowden. La Agencia Nacional de Inteligencia de los Estados Unidos no solo había desarrollado programas para espiar comunicaciones a nivel global, sino que cooperaba en esta tarea con otros Estados, específicamente con el grupo "*Five Eyes"*. Este grupo, cuyo nombre en español significa "*Cinco Ojos*", es una alianza de inteligencia que integran Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda, y sus lazos datan desde fines de la Segunda Guerra Mundial. Este grupo de países hicieron uso de herramientas informáticas de espionaje, con un alto nivel de complejidad y alcance, para perseguir objetivos geopolíticos.

Dentro de la lista de países espiados por el grupo *Five Eyes*, se encontraban algunos que no causaron sorpresa, como China, Cuba, Corea del Norte, Rusia, Irán, Pakistán, y Afganistán. Sin embargo, también se encontraron pruebas de espionaje en diferentes organismos que sí llamaron mucho más la atención. El Ministerio de Energía de Brasil, la embajada francesa en Washington, la embajada alemana en Ruanda, el Consejo de la Unión Europea, el Organismo Internacional de Energía Atómica y UNICEF, son algunas de las curiosas e inconexas agencias que se encontraron siendo espiadas por los programas de colaboración conjunta del grupo *Five Eyes* (Poitras, 2013).

Como se resaltó, estas capacidades de espionaje y recopilación de inteligencia se constituyen como una de las múltiples estrategias ofensivas posibilitadas por Internet, las cuales tienen la potencialidad de dar inicio a enfrentamientos mucho más serios y con mayores consecuencias en el ciberespacio. En el caso de llegar al extremo teórico de una *ciberguerra*, no existen tratados internacionales que la puedan llegar a regular, y

los tratados que rigen los enfrentamientos en el mundo material aún no se han actualizado para contemplar este tipo de casos.

De este modo, los Estados quedan librados a su capacidad de acción, en un estado de anarquía donde se evidencia una estructura realista de puja de poderes, en la cual se reconfiguran las capacidades ofensivas y defensivas de cada país. Como se sugirió, el ciberespacio y la virtualidad añaden complejidad, pero también existen medidas que la disciplina de la seguridad informática provee para minimizar las consecuencias de los ataques informáticos. Una combinación de programas libres de código abierto, y de políticas de capacitación proactiva, independientemente de las capacidades ofensivas de un Estado, lo posicionarían de manera más robusta en el ciberespacio. Sin embargo, hasta que se apliquen este tipo de medidas, o medidas similares que tiendan a mejorar la seguridad informática de los Estados, seguirán existiendo potencialidades cada vez mayores de ataques informáticos.

Capítulo III. Amenazas Persistentes Avanzadas: Estudios de caso de Estados Unidos, China y Rusia

I. Introducción

Si bien en los capítulos previos se analizaron las implicancias del ciberespacio en el sistema internacional, y el rol fundamental que adquiere la seguridad informática en la Defensa de los Estados, la cualidad interdisciplinaria de este caso de estudio amerita un análisis empírico que evidencie la formulación teórica previamente expuesta. El ciberespacio se alza como un terreno en el cual se realizan múltiples ataques informáticos, entre actores estatales y no estatales, y con diferentes intereses. Frente a una cantidad tan grande de ataques, con variados objetivos, es imperioso aplicar algún criterio que sea útil para demostrar la influencia que puede llegar a tener el ciberespacio y la seguridad informática, específicamente en las relaciones interestatales.

Las potencias se destacan en el sistema internacional por su capacidad de acción en términos económicos, geopolíticos y militares, y es éste el caso también para las capacidades en el ciberespacio. Inclusive Joseph Nye (2010, p. 19), en el otro extremo del espectro teórico, admite que, si bien el ciberespacio introduce nuevas e innovadoras formas de difusión de poder, los Estados más importantes en el sistema internacional son los que conservan la capacidad de influir de mayor manera el escenario internacional.

El elemento principal que condiciona de manera estructural cualquier tipo de análisis de relaciones internacionales en el ciberespacio es la *atribución*. Como se argumentó previamente, existe un nivel de complejidad mayor para determinar la procedencia y la identidad de los ataques informáticos en relación a los ataques acontecidos en el mundo material, motivo por el cual la atribución de las agresiones en el ciberespacio es una tarea muy delicada. Sin embargo, existen diversos parámetros que pueden servir de indicadores para determinar la participación de un actor en un ataque informático. Es por este motivo que se analizarán a continuación diversos ataques informáticos que poseen evidencia suficiente como para señalar a los gobiernos de las principales potencias del sistema internacional como orquestadores de las agresiones, específicamente casos sospechados de originarse en Estados Unidos, China y Rusia, las tres potencias con mayores capacidades políticas, económicas y militares en el sistema internacional del siglo XXI.

El arsenal de ataques con los cuales un actor con suficientes recursos cuenta para realizar estrategias ofensivas en el ciberespacio es, como se describió en los capítulos anteriores, extremadamente amplio. Es por esta razón que se utilizarán como elemento de análisis un tipo específico de ataque, considerado uno de los más elaborados, denominadas Amenazas Persistentes Avanzadas (APT en la mayoría de la bibliografía, por sus siglas en inglés de Advanced Persistent Threat). Como se describió previamente, este tipo de ataques son de alta complejidad, ya que se caracterizan por ser extremadamente discriminatorios en sus objetivos, y por usar diversos métodos de ataque (DoS, *phishing*, *malwares*), para burlar las defensas de un sistema informático. La cualidad que distingue a los APT es que, como su nombre indica, son persistentes en su accionar, y modifican sus estrategias en el tiempo para lograr su cometido (Symantec, 2011, p. 1).

Anteriormente se analizaron casos que demostraron el alcance que pueden tener las capacidades de acción estatales en el ciberespacio, ya que son los actores que cuentan con más recursos económicos y humanos para realizar desarrollos, siendo una de las operaciones más destacables la estructura de vigilancia masiva internacional montada por la Agencia de Seguridad Nacional de los Estados Unidos, evidenciada en las filtraciones masivas realizadas por Snowden. Sin embargo, mientras esta operación realizó una recopilación generalizada e indiscriminada de datos e inteligencia, el factor que distingue los casos que se analizarán a continuación es que se constituyen como Amenazas Persistentes Avanzadas realizadas o promovidas por las potencias del sistema internacional, contra objetivos Estatales, y siempre enmarcadas en estrategias económicas, geopolíticas o militares.

De esta manera, se procederá a realizar en primer lugar una conceptualización introductoria del abordaje que cada una de las potencias posee del ciberespacio, para luego analizar casos empíricos de Amenazas Persistentes Avanzadas que evidenciarán las formulaciones teóricas de los capítulos previos, y la capacidad de afectar el equilibrio de poder en el sistema internacional a través de ataques emprendidos en el ciberespacio.

II. Estados Unidos

Los Estados Unidos no solo tienen el mérito de haber sido el país que creó y desarrolló gran parte de la infraestructura que permitió llegar al Internet actual, sino que es uno de los países más activos en el desarrollo de programas informáticos e

innovaciones tecnológicas. Si bien el desarrollo de sus capacidades informáticas se puede atribuir en gran medida al sector privado, con empresas de renombre internacional como *Apple, Microsoft y Amazon,* es innegable el hecho de que el sector público tiene a su disposición un inmenso capital humano con posibilidad de desarrollo de aplicaciones informáticas que incrementan la capacidad de acción de los Estados Unidos en el ciberespacio, volviéndolo uno de los actores más relevantes en este análisis.

El gobierno de los Estados Unidos es consciente de estas capacidades, pero también reconocen las potencialidades que otorga a otros actores, por lo que posiciona a la seguridad informática como una prioridad en la agenda de Defensa. En la "Estrategia de Seguridad Nacional" estadounidense del 2010, la administración demócrata de Obama sostuvo a las amenazas de seguridad informática como "uno de los desafíos más serios de seguridad nacional, seguridad pública y economía que enfrentamos como nación" (Gobierno de Estados Unidos, 2010, p. 27). Esta postura también se replicó en la edición del año 2017 de la Estrategia de Seguridad Nacional, cuando la administración republicana de Trump enfatizó el peligro de las "actividades cibernéticas maliciosas" para las infraestructuras comerciales, gubernamentales y militares (Gobierno de Estados Unidos, 2017, p. 13).

La mencionada relevancia que adquiere el ciberespacio y la seguridad informática para el gobierno estadounidense no solo tiene su impronta en sus documentos más generales de Defensa, sino que también se evidencia en el énfasis con el cual sus agencias abordan la temática: el Departamento de Seguridad Nacional, encargado de la seguridad interna, posee un documento titulado "Estrategia Nacional para Asegurar el Ciberespacio"; y el Departamento de Defensa (mayormente conocido como el *pentágono*), encargado de las acciones militares, posee también su documento llamado "Estrategia para Operar en el Ciberespacio". Si bien las estrategias orquestadas por el Departamento de Seguridad Nacional en relación al ciberespacio remiten a una cuestión de control interno del crimen, la concepción del Departamento de Defensa es la más relevante para este análisis, ya que es el encargado de coordinar las agencias gubernamentales relacionadas con la defensa y las fuerzas armadas, y su postura es la que explica las acciones que los Estados Unidos emprenden en el ciberespacio.

En el documento "Estrategia para Operar en el Ciberespacio", el Departamento de Defensa plantea cinco estrategias que resumen sus perspectivas del ciberespacio. La primera estrategia plantea tratar al ciberespacio como un "dominio operacional", lo que

permite al Departamento “organizar, entrenar y provisionar para el ciberespacio como lo hacemos en el aire, la tierra, el mar y el espacio para respaldar los intereses de seguridad nacional” (Departamento de Defensa de los Estados Unidos, 2011, p. 5). Esta estrategia es la principal, y revela una visión militarista del ciberespacio, que es abonada por el resto de las estrategias detalladas en el documento: desarrollar nuevos sistemas de defensa para defender su infraestructura; asociarse con otras agencias y con el sector privado; construir relaciones con socios internacionales; y desarrollar nuevos talentos para impulsar nuevas innovaciones militares en el ciberespacio (Singer y Friedman, 2014, p. 134).

Para cumplir con estos objetivos, el Departamento de Defensa cuenta con dos agencias principales bajo su órbita: la *Agencia Nacional de Inteligencia* y el *Cibercomando de los Estados Unidos* (Nakashima, 2016). La Agencia Nacional de Inteligencia es la responsable de monitorear, recopilar y procesar información con propósitos de inteligencia y contraespionaje extranjero. Esta agencia adquirió mayor relevancia a partir de los ataques terroristas de septiembre del 2001, y no solo la capacidad, sino también el permiso expreso del gobierno estadounidense para recopilar “datos sospechosos de espionaje o terrorismo” en cualquier parte del mundo (Risen y Lichtblau, 2005).

El alcance en las capacidades de la Agencia Nacional de Seguridad se evidenció en la enorme filtración de datos que realizó Snowden, un contratista con permisos de acceso que le permitieron llegar a una gran cantidad de información secreta. El informático reveló que, por ejemplo, un solo programa, llamado *PRISM*, tenía la capacidad de recopilar comunicaciones de las principales compañías de Internet en todo el mundo, lo que le permitía a la Agencia supervisar las comunicaciones en vivo, la información almacenada de correos electrónicos, videos y chat de voz, fotos, chats de voz sobre IP (como *Skype*), transferencias de archivos y detalles de redes sociales (Whittaker, 2013).

Esta Agencia con enormes capacidades se encuentra respaldada por el *Cibercomando de los Estados Unidos*, que se constituye como la segunda entidad que el Departamento de Defensa tiene para operar en el ciberespacio. Creado inicialmente bajo la órbita de la Agencia Nacional de Seguridad, la importancia de esta división no hizo más que aumentar, y llegó a su punto máximo en el 2018, cuando fue elevado por la administración de Trump a “comando de combate unificado” (The White House, 2017, traducción propia). Este rango dentro de las fuerzas armadas estadounidenses no es

menor, ya que son comandos persistentes que se encargan de coordinar estrategias militares en períodos de guerra y de paz, lo que plasma una concepción claramente militarista del ciberespacio. El Cibercomando es la entidad que se encarga específicamente de los enfrentamientos en el ciberespacio y de las *ciberguerras*, y tiene tres tipos de fuerzas: *fuerzas de ciberprotección* para defender las redes de computadoras militares, *fuerzas de misión de combate*, para apoyar a las tropas del campo en guerras en el mundo material, y *fuerzas de misiones nacionales* para proteger la infraestructura crítica dentro de las fronteras estadounidenses (Singer y Friedman, 2014, p. 134).

La postura del Departamento de Defensa estadounidense es la que explica mayoritariamente el accionar estadounidense en el ciberespacio, y específicamente en las acciones que emprende en su relación con otros Estados. Entendiendo al ciberespacio como un "dominio operacional" más en el cual las fuerzas armadas estadounidenses tienen la capacidad de desempeñarse, se añade una nueva dimensión a los escenarios militares. Esta postura agresiva y belicista en el ciberespacio enmarca no solo los mencionados ejemplos de espionaje internacional, sino que encauza los casos de Amenazas Persistentes Avanzadas realizadas por los Estados Unidos, convirtiéndolo en una de las mayores potencias ofensivas en el ciberespacio.

1. Stuxnet: sistemas de control industrial e infraestructura crítica

Si bien se han hecho breves referencias a *Stuxnet* a lo largo del trabajo de investigación, sus ramificaciones y complejidad convierten a este ataque informático en una de las Amenazas Persistentes Avanzadas más sofisticadas conocidas hasta la actualidad, y requiere un análisis de sus capacidades y las consecuencias que un ataque de estas características produjeron en el escenario internacional. Como sostiene Langner, especialista en seguridad informática que estudió el ataque en profundidad, *Stuxnet* aún sigue desconcertando a estrategas militares, expertos en seguridad, tomadores de decisiones políticas y hasta al público en general; y considera que sus capacidades ofensivas lo convierten en un "claro giro en la historia de la seguridad informática, así como también de la historia militar" (Langner, 2013, p. 4).

El concepto de un ataque en el ciberespacio conserva algunas características de los ataques en el mundo material. Para realizar un ataque nuclear interestatal o intercontinental, por ejemplo, no solo basta con poder fabricar una bomba nuclear, sino que también es necesario desarrollar la capacidad misilística para transportar de manera

efectiva el explosivo hasta el objetivo. De manera similar, salvando las particularidades que la virtualidad introduce, un ataque llevado a cabo en el ciberespacio mantiene una estructura análoga: se compone por su *carga útil*, es decir el ataque *per se*, y también por diversos mecanismos que le permiten llegar hasta el objetivo. *Stuxnet* puede ser considerado como un "tipo ideal" weberiano de Amenaza Persistente Avanzada, ya que alcanza un nivel de sofisticación sin precedentes, haciendo un uso ecléctico de diversas estrategias no solo para realizar su cometido, sino también para transportarse y propagarse a computadoras en todo el mundo.

En primer lugar, se constituye como uno de los *gusanos informáticos* más infecciosos del mundo, ya que hace uso de múltiples vulnerabilidades desconocidas (*zero days*, o *días cero)* en el sistema operativo Windows, exclusivamente para infectar y expandirse por redes de computadoras, con una capacidad y una escala de propagación sin precedentes hasta el momento de su descubrimiento (Fruhlinger, 2017). Esta característica no es menor, ya que las vulnerabilidades día cero se llegan a subastar por cientos de miles de dólares en la *dark web*, y el hecho de que un ataque informático posea más de una unidad de este tipo de vulnerabilidades, es un indicador no solo de los recursos con los que cuenta el orquestador de *Stuxnet*, sino también de su obstinación para lograr su objetivo (Langner, 2013, p. 4). Las estadísticas ilustran esta capacidad superlativa de propagación, ya que apenas un mes después de su descubrimiento y publicación en julio de 2010, existían más de 100.000 infecciones reportadas de *Stuxnet*, en más de 115 países diferentes.

En segundo lugar, una vez que logra colarse en un sistema informático, *Stuxnet* se configura como un *malware* altamente disruptivo y peligroso, pero sólo realiza las acciones maliciosas si se conjugan una serie de variables muy específicas. Este es uno de los elementos que más llamó la atención de los especialistas en seguridad informática que diseccionaron y estudiaron el accionar de *Stuxnet*: estaba diseñado para infectar una computadora y mantenerse inactivo, a no ser que a ésta se encontrara conectado un modelo específico de controlador lógico programable de la marca alemana *Siemens* (Kushner, 2013). Cuando comenzaron a indagar, los especialistas descubrieron la trama de una de las operaciones en el ciberespacio más elaboradas hasta el momento, ya que los controladores *Siemens* contra los que apuntaba *Stuxnet* son especialmente utilizados para controlar la velocidad de rotación de centrifugadoras de uranio, equipamientos utilizados para producir uranio enriquecido, componente primordial en la generación de energía nuclear.

Sin embargo, la discriminación de *Stuxnet* para realizar su ataque no se detenía en la detección de este tipo de equipamiento industrial, sino que era aún más minuciosa: buscaba una formación de centrifugadoras organizada en seis grupos, cada uno compuesto por 164 máquinas. Este nivel de especificidad fue el factor que más llamó la atención a los expertos en seguridad informática que descubrieron *Stuxnet*, y fue lo que permitió determinar rápidamente el objetivo del ataque, ya que esta formación de centrifugadoras era la presente en la planta de enriquecimiento de uranio de Natanz, en Irán (Albright et al., 2010, p. 1).

De esta manera, *Stuxnet* se configuró como una Amenaza Persistente Avanzada que infectó miles de computadoras en todo el mundo, con el objetivo de alcanzar las computadoras que controlaban los sistemas de control industrial de la planta nuclear de Irán. Una vez que detectaba estas variables, *Stuxnet* desplegaba su ataque: tenía la capacidad de alterar la programación de los controladores, variando la velocidad y el tiempo de rotación de las centrifugadoras. Esto se traducía en que los rotores giraran más lento que las velocidades necesarias para el proceso de refinamiento de uranio; o también en que giraran más rápido y por períodos de tiempo mayores, resultando en un desgaste y un daño de los equipos. Estas alteraciones se tradujeron en la destrucción efectiva de las centrifugadoras: entre los años 2009 y 2010, resultaron dañados, o totalmente destruidos hasta 1.000 equipos que confirmaban la planta de enriquecimiento de uranio de Natanz (Albright et al., 2010, p. 1).

Por último, para coronar este elaborado ataque, *Stuxnet* toma el control de a las computadoras que están conectadas a los controladores *Siemens*, y muestra a los operadores de la misma que el proceso industrial se está ejecutando de manera correcta. De esta manera, era imposible para los expertos iraníes diagnosticar el motivo por el cual su equipamiento no producía eficientemente, o directamente se destruía, ya que las computadoras que controlaban el sistema no mostraban errores o anomalías (Fruhlinger, 2017). Esta breve descripción de las capacidades ofensivas altamente dañinas de *Stuxnet*, que se constituyó en un ataque informático integral y persistente al proceso industrial de refinamiento de uranio en instalaciones iraníes, lleva a la pregunta de quién es el actor con la capacidad y la intención de crear un ataque informático de esta envergadura, que, debido a sus capacidades concretas de causar daño físico en el mundo material, lo convierten en un arma informática.

La respuesta a este interrogante se encuentra enmarcada en el mencionado dilema de la atribución en el ciberespacio, motivo por el cual se complejiza la

determinación fehaciente del atacante. Sin embargo, hay dos elementos clave para lograr reducir los posibles perpetradores de una APT tan compleja: el primero se remite a las capacidades de acción, ya que no son muchos los actores capaces de emprender un ataque informático de estas características; y el segundo elemento refiere a los beneficios obtenidos a partir de la acción de este ataque. La extensión y la sofisticación de *Stuxnet* no solo elimina a los *crackers* individuales y a los movimientos *hacktivistas* de los posibles atacantes, dejando como única alternativa a un Estado, sino que también descarta a los Estados que no cuentan con los recursos económicos y humanos para realizarlo.

Esta reducción de los posibles agresores, sumada a algunos indicios que los especialistas informáticos encontraron en el código, lleva a los expertos a sugerir que *Stuxnet* fue desarrollado por un trabajo conjunto entre Estados Unidos e Israel, ya que fueron éstos los actores que mayor provecho geopolítico obtuvieron de las consecuencias del ataque. Aunque no fue admitido por ninguno de los dos Estados, existe un consenso generalizado de que esta Amenaza Persistente Avanzada fue efectivamente elaborada por el trabajo conjunto de ambos países con el objetivo de frenar el desarrollo de las capacidades nucleares en Irán (Nakashima y Warrick, 2012).

Esta APT se enmarca en un conflicto geopolítico extenso entre Estados Unidos e Irán, el cual se constituye en un caso de estudio específico de las relaciones internacionales. En el momento de redacción de este trabajo de investigación, se encuentra vigente un acuerdo internacional firmado en el 2015 entre Irán, el P5+1 (los miembros del Consejo de Seguridad de la ONU más Alemania), y la Unión Europea, llamado *Plan de Acción Conjunto y Completo*, más conocido por sus siglas en inglés *JCPOA*. En este acuerdo, Irán se compromete a minimizar las capacidades de su programa nuclear y a aceptar rigurosas inspecciones rutinarias de la OIEA, a cambio del levantamiento de sanciones comerciales, previamente impuestas por el resto de los países involucrados en el acuerdo. Este acuerdo se constituyó como un hito de cooperación y consenso internacional en el siglo XXI, pero antes de su negociación, la relación histórica entre la República Islámica de Irán y occidente no se caracterizó por poseer tintes particularmente benévolos.

A partir de la revolución islámica de 1979, en la cual se estableció la República Islámica de Irán bajo el mando del Ayatollah Khomeini, Irán adoptó una postura internacional de un marcado antisemitismo, y profundamente anti-israelí y anti-occidental. Desde la emblemática toma de rehenes en Teherán de 1979, Estados Unidos

tuvo un cambio radical de política externa respecto de quien había sido uno de sus principales socios en medio oriente: le impusieron a Irán sanciones comerciales y financieras, e inclusive prohibieron la inversión de capitales estadounidenses en el país. Los atentados del 11 de septiembre del 2001 no hicieron más que incrementar la conflictividad, ya que Irán fue incluido por el presidente Bush en el "Eje del Mal", y fue acusado explícitamente de financiar al terrorismo internacional.

El programa nuclear iraní se presenta como una paradoja de las estrategias de política exterior estadounidenses en medio oriente: el puntapié que permitió el desarrollo nuclear en Irán fue un reactor nuclear obsequiado en la década de 1960 por los Estados Unidos a la administración del Shah de Irán, un gobierno caracterizado por una relación amigable con occidente. Irónicamente, fue el Estado norteamericano quien permitió de manera involuntaria el desarrollo de las capacidades nucleares de uno de los gobiernos islámicos más radicalizados en Medio Oriente, que comenzó a regir Irán desde 1979. Cuando el plan nuclear iraní se comenzó a percibir como una amenaza, las posiciones estadounidenses hacia Irán comenzaron a endurecerse, y la secretaria de Estado de Bush, Condolezza Rice, llegó a emitir la advertencia en el 2008 de que los Estados Unidos defenderían "vigorosamente a sus amigos y sus intereses" si Irán no cambiaba su postura respecto al desarrollo de un programa nuclear con capacidades ofensivas (Rice, 2008).

De esta manera, y enmarcado en el contexto la *guerra contra el terrorismo* de la administración estadounidense de George W. Bush, se comenzó en 2005 con la implementación de estrategias que pudieran limitar los desarrollos nucleares de Irán, destacándose dentro de éstas la Amenaza Persistente Avanzada que posteriormente se conoció como *Stuxnet*. Un hecho significativo es que esta APT fue descubierta en 2010, por lo que fue también utilizada por la administración de Obama, la cual detrás de una política exterior aparentemente más dialoguista, evidenciaba elementos que perpetuaban estas estrategias intervencionistas en Medio Oriente. La capacidad de acción de *Stuxnet* en el momento de su descubrimiento no tenía parangón con otro ataque informático, e inclusive fue catalogado por los expertos en seguridad informática que lo desentrañaron como "la pieza de código más compleja que hemos visto, en una liga completamente diferente respecto a lo que habíamos visto antes" (Fruhlinger, 2017).

Stuxnet es relevante por diversos motivos. Es uno de los ataques informáticos más tangibles llevados a cabo por una potencia que tuvieron consecuencias en el mundo material, y que efectivamente convirtieron un ataque informático en un arma. La

capacidad de acción de *Stuxnet* llamó la atención de diversos académicos, que inclusive llegaron a describirlo como un ataque que cambió las reglas de juego en el ciberespacio, y que da lugar a una carrera armamentista digital (Singer y Friedman, 2014, p. 117). Mediante la utilización de *Stuxnet*, los gobiernos de Estados Unidos e Israel lograron efectivamente ralentizar el programa nuclear iraní, alterando el balance de poder en medio oriente y en el sistema internacional. Así, esta APT abre una gran incógnita respecto a las capacidades que introducen las herramientas informáticas en manos de actores con suficientes recursos como para desarrollar ataques persistentes y avanzados de estas características.

2. Flame, una herramienta de espionaje sin precedentes

Flame ("*llama*" en inglés), también denominado como *Flamer* y *sKyWIper*, es el nombre por el cual se conoce a un ataque informático descubierto en 2012 por una firma de seguridad informática rusa muy reconocida en el mercado, llamada *Kaspersky.* Este ataque también se destaca por su gran capacidad de acción, y supone ser la principal herramienta de una Amenaza Persistente Avanzada realizada sobre diferentes países de medio oriente, con el objetivo de recopilar información e inteligencia.

Flame se aprovecha, al igual que *Stuxnet*, de diversas vulnerabilidades en el sistema operativo *Windows*, las cuales le permiten propagarse de manera acelerada en muchos dispositivos, constituyéndose por definición en un *gusano informático*. Los especialistas rusos que se encargaron de investigar su funcionamiento dedujeron que *Flame* había estado operativo desde 2010, y una vez dentro de las computadoras infectadas poseía funcionalidades de *rootkit* y de *spyware*, ya que puede utilizar los micrófonos conectados a las computadoras para grabar audio, tiene la capacidad de sacar capturas de pantalla, grabar conversaciones de *Skype*, guardar todo lo que el teclado escriba, e inclusive recopilar información del tráfico dentro de la red de la cual forma parte. Esta capacidad de espionaje sorprendió mucho a los expertos, sobre todo cuando se observa que el *malware*, una vez que obtiene toda la información, la envía haciendo uso de la conexión a Internet de la computadora a servidores que tiene a su disposición, esparcidos en todo el mundo, que inclusive pueden darle nuevas instrucciones de acción (Gostev, 2012).

Estas capacidades de diseminación y de recopilación de datos constituye a *Flame* en uno de los ataques informáticos más sofisticados en materia de espionaje, con capacidades de operar tan sorprendentes como las observadas en *Stuxnet*, y que también

tiene como objetivo países de Medio Oriente. Sin embargo, los expertos en seguridad informática de *Kaspersky* sostienen que a diferencia de *Stuxnet*, que fue diseñado para sabotear un proceso industrial, *Flame* no parece apuntar a una industria específica, sino que es un complejo sistema de herramientas diseñado para realizar espionaje cibernético. En particular, los expertos descubrieron que una gran mayoría de los objetivos afectados estaban dentro de Irán, y los atacantes buscaron dibujos de *AutoCAD* (programa privativo para el diseño de planos y modelos 2D y 3D), archivos PDF y archivos de texto (Lee, 2012).

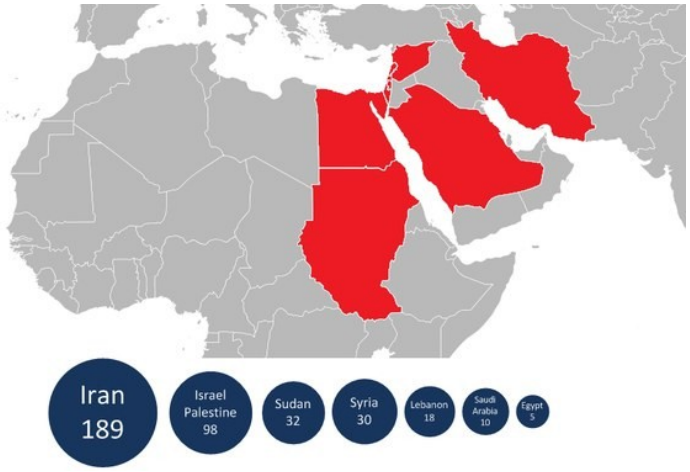

Ilustración 7: Países afectados por Flame. Fuente: Gostev (2012).

El uso de las funcionalidades de *gusano informático* y de *spyware* para lograr adquirir la información previamente descrita, de manera continua, es lo que hace sospechar a los especialistas en que *Flame* se constituye en una Amenaza Persistente Avanzada. Una vez más, el destino geográfico y la orientación cuidadosa de los ataques, combinadas con vulnerabilidades desconocidas en los sistemas operativos y programas informáticos utilizados por los objetivos, es lo que descarta, por su complejidad y costo, a los actores individuales del ciberespacio como posibles perpetradores de este ataque (Gostev, 2012). De esta manera, un Estado es el único actor que los especialistas consideran capaz de realizar un ataque tan complejo y prolongado en el tiempo, contra objetivos estatales.

Al igual que *Stuxnet*, la inexistencia de declaraciones públicas asumiendo la responsabilidad de los ataques por parte de algún Estado es un factor que impide determinar de manera fehaciente la procedencia de los ataques. Y también, como se sostuvo con el resto de los ataques informáticos, la complejidad que implica la atribución de un ataque en el ciberespacio, limita a los especialistas en su capacidad de inferir la identidad del atacante, ya que no pueden basarse estrictamente en el relevamiento de datos técnicos. Un tercer elemento que agrega aún más complejidad a la hora de determinar quién fue el perpetrador de este ataque es que, a diferencia de *Stuxnet* que estaba destinado a una industria en particular, *Flame* está diseñado para

propagarse lo más posible, y una vez expandido elegir los blancos de los cuales se pretende extraer inteligencia e información, por lo que los objetivos del ataque pueden llegar a ser inadvertidos dentro de semejante despliegue operativo (Zetter, 2012).

A pesar de los obstáculos que la situación descrita plantea para determinar qué Estado o Estados fueron los autores intelectuales y materiales de *Flame*, existen diversos indicios que parecerían apuntar a los Estados Unidos. Tate, Nakashima y Miller (2012), tres periodistas de investigación especializados en defensa, plantean la hipótesis de que *Flame* se posiciona como una herramienta más, junto con *Stuxnet*, dentro una operación mayor sobre Medio Oriente, destinada a retrasar las capacidades nucleares de la región. La operación a la que los investigadores hacen referencia recibió el nombre en clave *"Juegos Olímpicos"* (*Operation Olympic Games* en inglés), y, aunque no ha sido admitida, existen diversos argumentos de diferentes especialistas que la señalan como una campaña de sabotaje encubierta, haciendo uso de ataques informáticos, dirigida a las instalaciones nucleares iraníes y a controlar la región de Medio Oriente. Esta campaña se comenzó bajo la administración de George W. Bush en el año 2006, y se intensificó aún más en los primeros años del presidente Obama, el cual trabajó en conjunto con el gobierno de Israel, para realizar diversas Amenazas Persistentes Avanzadas para socavar las capacidades nucleares y los sistemas informáticos de la región (Sanger, 2012).

De esta manera, *Flame* se conjuga con *Stuxnet* en una serie de ataques informáticos de alta complejidad, que tuvieron lugar entre 2009 y 2012, y que persiguieron y lograron objetivos geopolíticos muy específicos. Como sostiene Steve Coll, decano de la Facultad de Periodismo de la Universidad de Columbia y ganador de dos premios Pulitzer, los logros de esta combinación de APT convierten a la *Operación Juegos Olímpicos* en el "primer acto ofensivo formal de sabotaje cibernético de Estados Unidos contra otro país, si no se cuentan las penetraciones electrónicas que precedieron los ataques militares convencionales, como el de las computadoras militares de Irak antes de la invasión de 2003" (Coll, 2012, traducción propia).

Las consecuencias que produjo la *Operación Juegos Olímpicos* tiene dos lecturas entre los principales especialistas y académicos que la han estudiado. La primera de ellas, la destaca como una estrategia novedosa para lograr objetivos geopolíticos a través de acciones que concurren específicamente en el terreno virtual del ciberespacio, y su efectividad quedó demostrada en los hechos, ya que se estima que solamente *Stuxnet* logró retrasar el desarrollo nuclear iraní por al menos dos años (Katz,

2010). Sin embargo, la segunda lectura que se realiza sobre los ataques que se realizaron bajo la Operación, los plantean como resultado de una clara militarización del ciberespacio. Este factor preocupa a muchos analistas, ya que sostienen que a pesar de los eficaces logros geopolíticos que evidenciaron estas estrategias, la militarización del ciberespacio puede incentivar a otros Estados a desarrollar o copiar capacidades ofensivas virtuales (Coll, 2012).

Stuxnet y *Flame* pueden ser utilizadas por los Estados afectados como una justificación para lanzar represalias con medios similares, por lo que muchos especialistas han señalado que estos ataques se constituyen en la demostración de un tipo arma que sólo puede mejorar y complejizarse en su accionar, lo cual empieza a plantear potenciales escaladas en las capacidades de acción y los riesgos que este tipo de ataque pueden tener (Singer y Friedman, 2014, p. 117). Como se sostuvo previamente, aunque el valor reside en la capacidad de desarrollo, la capacidad de copiar y reproducir un ataque informático puede llegar a ser tan simple como *copiar y pegar* su código, motivo por el cual los desarrollos cada vez mayores pueden dar lugar a carreras armamentistas que produzcan ataques cada vez más ofensivos.

El accionar estadounidense en el ciberespacio se evidencia en estas APT, y se caracteriza no solo por un control electrónico e informático exacerbado sobre la actividad de sus ciudadanos, sino que también ha extendido estas herramientas a todo el mundo. Las filtraciones de la Agencia Nacional de Seguridad sobre estrategias de recopilación masiva de inteligencia, y la utilización de herramientas informáticas como *Flame* para realizar APTs contra otros Estados, demuestran que poseen la capacidad de acción para lograr ataques concretos y de gran escala.

Sin embargo, la *Operación Juegos Olímpicos* también sirve de ejemplo de la complejidad y los peligros nuevos que pueden engendrar las operaciones en el ciberespacio, ya que a pesar de ser Estados Unidos uno de los países con mayor capacidad de realizar ataques informáticos de esta escala y complejidad, siquiera ellos pudieron determinar y controlar los efectos de los ataques. La capacidad de aprovechar vulnerabilidades para expandirse de manera eficaz fue tal, que sólo *Stuxnet* infectó computadoras en más de 115 países, inclusive muchas de ellas operativas dentro de los Estados Unidos. Naturalmente, *Stuxnet* no atacó los sistemas industriales estadounidenses, pero sí ilustra el carácter imprevisible de estos ataques, y fue esta rápida expansión el motivo por el cual fue descubierta la APT, y desentramada por las firmas de seguridad informática más importantes del mundo.

Como sostienen Singer y Friedman (2014, p. 117), los Estados Unidos han logrado desarrollar herramientas informáticas con capacidades de acción sin precedentes, que lograron afectar objetivos físicos en el mundo material. Sin embargo, si estas herramientas pudieron ser descifradas mediante ingeniería inversa por empresas privadas de seguridad informática, también podrían ser descifradas y reimplementadas por otros Estados, los cuales podrían usarlas para atacar también a los Estados Unidos. Estas posibilidades, si bien son teóricas, remiten a los mencionados debates sobre la posibilidad de proliferación de este tipo de armas, o a la posibilidad de una carrera armamentista cada vez mayor donde las armas son programas informáticos, por lo que la responsabilidad de un actor con tanta capacidad de acción como los Estados Unidos es crucial para determinar la escala de los conflictos en el ciberespacio.

III. La República Popular China

El rol de China en el ciberespacio está determinado de base por un atributo estructural de carácter cualitativo, que lo distingue de cualquier otro actor o Estado, y es la cantidad de usuarios y dispositivos chinos conectados a Internet: en diciembre de 2017 se contabilizaban 772 millones de usuarios chinos en Internet, el doble de los usuarios de Estados Unidos y Rusia sumados (China Internet Watch, 2018). Esta singularidad transforma a China en un objetivo muy redituable para cualquier *cracker* que realice ataques informáticos, ya que la utilización de una sola vulnerabilidad que afecte a los dispositivos chinos puede comprometer a un número mayor que en cualquier otro mercado. Un claro ejemplo de esta situación lo proporciona, *RottenSys,* un *malware* que desde 2016 se encuentra vulnerando dispositivos móviles *Android* en China, y sus márgenes de penetración preocupan cada vez más a los especialistas: en el 2018, luego de apenas dos años de haber estado infectando dispositivos, este *malware* ya logró afectar a más de cinco millones de dispositivos, los cuales pueden ser comandados remotamente, convirtiéndolo en una de las *botnets* más grandes del mundo (Cimpanu, 2018).

Sumado a esta situación, al incrementarse de manera constante la cantidad de usuarios que usan diversos tipos de dispositivos informáticos para acceder a Internet, también se diversifican la cantidad de ataques que esta creciente red recibe: el Ministerio de Seguridad Pública de China informó que, basado en sus propias estadísticas, el número de ataques informáticos dirigidos hacia la infraestructura informática China crece en una tasa de 80% anual (Singer y Friedman, 2014, p. 139). Si

bien una gran cantidad de estos ataques son realizados por *crackers* particulares en búsqueda de réditos económicos, también existen ataques que se destacan por perseguir objetivos mucho más específicos. En el 2013, por ejemplo, las filtraciones de Snowden sobre la Agencia Nacional de Seguridad de los Estados Unidos revelaron que China también formaba parte de los objetivos de las operaciones de espionaje internacional, ya que la Agencia había *crackeado,* con fines de recopilación de inteligencia, los sistemas de la Universidad de Tsinghua, una de las universidades más prestigiosas de Pekín, y sede de una de las seis redes troncales que transportan todo el tráfico de Internet de China continental (Singer y Friedman, 2014, p. 139).

Frente a esta realidad, el gobierno de la República Popular China adopta una postura muy marcada de definición de atribuciones en el ciberespacio, que se manifiesta principalmente en tres grandes estrategias. La primera estrategia se constituye en la implementación de diversas medidas que tienden a ejercer un férreo control de las conexiones de Internet dentro del territorio chino, estableciendo un sistema de vigilancia interna del ciberespacio. La segunda estrategia refiere a el desarrollo de herramientas informáticas que cuenten con una capacidad ofensiva tal, que puedan llegar a equilibrar las desventajas que China pueda tener respecto a otros países en las capacidades militares convencionales. Por último, la tercera gran estrategia se constituye en programas y operaciones de *ciberespionaje* de industrias estratégicas, con el objetivo de incrementar la competitividad de las empresas chinas al robar o copiar los desarrollos industriales de la competencia extranjera (Segal, 2017).

Como se puede observar, la primera estrategia se destaca del resto porque reviste un carácter mucho más defensivo, y es quizás una de las más conocidas y abordadas por la prensa internacional. Esta estrategia se sustenta principalmente en la premisa de que los Estados tienen derecho a controlar su propio ciberespacio, mediante las mismas atribuciones que poseen en cualquier otro dominio o territorio. Una de las acciones más claras de esta naturaleza realizadas por el gobierno chino es el denominado "*Gran Cortafuegos*" (*Great Firewall* en inglés). En informática, un *cortafuegos* es un sistema de seguridad de redes que controla y monitorea de manera constante el tráfico que entra y sale de una red, situándose como una barrera que permite o bloquea las conexiones, tomando como referencia una serie de criterios previamente establecidos. El "*Gran Cortafuegos*", entonces, es un gran sistema de control del tráfico de Internet en China, que filtra qué tipo de información está disponible para sus ciudadanos, y qué información se encuentra directamente bloqueada. Esto se traduce en que, por ejemplo,

el acceso a determinados sitios de empresas extranjeras como *Google* o *YouTube* no esté disponible en territorio chino, convirtiendo al *Gran Cortafuegos* en una herramienta de control y censura del ciberespacio chino, primordialmente con el objetivo de "prevenir la afluencia de creencias occidentales" (Wei, 2018).

Estas estrategias de control no sólo se manifiestan *de facto*, sino que también se encuentran institucionalizadas de derecho: la República Popular China no solo cuenta con una "Ley de Seguridad de Internet", sino que también existe desde 2014 la "Administración del ciberespacio de China", una oficina especialmente dedicada al control del ciberespacio (Cheung, 2015). Como se mencionó, la gran cantidad de dispositivos electrónicos chinos conectados a Internet convierten al ciberespacio de China en una de las redes más grandes del mundo, y por ende convierte al *Gran Cortafuegos* en una colosal tarea, que demuestra la capacidad operativa de los especialistas informáticos a disposición del gobierno chino. Estas capacidades en desarrollos informáticos también se evidencian en las mencionadas segunda y la tercera estrategia que China adopta frente al ciberespacio, de carácter mucho más ofensivo, y que se analizarán en las Amenazas Persistentes Avanzadas abordadas a continuación.

En síntesis, China no solo hace uso de las herramientas informáticas para controlar de manera estricta su ciberespacio, sino que las concibe como instrumentos que otorgan al gobierno capacidades sin precedentes en su accionar internacional, llegando a tener la capacidad inclusive de alterar el equilibrio de poder en el sistema internacional. Como se mencionó, los desarrollos informáticos ofensivos que el gobierno chino implementa en el ciberespacio persiguen el objetivo de mantener niveles de competitividad altos en diferentes industrias en las que compite con otras potencias, pero también usan estas capacidades ofensivas para compensar el desequilibrio comparativo que pueda tener con otros actores internacionales en las capacidades militares convencionales (Segal, 2017).

En el Libro Blanco de Estrategia Militar China del año 2015, un documento en el que el gobierno chino propone sus principales objetivos estratégicos en materia militar y geopolítica, se puso en relevancia el papel del ciberespacio, sosteniendo que inclusive el ejército chino debe prepararse para las posibles guerras informáticas contra adversarios tecnológicamente avanzados. Esta postura firme en el ciberespacio es lo que muchos analistas internacionales rescatan como principal factor de múltiples ataques informáticos sospechados de provenir de China, contra diferentes empresas tanto estatales como privadas, en general relacionadas con los objetivos geopolíticos chinos, y

con industrias pertenecientes al espectro militar. En 2017, por ejemplo, el Departamento de Defensa estadounidense registró una gran cantidad de ataques contra sus sistemas informáticos, y muchos indicios llevan al Departamento a afirmar que China estuvo detrás de los ataques, con el objetivo de obtener inteligencia sobre las capacidades militares de Estados Unidos en el ciberespacio (Segal, 2017).

La relación entre Estados Unidos y China en el ciberespacio se constituye como una de las más tensas, con una dinámica de acusaciones constantes de ambas partes sobre ataques informáticos, y una serie de desarrollos ofensivos y defensivos perseverantes que tienden a equilibrar a la contraparte. Esta relación de desconfianza mutua ha sido ampliamente abordada por diversos trabajos periodísticos y académicos, y es la que lleva a los expertos a sugerir que son estos dos Estados los más propensos a generar las condiciones para una carrera armamentista digital. Las dificultades para determinar los ataques informáticos en el ciberespacio complejizan de manera superlativa el análisis de la disuasión que pueden generar las herramientas informáticas creadas por ambos Estados, pero sin dudas tanto China como Estados Unidos cuentan con capacidades de acción que hasta el momento no han sido igualadas por ningún otro Estado. De esta manera, el despliegue de un arsenal ofensivo de ataques informáticos tendría consecuencias devastadoras para ambos Estados, y es lo que lleva a creer que los desarrollos constantes desemboquen en una carrera armamentista entre China y Estados Unidos, con una dinámica similar a la observada en la Guerra Fría entre los Estados Unidos y la Unión Soviética (Singer y Friedman, 2014, p. 144).

Un elemento curioso cuando se estudia el accionar de la República Popular China en el ciberespacio es que la mayoría de los trabajos la enmarcan en su tensa relación con los Estados Unidos, lo cual es comprensible debido a los mencionados factores. Sin embargo, estas hipótesis de conflicto desplazan de la escena a acciones mucho más concretas, y con más evidencias que señalan a China como su organizador. Curiosamente, a pesar de las rispideces con Estados Unidos, el mayor número de ataques informáticos sospechados de ser realizados por China se registra en su región de influencia más cercana: el sudeste asiático. A continuación, se analizarán dos grandes operaciones, que hicieron uso de Amenazas Persistentes Avanzadas, y que ejemplifican el accionar ofensivo sigiloso de China en el ciberespacio, contra objetivos estatales tecnológicamente inferiores, de la región de Asia-Pacífico, estratégica en términos comerciales y políticos para el gobierno chino.

1. Espionaje en el sudeste asiático

A partir de la Declaración de Bangkok de 1967, los países del sudeste asiático cuentan con una organización regional denominada "Asociación de Naciones del Sudeste Asiático", mayormente conocida por las siglas *ASEAN*, correspondientes a sus siglas en inglés. Basado en un punto de partida identitario común, los países del sudeste asiático hacen uso de la ASEAN para promover políticas de cooperación intergubernamental y de integración económica, política, de seguridad, educativa y sociocultural, entre otras, que promuevan la cohesión y el trabajo conjunto entre los países de la región.

Desde el año 1997, la ASEAN intensificó el proceso de cooperación con la región, al comenzar proyectos conjuntos y negociaciones con China, Japón y Corea del Sur, conformando lo que en la actualidad se conoce como ASEAN+3. Este proceso de integración, con la intención de fortalecer y profundizar la cooperación en Asia Oriental en diversas áreas, particularmente en los ámbitos económico y sociales, ha engendrado diversos proyectos conjuntos que demuestran la cualidad dinámica de la región. Uno de los proyectos más reconocidos es la *Iniciativa Chiang Mai*, la cual consiste de un sistema de *swaps* de divisas entre los países del ASEAN+3 para ayudar a afrontar cualquier tipo de desequilibrios financieros macroeconómicos sin la necesidad de recurrir a organismos internacionales como el Fondo Monetario Internacional (ASEAN, 2018, p. 3-4).

Esta armonía política, económica y social que genera el acuerdo regional del ASEAN+3 demuestra un activismo constante de China en la región de Asia-pacífico, ya que se conforma como su zona de influencia más importante. A pesar de esta postura amigable, también son los países del ASEAN el objetivo de un grupo de Amenazas Persistentes Avanzadas orquestadas por China descubiertas por la empresa de seguridad informática *FireEye*, las cuales estuvieron dirigidas a realizar espionaje sistemático de los Estados del sudeste asiático, durante más de una década. Este grupo de amenazas, denominado por los investigadores de *FireEye* como "*APT30*", reveló que, entre 2005 y 2015, un grupo de *malwares* fueron utilizados de manera constante en contra industrias y departamentos, tanto privados como gubernamentales, que contienen información clave sobre la región (FireEye, 2015, p. 3).

En términos técnicos, lo que sorprende a los especialistas en seguridad informática, es que *APT30* se destacaba, dentro de las cualidades que tienen las APT, por su persistencia: en vez de desarrollar ataques nuevos y diferentes para lograr objetivos más puntuales, los atacantes realizaban un trabajo constante de refinamiento y actualización de las estrategias ofensivas, para adaptar las herramientas existentes y lograr que éstas siguieran cumpliendo su función a lo largo del tiempo (FireEye, 2015, p. 6). Este factor no es menor, ya que muestra cómo la dinámica de los programas informáticos convencionales, los cuales se caracterizan por actualizarse de manera constante para adaptarse a los cambios en los sistemas operativos en los que operan, también es una dinámica utilizada por los grupos que realizan ataques informáticos para perfeccionar de manera constante sus capacidades ofensivas.

APT30 hace uso de dos grandes *backdoors* o *puertas traseras* presentes en el sistema operativo *Windows*, llamados *BACKSPACE* y *NETEAGLE*. Independientemente de las particularidades técnicas de estas vulnerabilidades, el factor importante es que ambas se constituyen como accesos previamente desconocidos a los sistemas operativos, lo que posibilitó a los atacantes infectar de manera rápida y efectiva grandes redes de computadoras. Una vez que las computadoras se encontraban comprometidas, podían ser controladas de manera remota y enviar información a servidores no autorizados, convirtiendo a *APT30* en una operación de gran capacidad, con fines de espionaje y recopilación de inteligencia (FireEye, 2015, p. 8-10). Si bien no es relevante para este análisis profundizar en detalles técnicos, sí es útil mencionar algunas particularidades que destacan a este ataque. Sumado a las *puertas traseras* mencionadas, cuando los atacantes infectaban una computadora, desplegaban un grupo específico de herramientas adicionales: *SHIPSHAPE*, *SPACESHIP*, y *FLASHFLOOD*. Estas tres herramientas, a pesar de lo capcioso de sus nombres (se traducen al español como "*ORDENADO*", "*NAVE ESPACIAL*", e "*INUNDACIÓN REPENTINA*" respectivamente), se convierten en herramientas clave para el éxito de *APT30*, ya que cumplen con la difícil función de vulnerar una técnica de seguridad informática llamada "*air gap*".

Air gap, "*espacio de aire*" en inglés, es una medida de seguridad de la red utilizada en una o más computadoras, que tiene el objetivo de protegerlas de redes consideradas no seguras, como por ejemplo Internet. Para lograrlo, literalmente se aíslan las computadoras que se intentan proteger, inhabilitando cualquier tipo de conexión

física o inalámbrica con Internet. Este concepto se constituye como casi la protección máxima que una computadora o una red de computadoras puede tener, exceptuando apagar el dispositivo. Generalmente, la información más sensible de un Estado o una empresa suele ser protegida mediante la utilización estas técnicas, y es por eso que los atacantes que llevaron a cabo *APT30* desarrollaron un grupo de ataques específicamente diseñados para sortear las técnicas de *air gapping:* una vez que SHIPSHAPE infectaba una computadora conectada a Internet, copiaba SPACESHIP y FLASHFLOOD a cualquier dispositivo de almacenamiento extraíble que se conectara a esa computadora (*pendrives*, discos externos, entre otros). Cuando alguno de estos un dispositivos extraíbles infectados era conectado a una computadora que se encontraba aislada, con la intención de transferir información o actualizar los sistemas, SPACESHIP y FLASHFLOOD se ponían en acción de manera sigilosa, escaneando, copiando, e inclusive eliminando los archivos que cumplían con el criterio de su algoritmo, y cuando tenían conexión a Internet con otra computadora, enviaban la información robada a servidores propios de los atacantes (FireEye, 2015, p. 17-18).

Esta destreza ofensiva en espionaje digital llamó la atención de *FireEye* debido a su capacidad superlativa para lograr sus objetivos de robo de información, y generó diversas hipótesis de conflicto, pero la ya aludida dificultad de establecer la atribución en el ciberespacio hace que sea muy complejo determinar quién es el actor que se encuentra detrás de *APT30*. Sin embargo, como se describió previamente, esta Amenaza Persistente Avanzada tiene uno de los historiales más largos de operaciones de espionaje informático, al haber estado activo desde 2005 hasta su descubrimiento en 2015. Este factor revela que *APT30* requirió de un desarrollo planificado y sostenido, y de una gran inversión de recursos, por lo que los expertos entienden que fue patrocinada por un Estado (FireEye, 2015, p. 3).

La actividad y los blancos atacados por *APT30* restringe aún más los posibles Estados detrás de este grupo de ataques, ya que se concentró en objetivos a lo largo del sudeste asiático e inclusive llegó a la India, priorizando la recolección de inteligencia de organismos gubernamentales y empresas públicas. Este factor, sumado a una serie de indicios, parecen incriminar a China como el Estado detrás de *APT30*: las interfaces de los programas utilizados para controlar los ataques estaban redactadas en chino, los ataques incrementaban su actividad en los encuentros de la ASEAN en las que se discutían temas de interés para China (como disputas territoriales y políticas), y también

se descubrieron ataques contra organizaciones de medios que realizaban coberturas de los sucesos políticos de la región. Esta evidencia lleva a *FireEye* a sostener que *APT30* satisface las necesidades de inteligencia del gobierno chino sobre entidades gubernamentales y de la industria en el sudeste asiático y la India, y que por eso fue desarrollado y perpetrado por el gobierno de la República Popular China (FireEye, 2015, p. 19-22).

Las operaciones de *APT30* concentran a un grupo de amenazas muy dinámico, persistente y con muchos recursos. Algunas de las capacidades de sus herramientas, en particular la capacidad de infectar redes con técnicas de *air gap*, sugieren tanto un alto nivel de planificación para obtener datos particularmente sensibles, como el que se encuentra en las redes gubernamentales. Esta APT se constituye en una de las Amenazas Persistentes Avanzadas más prolongadas en el tiempo, y demuestra las capacidades sin precedentes que China tiene a su disposición para recopilar información e inteligencia de su área de influencia más próxima.

Los expertos que diseccionaron y estudiaron *APT30* concluyen que en su accionar, a pesar de haber atacado diversas empresas e industrias de la región, no parece centrarse en robar propiedad intelectual o tecnologías de vanguardia desarrolladas en la zona, por lo que no podría ser enmarcada en la mencionada estrategia de espionaje para mantener la competitividad industrial de las empresas chinas. Por el contrario, los expertos destacan esta APT por enmarcarse en una estrategia con tintes militares, ya que apuntaba a adquirir datos confidenciales sobre las planificaciones oficiales de carácter confidencial de diversos gobiernos del sudeste asiático, Estados que se constituyen como estratégicos para la influencia y legitimidad de China en la región (FireEye, 2015, p. 28). De esta manera, estos ataques informáticos condicen con el abordaje férreo del ciberespacio adoptado por China, y demuestra que no escatima en el uso de herramientas que le permitan balancear el equilibrio de poder en Asia a su favor.

2. Operaciones de *spear phishing* contra industrias estratégicas

Como se mencionó, la tercera estrategia principal que la República Popular China tiene en el ciberespacio es el de aprovechar la dinámica de Internet para llevar a cabo ataques que le permitan adquirir tecnología extranjera mediante el espionaje cibernético, lo cual permitiría equilibrar desventajas en desarrollos estratégicos en el

mundo físico. La empresa estadounidense de seguridad informática *FireEye* ha realizado una recopilación exhaustiva de diferentes ataques informáticos, los cuales son considerados parte de una gran Amenaza Persistente Avanzada llevada a cabo por China con este objetivo, y que ha denominado "*UPS*".

UPS se constituye como un grupo de ataques informáticos, los cuales comparten una serie de objetivos comunes, con suficiente evidencia como para apuntar a China como el Estado detrás de los ataques. Identificado como una APT muy elaborada en su accionar, *UPS* hizo uso, en diferentes oportunidades, de vulnerabilidades presentes en los exploradores web más utilizados del mundo (*Internet Explorer, Firefox*), para diseminarse y para realizar sus ataques (Eng y Caselden, 2015).

Dentro de las principales operaciones de este grupo de ataques existen dos principales que son útiles para reflejar la capacidad de acción y los blancos atacados: *Operación Zorro Clandestino* (Scott, 2014) y *Operación Lobo Clandestino* (Eng y Caselden, 2015). La primera, *Operación Zorro Clandestino*, fue descubierta en el año 2014, y consistía inicialmente en una serie de ataques *phishing* a través de correos electrónicos, que hacían uso de una vulnerabilidad *día cero* en el navegador web instalado por defecto en el sistema operativo *Windows*, *Internet Explorer*. Lo curioso de esta operación, que a su vez revela su carácter persistente, fue que siguió estando activa inclusive luego de que *Microsoft* actualizara *Internet Explorer* para corregir la aludida vulnerabilidad: mediante la utilización de técnicas de *spear phishing*, la *Operación Zorro Clandestino* continuó atacando a un grupo específico de empresas, comunicándose por correo electrónico que simulaba ser un postulante que ponía a disposición su *currículum vitae*. Cuando un empleado de la empresa intentaba abrir el documento, automáticamente se instalaba una *puerta trasera* que permitía a un servidor remoto controlar y extraer información de las computadoras afectadas (Scott, 2014).

Con un nombre y un *modus operandi* similar, la *Operación Lobo Clandestino* realizaba ataques de *spear phishing* haciendo uso de una vulnerabilidad en *Adobe Flash Player*, una aplicación informática privativa ampliamente utilizada, que reproduce archivos multimedia dentro de los navegadores web. Esta operación enviaba correos electrónicos a empresas simulando ofrecer beneficios empresariales exclusivos, a los cuales se podían acceder siguiendo un enlace web. Cuando un empleado hacía clic en el enlace, era redirigido a una página web que parecía legítima, pero que reproducía un breve pero peligroso video haciendo uso de *Adobe Flash Player*: simultáneamente a la reproducción del video, el ataque instalaba el mismo *malware* usado por la *Operación*

Zorro Clandestino, el cual creaba *puertas traseras* que enviaban información a servidores que podían controlar remotamente las computadoras afectadas (Eng y Caselden, 2015).

A pesar del carácter técnico previamente descrito de ambas operaciones, estos ataques demuestran cómo las estrategias ofensivas en el ciberespacio tienen la capacidad de adquirir avatares cada vez más complejos y rebuscados, y también cada vez más eficaces en su capacidad de acción. El factor que volvió a *UPS* una APT extremadamente peligrosa fue el tipo de industrias a las cuales se atacó: empresas dedicadas a desarrollos aeroespaciales y de defensa, de construcción e ingeniería, empresas dedicadas al desarrollo de alta tecnología, conglomerados de telecomunicaciones y empresas de transporte. Si bien una porción considerable de los ataques de esta APT se concentraron en el sudeste asiático, existieron reportes de computadoras y redes afectadas en todo el mundo, por lo que *UPS* se constituye en una amenaza muy significativa, al afectar empresas de los mencionados rubros, los cuales revisten un valor estratégico para un Estado.

Estos casos de *spear phishing* redoblan aún más la apuesta a la hora de establecer atribuciones, ya que por lo general hacen uso de servicios de correo electrónico comerciales utilizados por millones de usuarios, pero algunos factores delatan la posible proveniencia de los ataques que conformaron *UPS*. Concretamente, la especificidad de los actores atacados, sumada a la utilización de múltiples ataques de *día cero*, que como se mencionó son muy codiciados en el mercado negro de la *dark web*, lleva a creer a los especialistas que esta APT fue realizada por grupos respaldados por el gobierno chino, ya los objetivos atacados se alinean con las estrategias de la República Popular China en el ciberespacio (FireEye Threat Intelligence, 2015a).

UPS se alza como una serie de ataques que ponen en relevancia la adopción de medidas de seguridad informática integrales, no solo en organismos gubernamentales sino también en empresas que conforman sectores estratégicos para un Estado. En los casos de *phishing* resulta preponderante la capacitación del usuario final que hace uso de computadoras que almacenan datos sensibles, o que están conectadas a redes que contienen información importante. Sin embargo, *UPS* plantea una paradoja, ya que también hace uso de vulnerabilidades técnicas (*día cero)* desconocidas e imperceptibles inclusive para un usuario capacitado, que pudieron ser aprovechadas estrictamente por la utilización de programas y aplicaciones informáticas privativas. De esta manera, la utilización de programas auditables de código abierto podría haber minimizado, o

inclusive eliminado, la capacidad de acción de estos ataques. Una vez más, las diversas formas en las que se perfeccionan los atacantes para realizar sus acciones es un factor que llama a la aplicación de medidas integrales de seguridad informática, ya que ninguna implementación aislada puede suplir todas las debilidades que pueden surgir en los sistemas informáticos.

IV. La Federación de Rusia

La cosmovisión que Rusia posee del ciberespacio, y de los potenciales enfrentamientos que en éste puedan acontecer, es una de las más particulares de las tres potencias analizadas en este trabajo de investigación. Como punto de partida, los rusos en general no utilizan realmente el prefijo *ciber*, ni mucho menos un término como *ciberguerra*, excepto cuando hacen referencia a escritos extranjeros de la temática. Por el contrario, tienden a utilizar un término diferente: "*informatización*". Este factor, lejos de ser una mera distinción conceptual, revela la cosmovisión que los rusos tienen sobre el ciberespacio: lo comprenden como parte de un rubro mucho más amplio, que es el de la *información*. De este modo, los teóricos militares rusos emplean el término *informatización* como un concepto holístico que incluye ataques informáticos en el ciberespacio, pero también operaciones psicológicas y operaciones de información que hacen uso de la tecnología para cumplir con sus objetivos (Conner y Vogler, 2017, p. 3).

En disonancia con la percepción de los Estados Unidos y China, el gobierno ruso concibe al *terreno de la información* como un campo de acción más sobre el cual un Estado puede desenvolverse, y el ciberespacio se alza como una parte que integra el terreno de la información, pero no lo compone en su totalidad. De este modo, la hipótesis de conflicto de los estrategas rusos no gira en torno a las *ciberguerras*, sino que las considera como instrumentos para una hipótesis de conflicto más amplia: las *guerras de la información*, es decir el uso y la manipulación de la información para obtener ventajas por sobre un adversario.

Conner y Vogler (2017, p. 4-9) sostienen que las ramificaciones de esta distinción conceptual son considerables ya que condicionan la cosmovisión de los rusos sobre el ciberespacio. En la Doctrina Militar de la Federación Rusa de 2010, el gobierno sostiene que una de las características principales de los conflictos militares modernos es que se pueden implementar estrategias de *guerra de la información* para lograr objetivos políticos, sin la necesidad del uso de la fuerza militar. Esto convierte a las

herramientas informáticas en un vector de ataque válido en tanto logre contribuir a las guerras de la información, y convierte al ciberespacio en uno de los múltiples terrenos en los que se realizan estas estrategias generalizadas de control de la información.

La manera en que el gobierno ruso maniobra las implementaciones de estrategias de *guerra de la información* también es un factor que lo destaca del resto de los países. Si bien es un Estado que posee cuantiosos recursos y grandes capacidades de acción, en su estructura orgánica no posee agencias destinadas a operaciones de esta cualidad. De manera habilidosa, la acción del Estado ruso es limitarse a financiar grupos no gubernamentales, o grupos *hacktivistas*, para lograr sus objetivos de *guerra de la información* en el ciberespacio. Esta afirmación, si bien está sustentada por diversos indicios, se vuelve muy difícil de demostrar, ya que los vínculos entre el gobierno y los actores que realizan los ataques son informales y casi imposibles de probar, ya que el gobierno ruso niega activamente su patrocinio a grupos de *crackers* o grupos *hacktivistas*. De esta manera, la atribución de los ataques informáticos realizados o patrocinados por Rusia es aún más compleja de establecer, pero las capacidades de acción de los ataques, sumada a la alineación con objetivos políticos y económicos del Kremlin, permite a los especialistas aseverar que este es un *modus operandi* aplicado por el gobierno ruso para operar en el ciberespacio (Conner y Vogler, 2017, p. 10).

En síntesis, en el caso de que existan suficientes evidencias como para señalar a Rusia como la fuente de un ataque informático, en general éstos se observarán provenientes de grupos no gubernamentales. La negación constante del gobierno ruso de promover este tipo de acciones redobla aún más la dificultad en la atribución de las operaciones, por más que la percepción de los especialistas sea que estos grupos estén financiados por Rusia. De esta manera, para poder aseverar la atribución de un ataque se recae, una vez más, en los factores de la capacidad de acción, y de observar si éstos coinciden con intereses específicos del gobierno ruso. Un caso ejemplar para ilustrar este complejo escenario es el acontecido en el año 2016, cuando se realizaron una serie de ataques de *spear phishing* a actores de alta jerarquía dentro del Comité Nacional Demócrata de los Estados Unidos.

Como se describió previamente, el ataque logró robar las credenciales de ingreso a los correos electrónicos de muchos miembros del mencionado Comité, robando más de 30.000 correos electrónicos que posteriormente fueron publicados en Internet mediante la plataforma de difusión ofrecida por WikiLeaks. Este ataque logró inclinar la

balanza de unas elecciones estadounidenses muy reñidas al afectar la imagen pública de la candidata demócrata Hillary Clinton, y es considerado por los analistas como uno de los elementos centrales en la victoria electoral del actual presidente estadounidense Donald Trump. Sin embargo, este caso también resulta paradigmático porque un grupo de *crackers* rusos conocidos como *Fancy Bear* admitieron la responsabilidad en los ataques, y a pesar de identificarse como un grupo independiente, muchos investigadores señalan que la capacidad de acción y el beneficio obtenido son elementos que sugieren que el grupo de *crackers* operó bajo el patrocinio de agencias de inteligencia rusas (Stone, 2016).

De esta manera, es extremadamente complejo determinar con argumentos y evidencia concreta si los ataques del 2016 de *Fancy Bear* fueron una estrategia de *guerra de la información* utilizada por el Estado ruso contra los Estados Unidos. Existen elementos que permitirían sugerir que *Fancy Bear* conforma un grupo de *hackers patrióticos,* es decir grupos de ciudadanos que realizan ataques coordinados e independientes contra lo que perciben como enemigos de su país, sin ningún patrocinio estatal (Singer y Friedman, 2014, p. 111). Sin embargo, la mayoría de los especialistas y periodistas estadounidenses se apresuran en acusar al gobierno ruso de este ataque, sosteniendo que fue una estrategia para manipular las elecciones en favor de un candidato favorable para los intereses rusos, y que inclusive se enmarca en una operación mucho más extensa de *guerra de la información* contra los Estados Unidos (Newton, 2018).

Este accionar furtivo del gobierno ruso demuestra una utilización extremadamente perspicaz del terreno pantanoso creado por las dificultades de atribución en el ciberespacio, y sus acciones vinculantes en el ciberespacio se terminan reduciendo a interpretaciones, que varían respecto a la postura que se adopte para juzgar las situaciones. Ya quedó demostrado que por más que un ataque provenga de dispositivos ubicados en territorio ruso, no se puede considerar este factor como evidencia suficiente para incriminar al gobierno en un ataque. Sin embargo, en la mayoría de los casos es también una aplicación benévola del principio de presunción de inocencia, ya que tampoco suele existir evidencia suficiente como para denegar su interés o su participación en los ataques.

De este modo, Rusia se ubica en el ciberespacio como un actor clave por su capacidad de acción y por la cantidad de recursos informáticos que posee, y que utiliza la percepción del resto de los actores de manera estratégica para llevar a cabo acciones

en el ciberespacio. Es importante resaltar que, a pesar de la doctrina de *guerra de la información* promovida oficialmente por los organismos militares rusos, los ataques que se analizarán a continuación evidencian una gran capacidad de acción por parte del gobierno ruso en el ciberespacio. Así, las capacidades ofensivas digitales de Rusia no son plausibles de ser minimizadas como una parte insignificante de las *guerras de la información*, ya que logran objetivos concretos y estratégicos haciendo uso de Internet y el ciberespacio (Conner y Vogler, 2017, p. 28).

1. Ataques de denegación de servicio y *spywares* como parte del arsenal ofensivo militar

En el año 2007, el gobierno de Estonia tomó la decisión de mover una icónica estatua de bronce que personifica un soldado soviético, desde su ubicación histórica en la capital, Tallin, hasta un cementerio de guerra en las inmediaciones de la ciudad. A su vez, cambió el nombre de la escultura de "Monumento a los Liberadores de Tallin" a "Monumento a los Caídos en la Segunda Guerra Mundial". Este gesto fue considerado por muchos como un insulto hacia los soldados soviéticos que habían derrotado al ejército nazi durante la ocupación de Estonia en la Segunda Guerra Mundial, por lo cual generó una serie de tensiones no solo con las minorías rusas de Estonia, sino también con el gobierno ruso (Spiegel Online, 2007).

A la vez que se realizaban protestas masivas en contra del traslado de la estatua, se comenzó a observar un número cada vez mayor de ataques de denegación de servicio distribuidos (DDoS) contra páginas y servicios web del gobierno de Estonia. Los ataques estaban dirigidos a la página web del Parlamento estonio, los sitios web de los partidos políticos, los bancos más grandes del país, y los medios de noticias y telecomunicaciones más importantes (Traynor, 2007). Estos ataques se extendieron durante aproximadamente un mes, obligando a la mayoría de los sitios a cerrar o interrumpir sus conexiones, y su impacto fue muy significativo: Estonia se enorgullecía de estar a la vanguardia de la tecnología de la información, con el 60 por ciento de su población utilizando Internet con regularidad, y una administración pública que se consideraba "sin papeles" por los altos niveles de informatización. De este modo, un ataque de estas características entorpeció de manera efectiva el desarrollo de las actividades administrativas cotidianas en Estonia.

En términos técnicos, probar la atribución de este tipo de ataques se vuelve extremadamente complejo. En primer lugar, la complejidad proviene del hecho de que un ataque DDoS se caracteriza por atacar desde diferentes computadoras, en diferentes ubicaciones geográficas. Y, en segundo lugar, a pesar de que los estonios insistieron en señalar al gobierno ruso como claro orquestador de los ataques, la evidencia concreta de los ataques afirmaba que provenían de *botnets* ubicadas en todo el mundo, incluidos países como Egipto, Vietnam y Perú. De esta manera, los expertos sostienen que la carencia de evidencias técnicas que permitan determinar la identidad real del atacante requiere de una interpretación más holística de los hechos. El período de mayor intensidad de los ataques, por ejemplo, se observó en los días 8 y 9 de mayo de 2007, coincidentes con el feriado nacional de Rusia que conmemora la victoria soviética sobre Alemania en la Segunda Guerra Mundial. A su vez, los ataques acompañaron un accionar diplomático por parte del gobierno ruso que consistió en congelar los vínculos con Estonia, e inclusive imponer sanciones económicas (Conner y Vogler, 2017, p. 14).

Los mencionados indicios hacen que muchos analistas señalen a Rusia como el actor principal detrás de esta serie de ataques, lo que evidenciaría una utilización persistente de ataques informáticos como parte de una *guerra de la* información contra el gobierno de Estonia. El accionar del gobierno ruso durante los ataques fue paradigmático: realizó declaraciones alentando a los *crackers* que realizaban los ataques, pero negó cualquier participación oficial. De este modo, esta APT contra Estonia evidencia no solo el abordaje minucioso y calculador del ciberespacio que realiza Rusia, sino también la capacidad de estos ataques para constituirse como *bloqueos informáticos*, que llevaron a interrumpir muchos de los servicios políticos, económicos y de información de Estonia durante semanas.

Este mismo *modus operandi* de ataques de denegación de servicio se replicó en el 2008, durante un conflicto diplomático entre el gobierno ruso y Georgia. Sin embargo, estos ataques adquieren una característica diferencial, ya que fueron realizados como preludio a las invasiones militares rusas que dieron inicio a la Guerra de Osetia del Sur de 2008. Antes de que se realizara la invasión aérea, marítima y terrestre de la zona de Osetia en Georgia, una serie de ataques DDoS derribaron las redes de Georgia, cortando las comunicaciones gubernamentales y alterando los sitios web pertenecientes al gobierno. Los bancos georgianos, las empresas de transporte y las

empresas de telecomunicaciones privadas también fueron atacadas, paralizando casi todos los servicios de comunicación y transporte en georgianos (Markoff, 2008).

Bajo el constante aluvión de ataques DDoS proveniente de *botnets* en todo el mundo, Georgia fue sometida, al igual que Estonia en 2007, a un bloqueo informático que significó, en términos tácticos, una ventaja estratégica en el campo de batalla material. Nuevamente, el gobierno ruso negó su participación en los ataques, y los portavoces rusos inclusive llegaron a sostener que estos ataques se enmarcaban en movimientos espontáneos de individuos, en Rusia o en otros lugares del mundo, que se habían comprometido a atacar los sistemas en Georgia en favor de Rusia. Al igual que en el caso de los ataques en Estonia, la participación del gobierno ruso no se pudo demostrar de manera concluyente, pero el hecho de que los ataques se realizaran específicamente con anterioridad a la invasión militar, y el hecho de que las capacidades ofensivas se tradujeran en la anulación de los servicios de comunicación georgianos, llevan a los expertos a sospechar que el gobierno ruso estuvo detrás, o al menos facilitó, los ataques DDoS contra Georgia (Conner y Vogler, 2017, p. 17).

El caso de Georgia es relevante para analizar los resultados de las primeras utilizaciones del ciberespacio como una herramienta más dentro del arsenal militar ruso, pero los ataques informáticos sobre los sistemas informáticos en Ucrania demuestran, hasta la actualidad, cómo estas estrategias se encuentran en constante refinamiento y mejora. En el momento de redacción de este trabajo de investigación, se mantiene la intervención militar de Rusia en Crimea. Desde el inicio del conflicto en 2014, se registraron una serie de actividades informáticas que redujeron sistemáticamente la capacidad del gobierno ucraniano para asegurar sus sistemas de información: ataques de *phishing,* diversos *malwares*, múltiples ataques DDoS, y acciones de ciberespionaje han sido dirigidos de manera constante contra el gobierno de Ucrania, contra su ejército, y sus empresas de telecomunicaciones. Los especialistas sugieren que estos ataques son parte de una estrategia del gobierno ruso enmarcada en su ocupación de Ucrania, y advierten que es un *modus operandi* muy similar al utilizado con anterioridad en Estonia y Georgia (Ross, 2014).

Sin embargo, a partir de fines de 2015, los ataques informáticos sobre Ucrania adquirieron un carácter diferente, ya que no se limitaron a realizar un bloqueo de los servicios informáticos, sino que se ejecutó lo que se cree que fue el primer ataque informático en el mundo contra la red eléctrica de un país (Cherepanov y Lipovsky,

2017). Con un trabajo de recopilación de inteligencia previo, este APT utilizó un conjunto de ataques denominado por algunas empresas de seguridad informática como "*Industroyer"* (acrónimo de *industry destroyer, destructor de industrias* en inglés), y apuntaron específicamente contra los sistemas de control industrial SCADA de las subestaciones eléctricas en Ucrania (Finkle, 2016).

La utilización de *Industroyer* permitía a los atacantes de esta Amenaza Persistente Avanzada controlar las subestaciones eléctricas en Ucrania, y se tradujo en un inédito corte del suministro eléctrico de zonas estratégicas, durante más de 16 horas, que terminó afectando a más de 220,000 residentes ucranianos. El nivel de complejidad y elaboración que adquirió este ataque es lo que lleva a los expertos a sugerir que fue una APT, ya que además de poder controlar el suministro eléctrico ucraniano, hacía uso de otros *malware* que permitían a los atacantes borrar información de los sistemas informáticos de las empresas eléctricas, e inclusive se registraron ataques DDoS contra las páginas oficiales que tomaban los reclamos de los clientes afectados por los cortes (Conner y Vogler, 2017, p. 19-21).

Este APT alertó de manera significativa a muchos especialistas en seguridad informática, ya que demostró, al igual que *Stuxnet*, la capacidad de un ataque informático de tener consecuencias físicas en el mundo material (Cherepanov y Lipovsky, 2017). Además, este ataque ejemplificó cómo un actor con suficiente capacidad de acción puede vulnerar una de las industrias principales que conforman la infraestructura crítica de un Estado, como es el suministro de energía eléctrica. A pesar de que, una vez más, el gobierno ruso negó cualquier tipo de participación en los ataques, esta APT cuenta con factores que señalan a Rusia como principal actor detrás de la misma, y en el caso de así serlo, los especialistas se preguntan si este ataque tan elaborado y exitoso se conforma como un hecho aislado de demostración de poder, o debería ser interpretado como una preocupante tendencia para lograr consecuencias físicas en el mundo material por parte de Rusia (Conner y Vogler, 2017, p. 19-22).

Los mencionados casos de Estonia, Georgia y Ucrania son extremadamente relevantes para este análisis, ya que, a pesar de las salvedades realizadas respecto a la atribución, se señala al gobierno de Rusia como el actor principal detrás de los ataques. De esta manera, se constituyen como Amenazas Persistentes Avanzadas realizadas por una potencia clave del sistema internacional contra objetivos regionales que revisten importancia estratégica. Estos ataques demuestran lo dispar que pueden ser las

capacidades de acción de los Estados, y cómo un estado con los recursos y las capacidades informáticas que posee Rusia, puede obtener ventajas significativas por sobre otros Estados vecinos.

2. Ataques informáticos como componentes de la *guerra de la información*

Como se mencionó previamente, el ciberespacio es entendido por la doctrina militar del gobierno ruso como un medio para lograr un objetivo mayor, definido como "*guerras de la información"*. En relación a esto, el accionar ruso en el ciberespacio no sólo está signado por las funciones de desorientación o disuasión que pueden generar los ataques informáticos, como se vio en los casos anteriores, sino que también las capacidades informáticas ofensivas son usadas en estrategias persistentes de espionaje funcionales a las guerras de la información.

Una de las amenazas persistentes avanzadas más significativas que la empresa de seguridad informática *FireEye* señala dentro de este tipo de operaciones de espionaje recibe el nombre de *Tsar Team,* "Equipo del Zar" en inglés. Esta APT tiene la capacidad de infectar computadoras y descargar archivos que crean *puertas traseras,* las cuales permiten el control y monitoreo remoto de los dispositivos afectados, y el robo de la información que éstas contienen al ser enviado a diferentes servidores. *Tsar Team* es señalado por los especialistas en seguridad informática como una operación que realiza un uso extremadamente metodológico de las herramientas informáticas, persiguiendo objetivos específicos y precisos (FireEye, 2014, p. 19-24).

La cualidad técnica detrás de *Tsar Team* para propagarse e infectar computadoras revela desde un principio que fue realizada por actores con grandes recursos económicos y capacidades de acción, limitando los posibles atacantes a un Estado. Adicionalmente, hay dos grandes evidencias que llevan a los expertos a señalar que es específicamente el gobierno ruso el que está detrás de estas operaciones de espionaje. El primero de los factores que así lo sugieren refiere a que todos los objetivos que fueron espiados son estratégicos para Rusia: Georgia, los países de Europa del Este, países miembros de la OTAN, y organizaciones y empresas de seguridad y de defensa en todo Europa (FireEye, 2014, p. 4). A su vez, el segundo gran factor que compromete al gobierno ruso es que la mayoría de los *malware* utilizados por *Tsar Team* no solo contienen partes en idioma ruso, sino que todos los programas que formaron parte de esta APT fueron compilados en las horas laborables de las zonas horarias de las

principales ciudades de Rusia. Este hecho no es menor, ya que estas herramientas fueron creadas entre las 8:00hs y las 18:00hs de Moscú y San Petersburgo (FireEye, 2014, p. 25-28).

Estos dos indicadores, sumados a la complejidad técnica de los ataques informáticos, es lo que lleva a sugerir a los especialistas en seguridad informática a afirmar que el gobierno de Rusia es el principal promotor de *Tsar Team.* Al igual que en el resto de las APT, a pesar de que en términos estrictamente técnicos sea incomprobable la participación de los Estados, esta serie de variables es uno de los elementos principales que permite a los especialistas afirmar que estos ataques son parte de operaciones de espionaje internacional en el ciberespacio promovidas por el gobierno ruso.

Una APT que también se evidencia como parte de las estrategias de espionaje emprendidas por Rusia, y que sorprendió de manera similar a los especialistas por sus capacidades ofensivas, recibe el nombre de *HAMMERTOSS*. Este ataque se caracteriza por ser extremadamente ecléctico en su accionar, ya que hace uso de diversas técnicas que giran alrededor de plataformas web con cuentan con millones de usuarios diarios: *Twitter*, *GitHub* y servidores de almacenamiento de datos en la nube (FireEye Threat Intelligence, 2015b, p. 3-4). Este ataque es muy particular, ya que aprovecha estas redes sociales y servicios para esconder su verdadera función, dentro del gran tráfico que reciben los servidores de estas redes sociales, haciendo así que su detección sea absolutamente compleja.

HAMMERTOSS hace uso de vulnerabilidades similares al resto de las APT de espionaje previamente abordadas para infectar una computadora y robar información, pero la particularidad de este ataque es que, en vez de usar medios convencionales para transportar la información, hace uso del tráfico de Twitter para enviar los datos robados. Esta técnica es muy innovadora, ya que esta red social tiene una cantidad constante de transferencia de datos, y encontrar el tráfico y los usuarios maliciosos sería efectivamente tratar de encontrar una aguja en un pajar. De esta manera, esta Amenaza Persistente Avanzada fue utilizada para robar información de diferentes gobiernos de Europa occidental y grupos de estudios de política exterior. A su vez, al igual que *Tsar Team,* los horarios de actividad registrados por este APT coinciden con los horarios laborables de las principales ciudades de Rusia. Una vez más, estos indicios técnicos, sumados a la cualidad de la información robada y los objetivos regionales estratégicos,

llevan a los especialistas a suponer que fue el gobierno ruso quien estuvo detrás de *HAMMERTOSS* (FireEye Threat Intelligence, 2015b, p. 13).

Tsar Team y *HAMMERTOSS* se constituyen como dos Amenazas Persistentes Avanzadas que han logrado extraer una gran cantidad de inteligencia de países estratégicos para el posicionamiento geopolítico de Rusia, y ambas tienen la cualidad de ser virtualmente imposibles de rastrear para obtener algún tipo de evidencia que pueda incriminar al gobierno ruso. Estas APT muestran lo advertido previamente sobre la utilización estratégica que Rusia hace de los impedimentos para establecer atribuciones en el ciberespacio, y a pesar de lo que los especialistas puedan aseverar, la negación constante por parte del gobierno ruso sobre la participación en estos ataques complejiza aún más un análisis de política regional. Salvando estas particularidades, si se toman como válidas las proposiciones de los especialistas en seguridad informática que estudiaron estos ataques, se puede evidenciar, como mínimo, la financiación por parte Rusia de grupos que se encargan de realizar ataques informáticos contra los objetivos estratégicos para el país, por lo que se puede afirmar que el ciberespacio es un factor central en la doctrina de *guerras de la información* promovida por Rusia.

V. Conclusiones parciales

Las Amenazas Persistentes Avanzadas analizadas, a pesar de sus diferencias, demuestran las capacidades ofensivas que los Estados pueden alcanzar al utilizar herramientas informáticas para perseguir objetivos geopolíticos. También son funcionales para constatar la implementación de estrategias empíricas en sintonía con los supuestos teóricos planteados en los capítulos previos, tales como los enfrentamientos en el ciberespacio, o también la hipótesis de una posible carrera armamentista digital. Referido a esto, hay un factor que resulta particularmente interesante cuando se recopila información y bibliografía sobre los ataques realizados por estas tres potencias. En términos generales, todos los reportes sobre *Stuxnet*, *Flame*, y las estrategias ofensivas en el ciberespacio realizadas por los Estados Unidos, son descubiertas y estudiadas en profundidad por empresas rusas o europeas. Esto es un factor llamativo, ya que las empresas de seguridad informática estadounidenses, como por ejemplo *FireEye*, no otorgan importancia a estos ataques, limitándose a una cobertura periodística de los casos.

Independientemente de la escala industrial que puedan adquirir los ataques en el ciberespacio patrocinados por actores con muchos recursos, las Amenazas Persistentes

Avanzadas abordadas demuestran el alcance de las capacidades ofensivas en el ciberespacio. Todos los realizados, promovidos o patrocinados por un Estado se destacan por ser altamente efectivos en su accionar, y un factor interesante que se observa es que las diferencias operativas entre las APT estudiadas parecen alinearse con las políticas exteriores de los países que las realizaron: Estados Unidos demuestra una actitud belicista e invasiva en el ciberespacio, China se empeña por controlar lo más posible su ciberespacio y las interacciones que afecten sus intereses en la región, y Rusia se mantiene expectante y precavida en su accionar, realizando esfuerzos para eliminar cualquier tipo de atribución hacia su gobierno.

De esta manera, los ataques informáticos se demostraron herramientas efectivas para afectar el equilibrio de poderes tanto a nivel regional como a nivel global en el sistema internacional. Si bien predominan las estrategias sigilosas que pretenden funcionar como herramientas de espionaje para recopilación de inteligencia, casos como los de *Stuxnet* e *Industroyer* demuestran de qué manera un Estado con grandes capacidades de desarrollo pueden llegar a afectar dispositivos físicos en el mundo material, sólo a través de ataques informáticos lanzados en el ciberespacio.

Como se mencionó, una de las diferencias principales que existen entre un ataque informático y otros desarrollos ofensivos en el mundo material, es que, para reproducir un *malware,* basta simplemente con copiar y pegar su código. Si un Estado considera un ataque informático en su contra como una justificación suficiente para lanzar represalias con medios similares contra su atacante, se podrían crear las peligrosas condiciones que den inicio a una carrera armamentista, donde las armas dejan de ser materiales y se convierten en programas informáticos que sólo pueden mejorar y complejizarse en su accionar (Singer y Friedman, 2014, p. 117).

La fácil reproducción de los ataques informáticos puede suponer también un peligro de proliferación vertical de herramientas informáticas con capacidades ofensivas disruptivas, hecho que también preocupa a los especialistas. Sin embargo, no es lo mismo copiar un ataque informático, que contar con los recursos y las capacidades como para crearlas. Éste es el papel que cumplen las potencias del sistema internacional en el ciberespacio: al igual que en el resto de las áreas, se constituyen como los actores con mayores capacidades y recursos, y por ende las que marcan el paso en materia de avances ofensivos y defensivos en el ciberespacio. De esta manera, también se constituyen como los principales garantes del orden en el ciberespacio, tarea que, como se demostró, puede volverse muy compleja.

Una última conclusión interesante es que, como se hizo hincapié, la mayoría de las Amenazas Persistentes Avanzadas analizadas pudieron ser llevadas a cabo con éxito principalmente porque aprovecharon vulnerabilidades desconocidas por las víctimas en los programas privativos que sus sistemas informáticos utilizaban. Este dato no es menor, ya que la utilización de programas informáticos y sistemas operativos libres, de código abierto, hubiesen indudablemente minimizado los efectos de los ataques informáticos abordados, principalmente por la capacidad de auditabilidad que proveen este tipo de sistemas. De esta manera, a pesar de la capacidad casi exclusiva de las grandes potencias para desarrollar herramientas informáticas ofensivas, las herramientas para generar sistemas informáticos más robustos para la defensa de los recursos informáticos de los Estados están disponibles independientemente de los recursos con los que cuente un Estado, y sólo dependen de la decisión de gubernamental de implementar políticas de seguridad informática integrales.

Conclusiones Finales

La hipótesis de este trabajo de investigación sostuvo que la Seguridad Informática es una disciplina de especial interés para las Relaciones Internacionales, cada vez más influidas por Internet y el ciberespacio, cuya mayor evidencia reside en relaciones entre las grandes potencias, Estados Unidos, China y Rusia, y las acciones que éstas emprenden respecto a sus recursos informáticos.

Con fin de encauzar estas discusiones de carácter interdisciplinario, y alcanzar los objetivos propuestos, en el primer capítulo se comenzó por presentar a Internet como la plataforma de comunicaciones más revolucionaria de los últimos decenios, por contextualizar sus orígenes, y por resaltar su cualidad material y tangible. Como se pudo observar con un breve repaso histórico, Internet nació como una herramienta de índole militar en los Estados Unidos, y fue alterando su morfología hasta lograr extenderse a escala global, tanto por variables técnicas como por variables sociales, modificando sustancialmente los mecanismos de comunicación y producción de los esquemas tradicionales.

El mundo contemporáneo se encuentra cada vez más interconectado por Internet, pero a los fines de este trabajo de investigación, se focalizó el análisis en el campo de acción que esta tecnología crea: el *ciberespacio.* Definido como un entorno virtual de información, compuesto por datos digitalizados que son almacenados y compartidos utilizando tecnologías de la comunicación, el ciberespacio se vuelve nodal para este análisis de las relaciones internacionales ya que es también un terreno en el cual los Estados interactúan. Si bien el ciberespacio, con la multiplicidad de factores que introduce, da lugar a la generación de nuevos actores, aquellos actores tradicionales del sistema internacional conservan su representación en el ciberespacio: personas individuales, grupos, empresas, organizaciones no gubernamentales, gobiernos subnacionales y Estados nacionales, todos tienen su identidad en el ciberespacio.

Desde el abordaje teórico realista utilizado para encauzar este trabajo de investigación, se establecieron dos grandes paralelos entre el ciberespacio y el sistema internacional neorrealista estructural. En primer lugar, se señaló que el ciberespacio conserva las estructuras de poder existentes en el sistema internacional, ya que a pesar de las nuevas capacidades que pueden generar Internet y el ciberespacio, aquellos actores con mayores recursos son los que conservan las mayores capacidades de acción. En segundo lugar, y derivado del primer punto, tanto el sistema internacional como el

ciberespacio se caracterizan por ser anárquicos, no entendido como un desorden fruto de la falta de autoridades (tanto en el sistema internacional como en Internet existen entidades que tienden a regular los comportamientos), sino por el contrario, carente de un gobierno único y generalizado. El resultado de esta acefalía es que en ambos espacios reine una estabilidad producida por el equilibrio de poderes entre aquellos actores que conservan las mayores capacidades de acción.

Como se señaló durante la introducción, abordar todas las variables que Internet, el ciberespacio y la virtualidad introducen en las relaciones internacionales, sería una tarea ciclópea que se extralimitaría de los alcances teóricos y físicos de este trabajo de investigación, ya que son múltiples los factores que se pueden analizar. Es por este motivo que, conservando la perspectiva teórica realista, se utilizó a la disciplina de la seguridad informática para analizar el impacto de la virtualidad en las relaciones internacionales. La seguridad informática se definió en el primer capítulo como el área de la informática que se enfoca en la protección de la información almacenada o circulante en una red de computadoras, y se alza como una disciplina central para abordar la protección de los recursos virtuales de los Estados en el ciberespacio.

Se sostuvo que el concepto de *seguridad informática* posee la característica tácita de estar asociado con la presencia de un adversario. Por definición, las estrategias de seguridad se plantean en base a un supuesto de amenaza, que en este caso se configura como una amenaza informática enmarcada en la virtualidad del ciberespacio. Lo diferencial entre una acción ofensiva en el mundo material, y un ataque informático, no reside en los actores que pueden efectuarlos, sino en los medios que éstos pueden utilizar para llevarla a cabo, en este caso medios virtuales. Es por este motivo que se introdujeron también en el primer capítulo los principales ataques informáticos, acompañados de ejemplos funcionales para entender los alcances de un ataque lanzado desde una computadora.

Al afirmar que las estructuras de poder del sistema internacional se mantienen prácticamente inalteradas en el ciberespacio, se reproducen también factores que destacan a los Estados por encima del resto de los actores internacionales. La teoría neorrealista plantea a los Estados no como los únicos actores, sino como los más relevantes del sistema internacional, y los únicos que concentran tanto poder como para lograr imponer reglas de juego al resto de los actores. En el esquema virtual del ciberespacio, se reproduce la misma situación, y los Estados son aquellos actores que conservan mayor capacidad de acción en términos de seguridad informática,

principalmente debido a su mayor disponibilidad de recursos económicos y técnicos. De esta manera, el segundo capítulo restringió el análisis a los Estados, haciendo foco en la influencia que los factores virtuales tienen sobre las relaciones intergubernamentales.

Se revisó cómo el ciberespacio otorga nuevas variables de análisis a conflictos internacionales como el terrorismo, dando lugar a la posibilidad del fenómeno del *ciberterrorismo*, y se observó de qué manera se reconfiguran conceptos tan tradicionales como la guerra. Una de las conclusiones principales respecto a este último punto reside en que la posibilidad de un enfrentamiento militar tradicional en el ciberespacio, en el que dos o más bandos intercambian ataques, se ve determinado por una gran cantidad de variables. Como punto de partida, el factor principal reside en la dificultad para establecer con certeza la procedencia de un ataque informático, hecho que desestimaría la posibilidad de que se produzca un conflicto de estas características en el ciberespacio. Hasta el momento de redacción de este trabajo de investigación, si bien existen múltiples libros y artículos abordando la temática de *ciberguerra*, aún no existen casos que se configuren como un enfrentamiento bélico en el ciberespacio. Esta realidad no implica una desestimación de la posibilidad de que suceda, sino que invitó a realizar un análisis más certero sobre las formas que puede adoptar un conflicto entre Estados en el ciberespacio.

Como se demostró, el primer factor determinante para estudiar las estrategias informáticas ofensivas implementadas por los Estados, reside en la dificultad de establecer la atribución en el ciberespacio. A todos los factores técnicos que se introdujeron para justificar esta afirmación en el primer y segundo capítulo, se suma la posibilidad de utilizar herramientas especialmente diseñadas para ocultar las identidades en el ciberespacio (*botnets* o redes privadas virtuales, por ejemplo), lo cual termina condicionando el estudio de estos ataques. A su vez, en aquellos casos en los que existen suficientes evidencias técnicas y geopolíticas como para señalar a un Estado como el orquestador de un ataque informático, los gobiernos siempre deniegan las acusaciones, y aprovechan el pantanoso estado de atribución de los ataques en el ciberespacio. Es por este motivo que se concluyó que los conflictos entre Estados están tomando, y continuarán tomando, la forma de ataques sigilosos y secretos, más que el despliegue público de arsenales informáticos.

Este factor complejiza los análisis y no permite establecer generalizaciones certeras, pero sí se pudieron extraer lineamientos que contribuyen a analizar la situación de los Estados en el ciberespacio. En primer lugar, se sugirió que las complejidades de

atribución generan un terreno fértil para una carrera armamentista, la cual posee diversos indicadores que parecerían sugerir que ya está en curso, y en la cual los desarrollos informáticos ofensivos tendrían una capacidad de acción cada vez mayor. En segundo lugar, el aumento cuantitativo de técnicos dedicados a la seguridad informática en empresas privadas dentro de las principales potencias, parecería indicar la gestación de un complejo industrial que se avoque a desarrollar estrategias ofensivas y defensivas para los Estados en el ciberespacio. Por último, se puede concluir que las interacciones ofensivas entre Estados en el ciberespacio requieren de un análisis interdisciplinario y dinámico, que conjugue las concepciones geopolíticas con las variables técnicas para comprender las motivaciones detrás de un conflicto informático.

Frente a estos hechos, uno de los elementos que se destacó en el segundo capítulo fue que, a pesar de que muchos Estados lo intentaron, hasta el momento no se han logrado acuerdos internacionales que puedan tender a un entendimiento sobre el uso seguro y comunitario del ciberespacio. Si bien han existido iniciativas con este fin, su complejidad reside en la multiplicidad de actores diferentes, que tienen diferentes perspectivas y usos sobre el ciberespacio, y a su vez sería, por las razones esgrimidas previamente, muy difícil de controlar su aplicación. La sumatoria de estos factores llevó presentar un escenario anárquico en los términos planteados por la teoría neorrealista, y a la conclusión preliminar de que la seguridad y la defensa informática que los Estados poseen para proteger sus recursos informáticos está determinada por las políticas y la asignación de recursos que cada uno realice. A pesar de este factor, se señalaron puntos estructurales en la disciplina de la seguridad informática que se resaltan por constituirse en estrategias de bajo costo, aplicables por todos los Estados, sin ser determinante la cantidad de recursos económicos y técnicos disponibles.

La primera estrategia, de carácter técnico, refiere a la implementación de sistemas informáticos basados en programas informáticos libres, de código abierto. Diversos casos empíricos demuestran que estos programas son más auditables y seguros, y su implementación planificada, mejoraría estructuralmente el posicionamiento de cualquier estructura estatal en el ciberespacio. El segundo elemento no necesariamente es de carácter técnico, sino que refiere a la generación de políticas que tiendan a la capacitación y concientización del personal público encargado de gestionar información sensible, para que no se convierta en el eslabón débil dentro de las estrategias de seguridad informática.

Si bien la presentación de las principales amenazas informáticas se realizó en el primer capítulo acompañada de diversos ejemplos ilustrativos, el objetivo del tercer capítulo fue demostrar el extremo teórico y práctico de los ataques informáticos, mediante el análisis del accionar de las principales potencias del sistema internacional en el ciberespacio. Si bien no se logran enmarcar en el supuesto teórico de una *ciberguerra,* los casos analizados son Amenazas Persistentes Avanzadas, es decir los ataques informáticos más complejos y costosos, con suficientes pruebas como para señalar a Estados Unidos, China y Rusia como los atacantes. Estas acciones ofensivas ilustran las capacidades que puede tener una amenaza en el ciberespacio para explotar vulnerabilidades estructurales en otros sistemas informáticos, y pudieron ser ejecutados por la disponibilidad de recursos económicos y técnicos de las grandes potencias, factor distintivo del resto de los Estados.

De este modo, en el tercer capítulo se realizó una introducción de las principales políticas que cada una de estas tres potencias posee respecto a su accionar en el ciberespacio, y se procedió a analizar casos empíricos de ataques informáticos que persiguieron un objetivo económico o geopolítico, con suficiente evidencia como para señalarlos como los Estados que los perpetraron. Este capítulo es funcional en el análisis de este trabajo de investigación por dos motivos. En primer lugar, revisa las legislaciones vigentes y las declaraciones que las potencias más poderosas del sistema internacional poseen en relación a Internet, el ciberespacio y la seguridad informática, lo cual resulta útil para resaltar, con evidencia institucional, la relevancia del ciberespacio en la esfera estatal. En segundo lugar, es funcional ya que toma, a pesar de los problemas de atribución aseverados, ejemplos que apuntan con suficiente evidencia a estas tres potencias como sus perpetradoras, evidenciando las potencialidades que adquiere el ciberespacio para reconfigurar el equilibrio de poder del sistema internacional.

Una conclusión interesante que se puede extraer es que todos los casos de ataques informáticos abordados a lo largo de esta tesis se constituyeron en una sorpresa para sus descubridores, tanto políticos como expertos en seguridad informática, ya que significaron la implementación de estrategias informáticas novedosas en el ciberespacio, y la combinación inédita de herramientas informáticas con grandes capacidades ofensivas. Si bien todos los casos analizados son recientes, ya que ocurrieron en los últimos dos decenios, es imposible saber cuáles son las estrategias que los Estados con

recursos están utilizando en este momento para obtener una ventaja en el ciberespacio, y por ende en el sistema internacional.

Si se toman los casos de ataques informáticos abordados en el tercer capítulo, y todos los mencionados a lo largo del desarrollo de la tesis, se puede extraer un hilo conector que une a todos los sucesos: tuvieron éxito porque los dispositivos atacados poseían una vulnerabilidad en un programa informático privativo, o tuvieron éxito por la negligencia de un usuario sin suficiente capacitación en las buenas prácticas de la seguridad informática, cuando no fueron una combinación de ambos factores. Por este motivo se vuelven relevantes las estrategias de seguridad informática planteadas en el segundo capítulo, ya que la implementación de políticas que tiendan a crear sistemas informáticos que hagan uso de programas informáticos libres de código abierto, sumada a políticas de capacitación en seguridad informática para los funcionarios que sean responsables de administrar información sensible para los intereses estratégicos de un Estado, significarían una mejora estructural sustancial en la seguridad informática de los Estados.

Es necesario resaltar que la mayoría de los ataques informáticos mencionados tuvieron éxito porque explotaron vulnerabilidades en el sistema operativo *Windows*, el más utilizado en el mundo, o porque los usuarios fueron engañados con tácticas de *phishing*. Si bien se constituye como una afirmación contrafáctica, la implementación de las políticas de seguridad informática sugeridas en el segundo capítulo, hubiesen reducido sustancialmente la capacidad de acción de los ataques, hecho que se vuelve estratégico si se considera que muchos de los ataques lograron afectar el equilibrio de poderes, tanto a nivel regional como a nivel global, en el sistema internacional.

De acuerdo a lo mencionado hasta aquí, se considera que, a lo largo del desarrollo de este trabajo de investigación, se ha podido responder a los interrogantes planteados, y se concretaron los objetivos propuestos. En función de lo expresado se considera que la hipótesis central ha sido constatada. De esta manera, se considera la seguridad informática es una disciplina que afecta las relaciones internacionales, condiciona la manera en que los Estados se insertan en la estructura internacional influida por la virtualidad, y tiene la capacidad de modificar las distribuciones de poder en el sistema internacional. El trabajo no se plantea como una fuente irrefutable de respuestas ante una trama interdisciplinaria de semejante dimensión, sino que buscó aportar una caracterización y un análisis general de la disciplina, con la ambición de

proporcionar elementos que permitan un abordaje más específico de una temática que posee una gran influencia en las relaciones internacionales del siglo XXI.

Referencias Bibliográficas

Adams, James (2001). "Virtual Defense", en *Foreign Affairs*, 80(2), pp. 98-112. Disponible en: https://www.jstor.org/stable/i20050144 [Consultado 16/06/18]

Albright, D., Brannan, P. y Walrond, C. (2010). "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?", en *Institute for Science and International Security Report*. Disponible en: http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf [Consultado 16/10/18]

Aldorisio, Jeff (2018). "What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More", en *Digital Guardian*. Disponible en: https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more [Consultado 09/10/18]

Alton, Larry (2018). "5 cybersecurity measures every small business should take this year", en *allBusiness*. Disponible en: https://www.allbusiness.com/5-cybersecurity-measures-every-small-business-should-take-this-year-103090-1.html [Consultado 04/10/18]

Asamblea General de las Naciones Unidas (1967). "Definición de la agresión", en *Resolución 3314 (XXIX)*

ASEAN (2018). "Overview of ASEAN Plus Three Cooperation", en *ASEAN Secretariat Information Paper*. Disponible en: https://asean.org/wp-content/uploads/2016/01/Overview-of-APT-Cooperation-Jul-2018.pdf [Consultado 22/10/18]

Barak, Boaz (2018). "Cryptography", en *Introduction to Theoretical Computer Science*. Disponible en: https://introtcs.org/public/lnotes_book.pdf [Consultado 27/08/18]

Barlow, Jeffrey (2010). *Cyber War and U.S. Policy: Part I, Neo-realism*. Oregón: Pacific University.

Barwise, Mike (2010). "What is an internet worm?", en *BBC WebWise*. Disponible en: http://www.bbc.co.uk/webwise/guides/internet-worms [Consultado 28/08/18]

BBC (2010). *Activists target recording industry websites*. Disponible en: https://www.bbc.co.uk/news/technology-11371315 [Consultado 18/09/18]

BBC (2015). *Thai government websites hit by denial-of-service attack*. Disponible en: https://www.bbc.com/news/world-asia-34409343 [Consultado 23/08/18]

BBC (2016). "Qué dicen los últimos correos electrónicos de Hillary Clinton filtrados por WikiLeaks", en *BBC Mundo*. Disponible en:

https://www.bbc.com/mundo/noticias-internacional-37686006 [Consultado 22/08/18].

Beeping Computer (2017). *Most industrial control systems get infected with malware by accident*. Disponible en: https://www.bleepingcomputer.com/news/security/most-industrial-control-systems-get-infected-with-malware-by-accident/ [Consultado 14/08/18]

Benzmüller, Ralf (2018). "Malware numbers 2017", en *G DATA Security Blog.* Disponible en: https://www.gdatasoftware.com/blog/2018/03/30610-malware-number-2017 [Consultado 28/08/18]

Bergman, Michael K. (2001). "White Paper: The Deep Web: Surfacing Hidden Value", en *Journal of Electronic Publishing*, 7(1).

Breene, Keith (2016). "Who are the cyberwar superpowers?", en *World Economic Forum.* Disponible en: https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/ [Consultado 29/09/18]

Calamur, Krishnadev (2017). "Putin says 'Patriotic Hackers' may have targeted U.S. election", *The Atlantic*, 1 de junio. Disponible en: https://www.theatlantic.com/news/archive/2017/06/putin-russia-us-election/528825/ [Consultado 03/07/18]

Cavalcante, Beatriz (2017). "WannaCry no Brasil e no Mundo", en *O Povo*. Disponible en: https://www.opovo.com.br/jornal/economia/2017/05/wannacry-no-brasil-e-no-mundo.html [Consultado 28/08/18]

Castells, Manuel (2000). *La era de la información: economía, sociedad y cultura. Volumen I. La Sociedad Red.* Madrid: Alianza Editorial.

Castells, Manuel (2001). *La Galaxia Internet.* Barcelona: Areté.

Chandler, Daniel (1995). *Technological or Media Determinism*. Disponible en: http://visual-memory.co.uk/daniel/Documents/tecdet/ [Consultado 26/09/18]

Cherepanov, A. y Lipovsky, R. (2017). "Industroyer: Biggest threat to industrial control systems since Stuxnet", en *WeLiveSecurity by* ESET. Disponible en: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ [Consultado 24/10/18]

Cheung, Jennifer (2015). "China's 'great firewall' just got taller", en *OpenDemocracy.* Disponible en: https://www.opendemocracy.net/digitaliberties/jennifer-cheung/china's-'great-firewall'-just-got-taller [Consultado 20/10/18]

China Internet Watch (2018). *Whitepaper: China Internet Overview*. Disponible en: https://www.chinainternetwatch.com/whitepaper/china-internet-statistics/ [Consultado 20/10/18]

Choucri, N. y Clark, D. (2012). "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma", en *MIT Political Science Department Research Paper No. 2012-29*. Disponible en: https://ssrn.com/abstract=2178586 [Consultado 11/09/18]

Cimpanu, Catalin (2018). "Chinese Crooks Assembling Massive Botnet of Nearly 5 Million Android Devices", en *Bleeping Computer*. Disponible en: https://www.bleepingcomputer.com/news/security/chinese-crooks-assembling-massive-botnet-of-nearly-5-million-android-devices/ [Consultado 20/10/18]

Cisco (2018). *What Are the Most Common Cyberattacks?* Disponible en: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html [Consultado 17/08/18]

Clough, Jonathan (2015). "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation", en *Monash University Faculty of Law Legal Studies Research Paper No. 2015/06*, pp. 698-736. Disponible en: https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf [Consultado 09/10/18]

Code.org (2016). *What is the Internet?*. Disponible en: https://www.youtube.com/watch?v=Dxcc6ycZ73M [Consultadoo 12/08/18]

Coll, Steve (2012). "The Rewards (and Risks) of Cyber War", en *The New Yorker.* Disponible en: https://www.newyorker.com/news/daily-comment/the-rewards-and-risks-of-cyber-war [Consultado 17/10/18]

Comité Permanente de la Asamblea Popular Nacional de la República Popular China (2017). *Ley de Seguridad Informática de la República Popular de China*. Disponible en: http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm [Consultado 22/08/18]

Committee on National Security Systems (2010). *National Information Assurance (IA) Glossary.* Instrucción n° 4009. Disponible en: https://www.hsdl.org/?view&did=7447 [Consultado 18/08/18]

Connell, M. y Vogler, S. (2017). *Russia's Approach to Cyber Warfare*. Virginia: CNA Analysis & Solutions.

Craig, A. & Valeriano, B. (2018). *Realism and Cyber Conflict: Security in the Digital Age*. Disponible en: http://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/ [Consultado 16/05/18]

CTED (2017). "Physical Protection of Critical Infrastructure against Terrorst Attacks", en *CTED Trends Report*. Disponible en: https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-March-2017-Final.pdf [Consultado 27/09/18]

Cybersecurity Ventures (2018). *2018 Cybersecurity Market Report.* Disponible en: https://cybersecurityventures.com/cybersecurity-market-report/ [Consultado 01/10/18]

Dahl, Melissa (2015). "So here's a study about Internet cats", en *The Cut*. Disponible en: https://www.thecut.com/2015/06/heres-a-study-about-internet-cats.html [Consultado 11/10/18]

Deibert, R. y Rohozinski, R. (2011). "The new cyber military-industrial complex", en *The Globe and Mail*. Disponible en: https://www.theglobeandmail.com/opinion/the-new-cyber-military-industrial-complex/article573990/ [Consultado 01/10/18]

Departamento de Defensa de los Estados Unidos (2011). *Estrategia para Operar en el Ciberespacio*.

Defense Advanced Research Projects Agency (2018). *About DARPA.* Disponible en: https://www.darpa.mil/about-us/about-darpa [Consultado 06/08/18]

Dewey, Caitlin (2014). "36 ways the Web has changed us", en *The Washington Post.* Disponible en: https://www.washingtonpost.com/news/arts-and-entertainment/wp/2014/03/12/36-ways-the-web-has-changed-us/?utm_term=.69d11bace401 [Consultado 18/08/18]

DHS Press Office (2016). *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security.* Disponible en: https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national [Consultado 04/09/18]

Dimov, Ivan (2015). “Spear-phishing statistics from 2014-2015”, en *Infosec Institute*. Disponible en: https://resources.infosecinstitute.com/spear-phishing-statistics-from-2014-2015/#gref [Consultado 20/08/18]

Dinstein, Yoram (2005). “What is war?”, en *War, Aggression and Self-Defence*, pp. 3-29. Cambridge: Cambridge University Press.

Donnelly, Jack (2009). *Realism. Theories of International Relations: 4th Edition* (cuarta edición, pp. 31–56). Nueva York: Palgrave Macmillan.

Dunlap, Charles (2011). “Perspectives for Cyber Strategists on Law for Cyberwar”, en *Strategic Studies Quarterly*, 5(1), pp. 81-99. Disponible en: http://www.jstor.org/stable/26270511 [Consultado 29/09/18]

Dunn, Myriam A. (2007). “Securing the Digital Age: The Challenges of Complexity for Critical Infraestructure Protection and IR Theory.” En: Eriksson, J. & Giacomello, G. *International Relations and Security in the Digital Age*. Londres: Routledge.

Edwards, Greg (2017). *Zero-Day Attack Examples*. Disponible en: https://www.linkedin.com/pulse/zero-day-attack-examples-greg-edwards/ [Consultado 06/10/18]

Eng, E. y Caselden, D. (2015). “Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign”, en *FireEye Threat Inteligence*. Disponible en: https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html [Consultado 23/10/18]

Europa Press (2015). *Esta semana Internet ha cumplido 46 años*. Disponible en: https://www.europapress.es/portaltic/internet/noticia-semana-internet-cumplido-46-anos-primera-conexion-arpanet-20151031115932.html [Consultado 28/08/18]

FBI (2012). *New Internet Scam. ‘Ransomware’ locks computers, demands payment*. Disponible en: https://www.fbi.gov/news/stories/new-internet-scam/new-internet-scam [Consultado 28/08/18]

FBI (2018). *What we investigate*. Disponible en: https://www.fbi.gov/investigate/cyber [Consultado 25/09/18]

Finkle, Jim (2016). “U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage”, en *Reuters*. Disponible en: https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108 [Consultado 24/10/18]

Finley, Klint (2013). “French National Police switch 37.000 desktop Pcs to Linux”, en *Wired*. Disponible en: https://www.wired.com/2013/09/gendarmerie-linux/ [Consultado 09/10/18]

FireEye (2014). *APT28: A window into Russia’s cyber espionage operations?* California: FireEye Labs. Disponible en: https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html [Consultado 24/10/18]

FireEye (2015). *APT30 and the mechanics of a long-running cyber espionage operation.* California: FireEye Labs. Disponible en: https://www.fireeye.com/current-threats/apt-groups/rpt-apt30.html [Consultado 22/10/18]

FireEye (2018). *M-Trends 2018*. Milpitas: FireEye.

FireEye Threat Intelligence (2015a). *Demonstrating Hustle, Chinese APT Groups Quickly Use Zero-Day Vulnerability (CVE-2015-5119) Following Hacking Team Leak.* California: FireEye Labs. Disponible en: https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html [Consultado 23/10/18]

FireEye Threat Intelligence (2015b). *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*. California: FireEye Labs. Disponible en: https://www.fireeye.com/current-threats/apt-groups/rpt-apt29.html [Consultado 24/10/18]

Fox News (2008). *Hackers Declare War on Scientology*. Disponible en: http://www.foxnews.com/story/2008/01/25/hackers-declare-war-on-scientology.html [Consultado 18/09/18]

Fruhlinger, Josh (2017). “What is Stuxnet, who created it and how does it work?”, en *CSO Online*. Disponible en: https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html [Consultado 16/10/18]

Fruhlinger, Josh (2018). “The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet”, en *CSO Online*. Disponible en: https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html [Consultado 23/08/18]

Gobierno de Estados Unidos (2010). *National Security Strategy.*

Gobierno de Estados Unidos (2017). *National Security Strategy.*

Goldsmith, Jack (2007). "Who Controls the Internet? Illusions of a Borderless World", *Strategic Direction*, 23(11). Disponible en: https://doi.org/10.1108/sd.2007.05623kae.001 [Consultado 03/10/18]

Goodin, Dan (2017). “NSA-leaking Shadow Brokers just dumped its most damaging release yet”, en *ARS Technica*. Disponible en: https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/ [Consultado 06/10/18]

Gordon, Philip H. (2007). “Can the War on Terror be Won?”, en *Brookings*. Disponible en: https://www.brookings.edu/articles/can-the-war-on-terror-be-won/ [Consultado 27/09/18]

Gostev, Alexander (2012). “The Flame: Questions and Answers”, en *Kaspersky Lab SecureList*. Disponible en: https://securelist.com/the-flame-questions-and-answers-51/34344/ [Consultado 17/10/18]

Graham, Chris (2017). “ NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history”, en *The Telegraph.* Disponible en: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/ [Consultado 28/08/18]

Greenberg, Andy (2012). “Anonymous Hackers Hit DOJ, FBI, Universal Music, MPAA And RIAA After MegaUpload Takedown”, en *Forbes*. Disponible en: https://www.forbes.com/sites/andygreenberg/2012/01/19/anonymous-hackers-claims-attack-on-doj-universal-music-and-riaa-after-megaupload-takedown/#4b28dda3c774 [Consultado 23/08/18]

Greenberg, Andy (2017). “‘Crash Override’: The malware that took down a power grid”, en *Wired*. Disponible en: https://www.wired.com/story/crash-override-malware/ [Consultado 26/09/18]

Guay, J. y Rudnick, L. (2017). “What the Digital Geneva Convention means for the future of humanitarian action”, en *United Nations High Commissioner for Refugees*. Disponible en: http://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/ [Consultado 09/10/18]

Hacquebord, Feike (2017). “How Cyber Propaganda Influenced Politics in 2016”, en *Trend Micro*. Disponible en: https://blog.trendmicro.com/trendlabs-security-intelligence/cyber-propaganda-influenced-politics-2016/ [Consultado 22/08/18]

Hoepman, J. y Jacobs, B. (2005). *Software Security Through Open Source*. Nijmegen: Institute for Computing and Information Sciences. Disponible en: https://www.cs.ru.nl/~jhh/publications/oss-acm.pdf [Consultado 04/10/18]

Hoffmann, Stanley (1991). "Sobre los orígenes de la Guerra Fría", en *Jano y Minerva*. Buenos Aires: Grupo Editor Latinoamericano.

Holland, Patrick (2017). "What is WikiLeaks?", en *CNET*. Disponible en: https://www.cnet.com/how-to/what-is-wikileaks/ [Consultado 10/09/18]

Internet Corporation for Assigned Names and Numbers (2012). *Resources for Country Code Managers*. Disponible en: https://www.icann.org/resources/pages/cctlds-21-2012-02-25-en [Consultado 18/08/18]

International Organization for Standarization (2018). *Country Codes - ISO 3166.* Disponible en: https://www.iso.org/iso-3166-country-codes.html [Consultado 18/08/18]

Internet World Stats (2017). *Internet Growth Statistics*. Disponible en: https://www.internetworldstats.com/emarketing.htm [Consultado 13/07/18]

Jané, Carmen (2017). "Un ataque informático masivo con 'ransomware' afecta a medio mundo", en *elPeriódico*. Disponible en: https://www.elperiodico.com/es/sociedad/20170512/un-ataque-informatico-masivo-infecta-a-las-grandes-empresas-de-espana-6033534 [Consultado 28/08/18]

Jargon File 4.4.7 (2003). Cra*cker*. Disponible en: http://catb.org/jargon/html/C/cracker.html [Consultado 10/08/18]

Jargon File 4.4.7 (2003). *Hacker*. Disponible en: http://catb.org/jargon/html/H/hacker.html [Consultado 10/08/18]

Jervis, Robert (1978). "Cooperation Under the Security Dilemma". En: *World Politics*, 30(2), pp. 167-214. Disponible en: http://www.jstor.org/stable/2009958 [Consultado 26/05/18]

Kabay, M. E. (1998). *Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy.* Munich: EICAR. Disponible en: http://www.mekabay.com/overviews/anonpseudo.htm [Consultado 02/09/18]

Katz, Yaakov (2010). "Stuxnet virus set back Iran's nuclear program by 2 years", en *The Jerusalem Post*. Disponible en: https://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years [Consultado 17/10/18]

Kingsbury, Alex (2010). “Documents Reveal Al Qaeda Cyberattacks”, en *US News*. Disponible en: https://www.usnews.com/news/articles/2010/04/14/documents-reveal-al-qaeda-cyberattacks [Consultado 25/09/18]

Knight, Shawn (2015). “Comcast using man-in-the-middle attack to warn subscribers of potential copyright infringement”, en *Techspot*. Disponible en: https://www.techspot.com/news/62887-comcast-/using-man-middle-attack-warn-//subscribers-potential.html [Consultado 05/11/18]

Koh, Harold H. (2010). *The Obama Administration and International Law*. Disponible en: https://2009-2017.state.gov/s/l/releases/remarks/139119.htm [Consultado 29/09/18]

Kumar, Mohit (2018). “TSMC Chip Maker Blames WannaCry Malware for Production Halt”, en *The Hacker News*. Disponible en: https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html [Consultado 28/08/18]

Kushner, David (2013). “The Real Story of Stuxnet”, en *IEEE Spectrum*. Disponible en: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet [Consultado 16/10/18]

Langner, Ralph (2013). *To Kill a Centrifuge. A Technical Analysis of What Stuxnet’s Creators Tried to Achieve*. Disponible en: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf [Consultado 16/10/18]

Larraz, Teresa (2010). “Spanish "botnet" potent enough to attack country: police”, en *Reuters*. Disponible en: https://www.reuters.com/article/us-crime-hackers/spanish-botnet-potent-enough-to-attack-country-police-idUSTRE6214ST20100303 [Consultado 04/08/18]

Lau, Mimi (2017). “Chinese police and petrol stations hit by ransomware attack”, en *South China Morning Post*. Disponible en: https://www.scmp.com/news/china/society/article/2094291/chinese-police-and-petrol-stations-hit-ransomware-attack [Consultado 28/08/18]

Lee, Dave (2012). “Flame: Attackers 'sought confidential Iran data'”, en *BBC*. Disponible en: https://www.bbc.com/news/technology-18324234 [Consultado 17/10/18]

Leiner, Barry (2009). “A Brief History of the Internet”, *ACM SIGCOMM Computer Communication Review*, 39(5). Barcelona. Disponible en:

https://www.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf [Consultado 26/07/18]

Lemos, Robert (2000). “Inside the ‘ILOVEYOU’ worm”, en *ZDNet News*. Disponible en: https://web.archive.org/web/20080428220655/http://news.zdnet.com/2100-9595_22-520463.html [Consultado 28/08/18]

Levy, Nat (2016). “Q&A: Cybersecurity expert explains the DNC email hack, and how you can prevent a similar attack”, en *GeekWire.* Disponible en: https://www.geekwire.com/2016/a-cyber-security-expert-explains-the-dnc-email-hack/ [Consultado 09/10/18]

Ley N.º 23.554 de Defensa Nacional. 1988. Argentina: Congreso de la Nación.

Leyden, John (2002). “Gummi bears defeat fingerprint sensors”, en *The Register.* Disponible en: https://www.theregister.co.uk/2002/05/16/gummi_bears_defeat_fingerprint_sensors/ [Consutlado 03/09/18]

Leyden, John (2003). “Help! my Belkin router is spamming me”, en *The Register*. Disponible en: https://www.theregister.co.uk/2003/11/07/help_my_belkin_router/ [Consultado 27/08/18]

Lueg, Christian (2018). “New malware every 10 seconds!”, en *G DATA Security Blog*. Disponible en: https://www.gdatasoftware.com/blog/2018/05/30735-new-malware-every-10-seconds [Consultado 28/08/18]

MacKenzie, D. y Wajcman, J. (1999). *The social shaping of technology.* Buckingham: Open University Press.

Maloney, Sarah (2017). “Attack attribution: it’s complicated”, en *Cybereason*. Disponible en: https://www.cybereason.com/blog/attack-attribution-its-complicated [Consultado 03/08/18]

Mari, Angelica (2018). “Brazilian federal government leads in open source adoption”, en *ZDNET.* Disponible en: https://www.zdnet.com/article/brazilian-federal-government-leads-in-open-source-adoption/ [Consultado 09/10/18]

Markoff, John (2008). “Before the Gunfire, Cyberattacks”, en *The New York Times*. Disponible en: https://www.nytimes.com/2008/08/13/technology/13cyber.html [Consultado 24/10/18]

Markoff, J. y Kramer, A. (2009). “U.S. and Russia differ on a Treaty for Cyberspace”, en *The New York Times*. Disponible en:

https://www.nytimes.com/2009/06/28/world/28cyber.html [Consultado 09/10/18]

Mastanduno, Michael (1997). “Preserving the Unipolar Moment: Realist Theories and U.S. Grand Strategy after the Cold War”. En: The MIT Press (1997). *International Security*, Vol. 21, No. 4. pp. 49-88.

Masters, Jonathan (2014). “What is Internet Governance?”, en *Council on Foreign Relations*. Disponible en: https://www.cfr.org/backgrounder/what-internet-governance [Consultado 03/10/18]

Menn, Joseph (2011). “Agreement on cybersecurity ‘badly needed’”, en *Financial Times*. Disponible en: https://www.ft.com/content/e595e568-f4dc-11e0-ba2d-00144feab49a [Consultado 03/10/18]

Meyer, David (2013). “Nokia: Yes, we decrypt your HTTPS data, but don’t worry about it”, en *Gigaom*. Disponible en: https://gigaom.com/2013/01/10/nokia-yes-we-decrypt-your-https-data-but-dont-worry-about-it/ [Consultado 27/08/18]

Microsoft (2018). “A Digital Geneva Convention to protect cyberspace”, en *Microsoft Policy Papers*. Disponible en: https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace [Consultado 09/10/18]

Micro Trend (2017). *2017’s Notable Vulnerabilities and Exploits*. Disponible en: https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/2017-notable-vulnerabilities-and-exploits [Consultado 28/08/18]

Miller, Daniel (2018). “The Weakest Link: The Role of Human Error in Cybersecurity”, en *SecureWorld*. Disponible en: https://www.secureworldexpo.com/industry-news/weakest-link-human-error-in-cybersecurity [Consultado 09/10/18]

Millman, Rene (2017). “Luxembourg government servers forced offline by DDoS attack”, en *SC Media UK*. Disponible en: https://www.scmagazineuk.com/luxembourg-government-servers-forced-offline-ddos-attack/article/1475172 [Consultado 23/08/18]

Miessler, Daniel (2009). *Obscurity ia a Valid Security Layer*. Disponible en: https://danielmiessler.com/study/security-by-obscurity/ [Consultado 10/09/18]

Moir, Robert (2003). “ Defining Malware: FAQ”, en *Microsoft TechNet. Disponible* en: https://technet.microsoft.com/en-us/library/dd632948.aspx [Consultado 27/08/18]

Moore, Scott M. (2010). “International Treaties and the Internet”, en *Pacific Standard*. Disponible en: https://psmag.com/news/international-treaties-and-the-internet-22622 [Consultado 09/10/18]

Morgan, Steve (2016). “One million cybersecurity job openings in 2016”, en *Forbes Tech*. Disponible en: https://pcage.edu/wp-content/uploads/2017/04/Forbes-Cybersecurity-Article-1.pdf [Consultado 01/10/18]

Moyer, Edward (2013). “NSA disguised itself as Google to spy, say reports”, en *CNET.* Disponible en: https://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports/ [Consultado 27/08/18]

Naciones Unidas (1945). “Capítulo VII”, en *Carta de las Naciones Unidas.* Disponible en: https://www.un.org/es/sections/un-charter/chapter-vii/index.html [Consultado 26/09/18]

Nakamura, D. y Phillip, A. (2017). “Trump Acknowledges Russian Involvement in Meddling in U.S. Elections”, en *The Washington Post.* Disponible en: https://www.washingtonpost.com/politics/trump-cites-kremlin-statement-to-deny-reports-of-russia-ties-asks-if-we-are-living-in-nazi-germany/2017/01/11/a710f2b4-d777-11e6-b8b2-cb5164beba6b_story.html?noredirect=on&utm_term=.49f3faa05acc [Consultado 05/08/18]

Nakashima, E. y Warrick, J. (2012). “Stuxnet was work of U.S. and Israeli experts, officials say”, en *The Washington Post*. Disponible en: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html [Consultado 16/10/18]

Nakashima, E., Miller, G. y Tate, J. (2012). “ U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say”, en *The Washington Post*. Disponible en: https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?noredirect=on&utm_term=.9bc7353042c8 [Consultado 17/10/18]

Nakashima, Ellen (2016). “Obama to be urged to split cyberwar command from NSA”, en *The Washington Post.* Disponible en: https://www.washingtonpost.com/world/national-security/obama-to-be-urged-to-split-cyberwar-command-from-the-nsa/2016/09/12/0ad09a22-788f-11e6-ac8e-

cf8e0dd91dc7_story.html?noredirect=on&utm_term=.f7cf0ea82cf7 [Consultado 15/10/18]

Naraine, Ryan (2010). “Stuxnet attackers used 4 Windows zero-day exploits”, en *ZDNet*. Disponible en: https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/ [Consultado 06/10/18]

National Cybersecurity and Communications Integration Center (2009). *Security Tip (ST04-015): Understanding Denial-of-Service Attacks*. Disponible en: https://www.us-cert.gov/ncas/tips/ST04-015 [Consultado 23/08/18]

Neira, Javier (2017). “Hackeo mundial a empresas: Confirman 150 detecciones de virus en Chile y Gobierno monitorea efectos”, en *Emol*. Disponible en: http://www.emol.com/noticias/Tecnologia/2017/05/12/858129/Ministerio-del-Interior-confirma-monitoreo-de-masivo-ataque-cibernetico-y-estudia-efectos-en-el-pais.html [Consultado 28/08/18]

Newton, Casey (2018). “The case that Russia is winning the cyberwar”, en *The Verge*. Disponible en: https://www.theverge.com/2018/9/25/17898804/cyberwar-kathleen-hall-jamieson-russia-election-interference [Consultado 24/10/18]

Nievas, Flabián (2015). “Terrorismo: en búsqueda del concepto”, en *Cuadernos de Marte. Revista latinoamericana de Sociología de la Guerra*. Buenos Aires: Universidad de Buenos Aires.

Nolan, Laura (1999). *The Computer, like all Technology, is Neutral. The Case Against this Statement*. Disponible en: https://www.scss.tcd.ie/tangney/ComputersAndSociety/99/StdPapers/P3-Revisited/ln.html [Consultado 26/09/18]

Nye, Joseph (2010). *Cyber Power*. Cambridge: Harvard Kennedy School. Disponible en: http://www.dtic.mil/dtic/tr/fulltext/u2/a522626.pdf [Consultado 25/10/18]

Nye, Joseph (2011). “Nuclear Lessons for Cyber Security?”, en *Strategic Studies Quarterly*, 5(4), pp. 18-38. Disponible en: *https://citizenlab.ca/cybernorms2012/nuclearlessons.pdf* [Consultado 29/09/18]

Perlroth, N. y Hardy, Q. (2013). “Bank Hacking Was the Work of Iranians, Officials Say”, en *The New York Times*. Disponible en: https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html [Consultado 23/08/18]

Petallides, Contastine J. (2012a). “Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat”, *Inquiries Journal*. Disponible

en: http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat [Consultado 16/05/18]

Petallides, Constantine J. (2012b). “Cracking the Digital Vault: A Study of Cyber Espionage”, en *Inquiries Journal*. 4(04). Disponible en: http://www.inquiriesjournal.com/articles/629/2/cracking-the-digital-vault-a-study-of-cyber-espionage [Consultado 12/09/18]

Piscitello, Dave (2015). “¿Qué es un ataque de intermediarios?, en *ICANN Blog*. Disponible en: https://www.icann.org/news/blog/que-es-un-ataque-de-intermediarios [Consultado 27/08/18]

Post, David (1995). “Anarchy State and the Internet”, *Journal of Online Law*, 3. Disponible en: https://ssrn.com/abstract=943456 [Consultado 03/10/18]

Prince, Brian (2010). “Defense Department Confirms Critical Cyber-attack”, en *eWeek*. Disponible en: http://www.eweek.com/security/defense-department-confirms-critical-cyber-attack [Consultado 09/10/18]

Protectimus (2018). *Cybersecurity vs. Information Security*. Disponible en: https://www.protectimus.com/blog/cybersecurity-vs-infosec/ [Consultado 22/08/18]

Radware (2018). *Operation Ababil DDoS Attacks*. Disponible en: https://security.radware.com/ddos-experts-insider/expert-talk/ddos-attacks-operation-ababil/ [Consultado 23/08/18]

Rea, Kari (2013). “Glenn Greenwald: Low-Level NSA Analyst Have ‘Powerful and Invasive’ Search Tool”, en *abcNews*. Disponible en: https://abcnews.go.com/blogs/politics/2013/07/glenn-greenwald-low-level-nsa-analysts-have-powerful-and-invasive-search-tool/ [Consultado 13/09/18]

Reardon, R. & Choucri, N. (2012). “The Role of Cyberspace in International Relations: A View of the Literature”, *2012 ISA Annual Convention*. MIT: San Diego. Disponible en: https://ecir.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf [Consultado 23/06/18]

Real Academia Española (2018). *Criptografía.* Disponible en: http://dle.rae.es/srv/search?m=30&w=criptograf%C3%ADa [Consultado 27/08/18]

Reed, John (2013). “U.S. Gov’t: Laws of war apply to cyber conflict”, en *Foreign Policy.* Disponible en: *https://foreignpolicy.com/2013/03/25/u-s-govt-laws-of-war-apply-to-cyber-conflict/* [Consultado 29/09/18]

Rice, Condolezza (2008). “Rethinking the National Interest. American Realism for a New World”, en *Foreign Affairs*. Disponible en: https://www.foreignaffairs.com/articles/2008-06-01/rethinking-national-interest [Consultado 16/10/18]

Risen, J. y Lichtblau, E. (2005). “Bush Lets U.S. Spy on Callers Without Courts”, en *The New York Times*. Disponible en: https://web.archive.org/web/20060206162614/http://www.commondreams.org/headlines05/1216-01.htm [Consultado 14/09/18]

Ross, Alec (2014). “Russia’s cyber weapons hit Ukraine: How to declare war without declaring war”, en *The CS Monitor’s Global Viewpoint*. Disponible en: www.csmonitor.com/Commentary/Global-Viewpoint/2014/0312/Russia-s-cyber-weapons-hit-Ukraine-How-to-declare-war-without-declaring-war [Consultado 24/10/18]

Saint Pierre, Héctor (2003). “¿Guerra de todos contra quién? La necesidad de definir terrorismo”, en López, Ernesto (comp.), *Escritos sobre terorrismo*. Buenos Aires: Prometeo, pp. 47-75.

Saint-Pierre, Héctor (2012), “Fundamentos para pensar la distinción entre defensa y seguridad”, en RESDAL (Ed.). *Atlas comparativo de la Defensa en América Latina y el Caribe*. Buenos Aires: RESDAL.

Sanger, David (2012). “Obama Order Sped Up Wave of Cyberattacks Against Iran”, en *The New York Times*. Disponible en: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 [Consultado 17/10/18]

Schatz, D., Bashroush, R., y Wall, J. (2017). "Towards a More Representative Definition of Cyber Security". *Journal of Digital Forensics, Security and Law,* 12(2). Disponible en: https://commons.erau.edu/cgi/viewcontent.cgi?article=1476&context=jdfsl

Schneier, Bruce (2005). “Sony's DRM Rootkit: The Real Story”, en *Wired.com*. Disponible en: https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html [Consultado 28/08/18]

Schneier, Bruce (2015). “Attack Attribution in Cyberspace”, en *Time*. Disponible en: https://www.schneier.com/blog/archives/2015/01/attack_attribut.html [Consultado 03/09/18]

Scott, Mike (2014). “Clandestine Fox, Part Deux”, en *FireEye Blog*. Disponible en: https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html [Consultado 23/10/18]

Secureworks (2016). *Threat Group-4127 Targets Hillary Clinton Presidential Campaign*. Disponible en: https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign [Consultado 20/08/18]

Segal, Adam (2017). “ How China is preparing for cyberwar”, en *The CS Monitor’s Passcode*. Disponible en: https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar [Consultado 20/10/18]

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Nueva York: Oxford University Press.

Singh, U. y Mardini, A. (2011). “Some weekend work that will (hopefully) enable more Egyptians to be heard”, en *Google Official Blog*. Disponible en: https://googleblog.blogspot.com/2011/01/some-weekend-work-that-will-hopefully.html [Consultado 17/09/18]

Sistema Operativo GNU (2018a). *¿Qué es el software libre?* Disponible en: https://www.gnu.org/philosophy/free-sw.es.html [Consultado 27/08/18]

Sistema Operativo GNU (2018b). *El software privativo es a menudo malware*. Disponible en: https://www.gnu.org/proprietary/proprietary.html [Consultado 28/08/18]

Sistema Operativo GNU (2018c). “Why C programming language?”, en GNU Astronomy Utilities Manual, v. 0.7. Disponible en: https://www.gnu.org/software/gnuastro/manual/html_node/Why-C.html [Consultado 26/09/18]

Shopify (2017). *Global Ecommerce: Statistics and International Growth Trends*. Disponible en: https://www.shopify.com/enterprise/global-ecommerce-statistics [Consultado 14/08/18]

Spiegel Online (2007). *Soviet Memorial Causes Rift between Estonia and Russia*. Disponible en: http://www.spiegel.de/international/europe/deadly-riots-in-tallinn-soviet-memorial-causes-rift-between-estonia-and-russia-a-479809.html [Consultado 24/10/18]

Sullivan, Dan (2011). “Beyond the Hype: Advanced Persistent Threats”, en *Advanced Persistent Threats and Real Time Threat Management. The Essential Series*. Realtime Publishers.

Sridhar, S., Altinkemer, K., y Rees, J. (2005). “Software Vulnerabilities: Open Source versus Proprietary Software Security”, en *AMCIS 2005 Proceedings*, 428. Disponible en: http://aisel.aisnet.org/amcis2005/428 [Consultado 28/08/18]

Stamp, M y Stavroulakis, P. (2010). “Phishing Attacks and Countermeasures”, en *Handbook of Information and Communication Security.* Berlin: Springer Science & Business Media.

Stone, Jeff (2016). “ Meet Fancy Bear and Cozy Bear, Russian groups blamed for DNC hack”, en *The CS Monitor's Passcode*. Disponible en: https://www.csmonitor.com/World/Passcode/2016/0615/Meet-Fancy-Bear-and-Cozy-Bear-Russian-groups-blamed-for-DNC-hack [Consultado 24/10/18]

Symantec (2011). *Advanced Persistent Threats: A Symantec Perspective.* Mountain View: Symantec Corporation.

The Economist (2017). *Where are the flaws in two-factor authentication?* Disponible en: https://www.economist.com/the-economist-explains/2017/09/13/where-are-the-flaws-in-two-factor-authentication [Consultado 02/09/18]

The White House (2011). *International Strategy for Cyberspace*. Prosperity, Security, and Openness in a Networked World. Disponible en: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Consultado 26/09/18]

The White House (2017). *Statement by President Donald J. Trump on the Elevation of Cyber Command.* Disponible en: https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-/elevation-cyber-command/ [Consultado 16/10/18]

Thornett, Chris (2018). “German government goes open source with cloud firm Nextcloud”, en *TechRadar*. Disponible en: https://www.techradar.com/news/german-government-goes-open-source-with-open-source-cloud-firm-nextcloud [Consultado 09/10/18]

Traynor, Ian (2007). “Russia accused of unleashing cyberwar to disable Estonia”, en The Guardian. Disponible en: https://www.theguardian.com/world/2007/may/17/topstories3.russia [Consultado 24/10/18]

Turley, Jonathan (2014). “Big money behind war: the military-industrial complex”, en *Al Jazeera*. Disponible en: https://www.aljazeera.com/indepth/opinion/2014/01/big-money-behind-war-military-industrial-complex-20141473026736533.html [Consultado 01/10/18]

Tuthill, David P. (2012). *Reimagining Waltz in a Digital World: Neorealsim in the Analysis of Cyber Security Threats and Policy.* Canterbury: University of Kent.

Universidad de Indiana (2018). *About viruses, worms and Trojan horses.* Disponible en: https://kb.iu.edu/d/aehm [Consultado 28/08/18]

Universidad de Yale (2017). *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*. Connecticut: Center for Global Legal Challenges. Disponible en: https://law.yale.edu/system/files/area/center/global/document/2017.05.10_-_law_of_attribution.pdf [Consultado 03/09/18]

Vaughan-Nichols, Steven (2017). “Linux totally dominates supercomputers”, en *ZDNet*. Disponible en: https://www.zdnet.com/article/linux-totally-dominates-supercomputers/ [Consultado 09/10/18]

Walt, Stephen M. (2010). “Is the cyber threat overblown?”, en *Foreign Affairs*. Disponible en: https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/ [Consultado 29/09/18]

Waltz, Kenneth (1988). *Teoría de la Política Internacional*. Buenos Aires: Grupo Editor Latinoamericano, pp. 119-150.

Watercutter, Angela (2013). “Why Free Software is more important now than ever before”, en *Wired*. Disponible en: https://www.wired.com/2013/09/why-free-software-is-more-important-now-than-ever-before/ [Consultado 08/10/18]

Wei, Chun Chew (2018). “How It Works: Great Firewall of China”, en *Medium*. Disponible en: https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475 [Consultado 20/10/18]

Wheeler, David A. (2013). What is Open Security?. Virginia: Institute for Defense Analyses. Disponible en: http://www.dtic.mil/dtic/tr/fulltext/u2/a607073.pdf [Consultado 10/09/18]

Whittaker, Zack (2013). “PRISM: Here’s how the NSA wiretapped the Internet”, en *ZDNet*. Disponible en: https://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/ [Consultado 13/09/18]

Wikimedia Commons (2007). Arpanet in 1974. Disponible en: https://en.wikipedia.org/wiki/File:Arpanet_1974.svg [Consultado 27/08/18]

Williams, Owen (2015). “Lenovo caught installing adware on new computers”, en *The Next Web*. Disponible en: https://thenextweb.com/insider/2015/02/19/lenovo-caught-installing-adware-new-computers/ [Consultado 27/08/18]

Wilson, Clay (2005). “Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress”, en *Congressional Research Service Reports for Congress*. Washington: Library of Congress.

WSIS (2005). “Tunis Agenda for the Information Society”, en *World Summit on the Information Society*. Disponible en: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html [Consultado 04/10/18]

Yeo, Vivian (2010). “Stuxnet infections spread to 115 countries”, en *ZDNet*. Disponible en: https://www.zdnet.com/article/stuxnet-infections-spread-to-115-countries/ [Consultado 28/10/18]

Zetter, Kim (2011). “How digital detectives deciphered Stuxnet, the most menacing malware in history”, en *Wired*. Disponible en: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/ [Consultado 20/10/18]

Zetter, Kim (2012). “Meet ‘Flame’, the massive spy malware infiltrating iranian computers”, en *Wired*. Disponible en: https://www.wired.com/2012/05/flame/ [Consultado 16/10/18]