La geopolítica y el complejo cyber industrial

Gabriela Coloma, Gian Tituaña, Francisco Alarcón, Andrés Bohórquez

Introducción

El libro 'This is How They Tell Me the World Ends' fue escrito por Nicole Perlroth, una periodista de ciberseguridad y ciberespionaje del The New York Times. En este libro, la autora investiga los orígenes y la evolución de la carrera armamentística cibernética, enfocándose en el lucrativo y oscuro mercado de vulnerabilidades de software (zero-days). La autora analiza cómo la búsqueda de superioridad cibernética ha reconfigurado la geopolítica global, dando lugar a lo que se describe como un 'Complejo Ciberindustrial'. Esta introducción se enfoca en desglosar la intersección crítica entre geopolítica, poder cibernético y seguridad nacional que el libro expone, sentando las bases para entender la actual competencia entre estados.

A lo largo del libro, la autora se enfoca en presentar diversos acontecimientos relacionados con el desarrollo de la ciberseguridad en Estados Unidos para combatir los ataques cibernéticos de otras naciones como la Unión Soviética en su momento y actualmente Rusia, China, Irán, entre otros. Entre las perspectivas fundamentales para el relato destacan la geopolítica y el complejo ciberindustrial (Cyber-Industrial Complex).

Uno de los puntos desarrollados para la geopolítica es la evolución del poder cibernético debido a los avances de la tecnología que desencadeno en la adaptación de cada una de las naciones a los últimos cambios en el intercambio de la información. Estados Unidos fue el ejemplo perfecto, al tener en un inicio un modelo pasivo en su Agencia de Seguridad Nacional (NSA) de esperar que las comunicaciones soviéticas llegaran a su sistema global de recopilación. Sin embargo, la espera no era suficiente debido a la migración de la información desde distintos dispositivos electrónicos hasta el internet. Volúmenes exuberantes de secretos de estado estaban siendo transmitidos en unos y ceros, y estaban disponibles para cualquier individuo con las capacidades necesarias para encontrarlo. Por esta razón, otras naciones desarrollaran sus capacidades de interceptación digital para tener una amplia ventaja en la guerra (Perlroth, 2021, pp. 93-94). A partir de este punto, surgiría la necesidad de adaptarse a las nuevas metodologías por las que se comunicaban las naciones y

encontrar una forma de interceptar la información discretamente, dando mayor importancia al poder cibernético debido a que la nación con mayor superioridad era aquella que lograra mantener su ventaja sobre las comunicaciones.

Del mismo modo, el enfoque del poder cibernético se relaciona estrechamente con la seguridad nacional dado que, así como las naciones estaban desarrollando su poder cibernético, debían adaptarse a los nuevos ataques que surgían. Las naciones crearon sus propios departamentos o agencias destinadas a mantener la seguridad nacional y el poder cibernético. Para ello, los involucrados eran expertos en temas relacionados con el hackeo o con los ataques de zero-days, que dominaban el mercado y serían los fundamentos para el desarrollo de armas cibernéticas. Asimismo, estos grupos eran considerados el "lado oscuro" de las naciones debido a lo cuestionable que era trabajar con métodos poco éticos como lo es el hackeo y programar armas para afectar a otras naciones. En este ámbito, la autora menciona la creación del lado oscuro de la NSA, conformada por la combinación de los trabajos clandestinos y conocida como la división de piratería informática de élite de la agencia denominada TAO (Perlroth, 2021, pp.100-101). La creación de este 'lado oscuro' institucionalizado plantea un profundo dilema ético y legal para las democracias: ¿hasta qué punto deben adoptar tácticas opacas y potencialmente ilegales para defender la seguridad nacional? El libro sugiere que esta elección, si bien comprensible desde una perspectiva de realismo geopolítico, erosiona los principios de transparencia y, paradójicamente, debilita la seguridad general de Internet al fomentar la acumulación y posterior filtración de herramientas de hackeo.

La carrera por el dominio cibernético se libró como un método de desmoralización adecuada para la era digital, dando origen al término destrucción mutuamente asegurada (mutually assured disruption) en el ciberespacio. El libro ilustra cómo este concepto surgió como una lógica estratégica entre potencias. Por un lado, muestra cómo Rusia, tras infiltrarse en los sistemas de control industrial de empresas de energía, presas y la red eléctrica de Estados Unidos, estaba "preparando el campo de batalla". Esta capacidad de causar daño físico masivo y prolongado a través de cortes de energía que podrían durar meses o años, funcionaba como una advertencia clara: si Washington actuaba contra sus intereses (como en la anexión de Crimea), Moscú podría responder con un ataque devastador a la infraestructura crítica. Esta dinámica, como señala la autora, era "destrucción mutuamente asegurada para la era de internet" (Perlroth, 2021, pp. 282-283). Por otro lado, este equilibrio del terror digital

se manifestó en tiempo real durante la escalada entre Estados Unidos e Irán. Mientras hackers iraníes atacaban infraestructura energética estadounidense, Estados Unidos ya tenía activos programas ofensivos como *Nitro Zeus*, con "bombas de tiempo" digitales instaladas en sistemas iraníes. Esta situación creó un escenario en el que, como observa Perlroth, "lo que la comunidad de seguridad presenció ese verano fue, en efecto, la destrucción mutuamente asegurada en tiempo real" (Perlroth, 2021, pp. 343-345). La advertencia del General Keith Alexander, arquitecto de Stuxnet, resume la paradoja de esta disuasión: "Tenemos un muy buen ataque, pero ellos también... y desafortunadamente, nosotros tenemos más que perder" (Perlroth, 2021, p. 343). Por esta razón, el poder cibernético no solo otorga capacidad ofensiva, sino que genera una vulnerabilidad compartida y una frágil estabilidad basada en la amenaza de una escalada catastrófica.

Otro motivo de la importancia de la seguridad nacional surge como una respuesta al uso de los mismos dispositivos cibernéticos por parte de cada nación que, en lugar de buscar avanzar de forma individual, se empezó a crear un estándar de los objetos que todos debían utilizar debido a su funcionalidad basta y confiable. De igual manera, todas las naciones ahora tenían los mismos objetivos que consistían principalmente en que “cada nación se enfocaba en el espionaje” y como todas las naciones disponían de una tecnología similar, encontrar una vulnerabilidad podría ser una forma de atacar otras naciones o de poder encontrar una solución y proteger a la propia nación de ataques enemigos que descubrieran la vulnerabilidad con anterioridad (Perlroth, 2021, p. 298). Además, encontrar un error y arreglarlo no garantizaba que no podría existir más errores, impulsando un mercado para descubrir estas vulnerabilidades y venderlas como una forma de aprender para defenderse o atacar, un punto que se tratará más adelante. Un ejemplo propio del libro con respecto a los errores es Linux pues el avance del código base desde miles a millones de líneas, involucra que, en cada implementación de una funcionalidad nueva, pueden surgir nuevos errores y al ser tantas líneas, es casi imposible descubrir todos los posibles errores (Perlroth, 2021, p. 99)

En conclusión, la dinámica geopolítica contemporánea está irremediablemente ligada a la competencia por el poder cibernético, donde la seguridad nacional se redefine en términos de capacidades ofensivas y defensivas en un entorno sin fronteras. Para comprender las implicaciones concretas de esta rivalidad, el siguiente apartado presenta un análisis comparativo de las capacidades y estrategias cibernéticas de Estados Unidos, China y Rusia,

seguido de un examen crítico de la proliferación global de herramientas ofensivas y su impacto desestabilizador y una simulación de escalada en un conflicto geopolítico.

Capacidades y estrategias cibernéticas de distintos países

A continuación, nos centraremos en analizar las capacidades cibernéticas de algunos de los países mencionados en el libro. Los países en los que nos enfocaremos serán Estados Unidos, Rusia, China e Israel. La elección de estas cuatro naciones tiene que ver con el hecho de que son actores sumamente importantes en el panorama de la ciberseguridad a nivel mundial, no solo por sus capacidades cibernéticas, sino también por las estrategias (ofensivas, defensivas) que utilizan para asegurar su participación en la industria cibernética global.

En primer lugar, en Estados Unidos tenemos a la NSA (National Security Agency), que es una agencia de inteligencia muy importante en Estados Unidos cuya misión es recopilar inteligencia extranjera y defender secretos nacionales. La agencia pasó interceptar señales a hackear puntos finales (dispositivos) gracias al auge de la encriptación y la fibra óptica. Esta agencia es conocida por sus presupuestos millonarios que suelen utilizarse para la compra de exploits a actores privados (Perlroth, 2021, pp. 30). Ahora bien, dentro de la NSA encontramos a TAO (Tailored Access Operations), que es la unidad de élite de hackers dentro de la agencia. Estos operan dentro del centro de operaciones remotas en Fort Meade (Perlroth, 2021, pp. 101). TAO se especializa en penetrar objetivos difíciles como terroristas, líderes extranjeros, etc., y son conocidos por desarrollar y mantener un catálogo masivo de exploits (Perlroth, 2021, pp. 117-118).

Asimismo, dentro de la NSA existe el Q Group que es la división de contrainteligencia cuya función principal es vigilar a sus propios espías para detectar posibles filtraciones. Este grupo fue útil durante la investigación de The Shadow Brokers quienes filtraron herramientas de la NSA (Perlroth, 2021, pp. 316). Otro actor estadounidense para la seguridad es Sandia National Laboratories, que tradicionalmente están asociados con la seguridad nuclear pero que fueron la cuna de la ciberseguridad ofensiva moderna de Estados Unidos, en la cual destaca la figura de James Gosler considerado como el padrino de la ciberguerra estadounidenses. Sandia estableció una relación estratégica con la NSA, realizando trabajos clasificados de explotación y vulnerabilidad de hardware y software para la agencia (Perlroth, 2021, pp. 95). Respecto a contratistas de defensa que colaboran con el gobierno estadounidense destacan VRL (Vulnerability Research Labs) y Cyberpoint. Por un lado, VRL es una empresa contratista de defensa descrita como una "tienda boutique de

exploits zero-day". Fue fundada por cinco ex-hackers de élite de la NSA (The Maryland Five) que dejaron la agencia en 2008, y se especializan en militarizar zero-days y vender herramientas de espionaje exclusivamente a agencias gubernamentales de Estados Unidos y a los socios de "Five Eyes" (Perlroth, 2021, pp. 148-154). Por otro lado, Cyberpoint es un contratista de seguridad que representa el lado mercenario y controvertido de la industria. Cyberpoint se expandió para trabajar con gobiernos extranjeros, específicamente los Emiratos Árabes Unidos (EAU), desde donde reclutaron ex-hackers de la NSA con salarios exorbitantes para trabajar en Abu Dabi. El problema con este grupo es que terminaron vigilando a disidentes, periodistas, activistas de derechos humanos e incluso hackeando a ciudadanos estadounidenses (Perlroth, 2021, pp. 164).

Estados Unidos siempre busca el dominio total sobre los exploits más avanzados y destructivos. En general, se basa en la política de NOBUS ("Nobody But Us") la cual busca retener vulnerabilidades de software (zero-days) en lugar de reportarlas para su corrección, bajo la premisa de que solo la NSA tiene la sofisticación técnica para encontrarlas y explotarlas (Perlroth, 2021, pp. 146). Con este tipo de armas, TAO se enfocó en realizar implantes masivos. Pasó de objetivos específicos a una explotación a escala industrial, por ejemplo, con el programa Genie gestionaba 85000 implantes en 2013, con planes de llegar a millones (Perlroth, 2021, pp. 123-124). Asimismo, para asegurar de la NSA pudiera explotar sistemas comerciales desarrollaron el SIGINT Enabling Project, gracias al cual la agencia podría influir en los estándares de encriptación internacionales (haciéndolos más débiles), colaborar con fabricantes de chips para introducir puertas traseras, e interceptar equipos físicos en tránsito para instalar programa maligno antes de que lleguen al objetivo (Perlroth, 2021, pp. 107).

Debido a la gran cantidad de vulnerabilidades que Estados Unidos posee se creó el Vulnerability Equities Process (VEP) el cual es el proceso liderado por la Casa Blanca para decidir si una vulnerabilidad zero-day descubierta por el gobierno debe ser revelada al fabricante para ser parchada o retenida para operaciones de espionaje ofensivo. Sin embargo, la retención de exploits como EternalBlue durante más de cinco años, que luego fueron robados y usados en ataques globales como WannaCry y NotPetya, demuestra las fallas de este cálculo (Perlroth, 2021, pp. 296, 324-329). Finalmente, ante la incapacidad de proteger todos los sistemas, el gobierno y empresas privadas comenzaron a pagar a hackers para encontrar fallos de seguridad a través de programas de recompensas. Esta estrategia enfrenta un problema económico y es que el mercado negro paga sumas mucho mayores por los

zero-days para uso ofensivo que lo que las empresas o programas defensivos ofrecen por arreglarlos.

En Rusia, la Unidad 74455 (Sandworm), es una unidad del GRU (Dirección de inteligencia del estado mayor ruso) y es responsable de algunos de los ataques más destructivos y agresivos como el de los apagones en Ucrania en 2015 (Perlroth, 2021, pp. 285-290). Asimismo, se le atribuye el ataque de NotPetya de 2017 donde se utilizó el exploit robado del a NSA Eternal Blue para paralizar sistemas globales. Además, esta unidad ha estado infiltrado en los servicios públicos de Estados Unidos especialmente aquellos que tienen que ver con software de sistemas de control industrial (Perlroth, 2021, pp. 316).

Otro actor ruso importante es el conocido como Fancy Bear (GRU Unit 26165), que se especializa sobre todo en espionaje de alto perfil y robo de credenciales. Esta unidad fue la responsable de la infiltración en los servidores del partido demócrata estadounidense en 2016 a través de un correo de phishing. En general, se enfocan en atacar periodistas, políticos, etc (Perlroth, 2021, pp. 303, 441). Ahora bien, IRA (Internet Research Agency) aunque no se especializa como tal en ataques informáticos tiene un papel importante en la guerra de la información. Aquí aparecen los famoso trolls rusos que crea cuentas falsas en redes sociales para exacerbar divisiones políticas o raciales especialmente en Estados Unidos (Perlroth, 2021, pp. 301, 302). Finalmente, tenemos al FSB (Servicio Federal de Seguridad), que viene a ser el sucesor de la extinta KGB, y que ha integrado a cibercriminales en sus operaciones de inteligencia. Esto permite que el régimen ruso trabaje con cárteles cibernéticos, protegiéndolos a cambio de acceso a sus víctimas y herramientas. Como se menciona en el capítulo 23 del libro, el FSB colaboró con cibercriminales para hackear millones de cuentas de Yahoo (Perlroth, 2021, pp. 308-309, 353).

Rusia en general lo que busca es una infiltración profunda en Estados Unidos, desde tomar control dentro de redes de plantas nucleares, hasta la red eléctrica, conel objetivo de tener la capacidad de sabotear o apagar el suministro eléctrico. Asimismo, han comprometido cadenas de suministro como proveedores de software de control industrial para infectar los objetivos con virus troyanos para tener acceso a oleoductos, represas o la red eléctrica. Otra de sus estrategias es la interferencia electoral la cual busca sembrar caos en países como Estados Unidos. Esto lo logran infiltrándose en sistemas de registro de votantes y robando sus datos, así como hackear empresas que proporcionan software para los libros de votación electrónica en ciertos estados. El robo y filtrado de información es otro de sus fundamentos

para operar. Esto se evidenció sobre todo con los ataques hacia el partido demócrata estadounidense, filtrando correos e información comprometedora para generar discordia entre sus miembros (Perlroth, 2021, pp. 307). Finalmente, la manipulación social que ejerce Rusia a través de agencias como IRA promueve protestas y enfrentamientos en suelo estadounidense. No solo haciendo propaganda hacia ciertos candidatos sino también creando noticias falsas desde cero para ampliar la desinformación y teorías de conspiración generadas por los propios estadounidenses (Perlroth, 2021, pp. 305, 349).

En China, encontramos al PLA (People's Liberation Army), cuyas cruzadas de hacking eran conducidas por el Segundo y Tercer Departamento del PLA. Distintas unidades tenían como objetivo hackear gobiernos extranjeros en ciertas zonas geográficas o robar propiedad intelectual de industrias concretas para beneficiar a las empresas estatales chinas y sus planes económicos (Perlroth, 2021, pp. 201). Dentro del PLA encontramos a la Unidad 61398, una de las unidades de hacking más exitosas dentro del ejército chino. Lo que hacían era lanzar miles de ataques contra empresas estadounidenses, entre las que destacan Coca-Cola, la empresa de seguridad RSA y el contratista de defensa Lockheed Martin. Sin embargo, en 2013 fueron expuestos por Estados Unidos, lo que llevó a que el departamento de justicia imputara a cinco miembros de la unidad, poniéndolos en la lista de los más buscados del FBI (Perlroth, 2021, pp. 267).

Ahora bien, en relación con algunas "legiones" dedicadas a atacar a empresas estadounidenses podemos destacar a Legion Yankee y a Legion Amber. Respecto a Legion Yankee, podemos destacar que fueron un grupo de contratistas del gobierno chino responsable de ataques altamente sofisticados, incluyendo el ataque a Google en 2009 (Operación Aurora). Además de Google, atacaron a varias empresas de Silicon Valley, contratistas de defensa y firmas financieras. Al parecer, lo que buscaban era el código fuente de estas empresas y acceder a cuentas de gmail de disidentes chinos (Perlroth, 2021, pp. 203-204). Respecto a Legion Amber, se sabe que operaban desde Guangzhou, China. Este grupo robó las armas del hacking de la NSA y las utilizaron para sus propios ataques. Su lista de objetivos incluía contratistas de defensa de Estados Unidos, desarrolladores de armas y laboratorios de investigación científica. Incluso llegaron a robar tecnologías aeroespaciales, satelitales y tecnología nuclear que permitió a China avanzar décadas en su desarrollo nuclear (Perlroth, 2021, pp. 340-341).

Lo que busca China básicamente es poder igualar el desarrollo tecnológico y económico de países como Estados Unidos. China utiliza su aparato de inteligencia para beneficio económico directo de sus industrias. Para ello una de sus principales estrategias es el ciberespionaje económico, cuyo objetivo es el robo masivo de propiedad intelectual estadounidense. Según Keith Alexander: “Greatest transfer of wealth in history”, debido al hecho que este robo le ha costado a Estados Unidos billones de dólares (Perlroth, 2021, pp. 398). Otra estrategia de China que fomenta este modelo de espionaje es el apoyo del gobierno y el modelo de contratistas. El gobierno chino emplea una estrategia híbrida que mezcla unidades militares oficiales con un ecosistema de hackers "privados" para mantener una negación plausible. A diferencia de los hackers estadounidenses que buscan recompensas en China los hackers talentosos a menudo son "reclutados" o forzados a colaborar. Es por esto, que en ocasiones los ataques son rastreados hasta universidades chinas que reciben fondos estatales, o empleados de gigantes tecnológicos (Perlroth, 2021, pp. 202).

En el caso de Israel, uno de sus principales actores es la Unidad 8200, que es la unidad de élite de inteligencia del ejército de Israel. Es conocida por producir una gran cantidad de talento cibernético a nivel mundial. Incluso muchos de sus veteranos pasan al sector privado para fundar o trabajar en empresas de ciberseguridad. Desde los inicios del mercado de zero-days, se consideraba que los hackers tenían su base en Israel y que muchos de ellos eran trabajadores de esta unidad (Perlroth, 2021, pp. 65).

Como se mencionó anteriormente, algunas empresas de seguridad privada han sido fundadas por ex miembros de la Unidad 8200. El caso más reconocido es el del NSO Group, una empresa privada israelí que se ha convertido en uno de los líderes en el mercado spyware gubernamental (Perlroth, 2021, pp. 182). Como se menciona el capítulo 13, desarrollaron Pegasus, un spyware capaz de convertir un teléfono inteligente en un dispositivo de vigilancia total. Este grupo tiene capacidades técnicas sumamente avanzadas, incluso afirman haber desarrollado un tipo de infección sigilosa por aire, es decir, que pueden infectar un teléfono sin que la víctima tenga que hacer clic en ningún enlace malicioso. A pesar de su impresionante desarrollo, no todas sus armas son usadas éticamente, ya que, aunque ellos afirman vender sus exploits solo a gobiernos democráticos, se ha registrado un uso indebido de su tecnología contra periodistas, disidentes y activistas en lugares como México, Emiratos Árabes Unidos y Arabia Saudita (Perlroth, 2021, pp. 184-185, 422-423).

Debido a las tensiones que Israel mantiene con ciertos países, este suele dirigir sus actividades al sabotaje de infraestructura crítica y nuclear (Stuxnet), que en colaboración con Estados Unidos llevó a cabo el primer ataque cibernético conocido destinado a causar la destrucción física en la infraestructura de otro país. Por ejemplo, la Operación "Olympic Games" que fue operación conjunta para sabotear el programa nuclear de Irán. Fue una colaboración sin precedentes entre la NSA, la CIA, la Unidad 8200 y el Mossad, así como el objetivo Natanz, donde utilizaron un gusano informático (Stuxnet) para infiltrarse en los sistemas de la planta de enriquecimiento de uranio en Natanz. De esta forma, Stuxnet destruyó una quinta parte de las centrifugadoras de Irán y retrasó su programa nuclear por años (Perlroth, 2021, pp. 131).

Otra estrategia para mantener preponderancia en el panorama mundial es el desarrollo y uso de zero-days como en el arsenal de Stuxnet donde se utilizaron siete exploits distintos (Perlroth, 2021, pp. 36). Asimismo, acumulan poder gracias al liderazgo en el mercado de spyware con empresas como NSO Group y Cellebrite las cuales basan su modelo de negocio en la acumulación y militarización de cadenas de zero-days para vender acceso a dispositivos móviles (Perlroth, 2021, pp. 237, 247).

Exportación de capacidades cibernéticas ofensivas y cómo eso ha desestabilizado la seguridad global

En este análisis vamos a hablar de cómo la exportación de armas cibernéticas, como lo son los zero-days, ha alterado y desestabilizado la seguridad global. Para empezar, hay que explicar qué son los zero days: estos son vulnerabilidades en el hardware o software en sistemas computacionales que no tienen un ‘parche’ encontrado hasta el momento (Perlroth, 2021, pp. 28). Normalmente se les dice de esta forma porque, cuando salen a la luz, los encargados de este sistema tienen cero días para arreglarlos. Una vez sabemos eso, podemos presentar el problema a ser analizado. El problema es que, como existen estos zero-days, se formó un mercado que busca comprar y vender estas vulnerabilidades. Pero no hay ninguna regulación para el mismo, por lo que existe una industria enorme en la que se venden estos zero days convertidos en armas para atacar a empresas, y esto causa una desestabilización en la seguridad global.

El capítulo 2 del libro nos menciona que primero hubo un gran leak de datos cuando Snowden, un ex trabajador de la NSA (la Agencia de Seguridad de los Estados Unidos), publicó información que nos indica que esta agencia está creando zero-days con una unidad

llamada Tailored Access Operations o TAO (Perlroth, 2021, pp. 30). Pero también se hizo claro que no solo estaban creando sus propios zero days, sino que también muchos de estos fueron traídos desde afuera de la agencia (Perlroth, 2021, pp. 30). Seguimos luego con la historia de dos italianos que buscaban zero-days y los convertían en armas cibernéticas para poderlos vender y monetizar con ellos (Perlroth, 2021, pp. 34). Pero como este mercado fue creciendo con el tiempo, los gobiernos o naciones tuvieron que ser partícipes de este mercado porque fue su forma de no "going dark", como dice Nicole Perolth en su libro (Perlroth, 2021, pp. 35).

En esto entra la idea de que los gobiernos ya no eran los reguladores, sino que eran clientes por sí solos (Perlroth, 2021, pp. 40). Estos zero-days se volvieron un componente crítico en el arsenal cibernético de muchos países, pero en este punto había un margen muy grande, ya que los países más ricos eran los que mayor acceso tenían a la compra de estos ataques. Con esta nueva necesidad encontrada, el mercado fue creciendo y, como nos indican en el capítulo 3, se crearon empresas como iDefense para darles a sus clientes una alerta temprana de cualquier tipo de amenaza cibernética, que empezó a pagar a hackers por sus bugs encontrados. Al tener estos bugs, los iban a entregar a los dueños del sistema para que sean parchados, pero ya los podían usar como aviso anticipado para sus clientes (Perlroth, 2021, pp. 46). Estos pagos empezaron con montos de 75 dólares, pero con el tiempo fueron incrementando y se volvió un mercado en el que subía el precio por el que pedían comprar un bug si se mantenía en secreto (Perlroth, 2021, pp. 56). También se volvió una competencia con otras compañías que buscaban hacer lo mismo y que pagaban más, entonces ya realmente se volvió un mercado sumamente competitivo. Gobiernos involucrados en este underground market que se creó, como dicen en el capítulo 4, son los que hicieron que el mercado explote y cause un incremento hasta de países que compraban y preparaban su arsenal de exploits.

Hablando de la NSA particularmente, en el capítulo 6 nos indican que esta misión de la agencia para encontrar zero days empezó tan atrás como en la era predigital (Perlroth, 2021, pp. 83). Y con este arsenal, un ejemplo de las cosas que podían hacer fue lo que se filtró en el problema con Snowden, donde se mostró en verdad la cantidad de cosas que se podían hacer, como filtrar llamadas de teléfono, mails, fotos o screenshots, contraseñas, búsquedas en internet, borrar información y hasta hacer que un malware se distribuya de servidor en servidor muy rápido (Perlroth, 2021, p. 144). Se muestra cómo, en realidad, Estados Unidos y la NSA buscaban guardar estos exploits sin parcharlos para poder usarlos como herramienta de ataque en su arsenal, sin tomarle importancia a que en cualquier

momento podrían ser utilizados en su contra. Solo en el capítulo 9 podemos ver cómo es que TAO empezó a guardar zero-days sobre las máquinas que usaban en el programa nuclear de Irán, con lo que lograron crear Stuxnet, que fue un ataque contra los centrifugadores de Irán, que en conjunto con Israel lograron infectar para intentar frenar este programa y lograron dañar 2000 de los 8700 centrifugadores que tenían en Irán (Perlroth, 2021, pp. 136).

El caso de los Shadow Brokers en verdad dio la vuelta a la idea del mercado de zero-days y de cómo el stock de estos es, en realidad, sumamente peligroso incluso para el propio país que los guarda. En el capítulo 21 nos cuentan cómo, en agosto de 2016, una cuenta de Twitter llamada shadowbrokerss comenzó a afirmar que habían hackeado a la NSA y que tenían sus exploits para entregarlos al mundo (Perlroth, 2021, pp. 311). Al inicio los intentaron vender, pero esa estrategia no funcionó, entonces solo publicaron el código textual de los exploits para el mundo entero. La gente no creyó en un inicio que era de verdad, pero cuando abrieron el código se dieron cuenta de que sí era real y algunos ex trabajadores de esta agencia reconocieron el trabajo (Perlroth, 2021, pp. 313). En realidad, esto fue como un estabilizador en términos de equipamiento cibernético, que estaba siendo parcialmente liderado por los Estados Unidos, y con este leak de todo el arsenal de la NSA se cerró una brecha que existía por capacidades económicas de ciertos países.

Uno de los primeros grandes ataques que sucedieron después de esta revelación llamado WannaCry, que fue generado por Corea del Norte en 2017, y que usó un exploit de la NSA llamado EternalBlue,que es el que permitía que el malware se distribuya muy rápido de servidor en servidor (Perlroth, 2021, pp. 300, 324). Se dieron cuenta por utilizar herramientas que fueron usadas en su ataque a Sony por burlarse de Kim Jong-un, su líder, en una película de comedia llamada The Interview, por lo que Sony perdió el 70 % de sus computadoras (Perlroth, 2021, pp. 271). Al reutilizar este código se dieron cuenta de que fueron ellos. Igual con el caso de NotPetya, también en 2017, que fue hacia Ucrania para mostrar que seguía al mando de ellos, por así decirlo, pero se salió de control (Perlroth, 2021, pp. 329). Una empresa llamada Linkos fue el primer caso, pero cualquier persona o país que esté en negocios con Ucrania se vio comprometido (Perlroth, 2021, pp. 330). Este ataque se volvió el ataque más destructivo del mundo, ya que estaba destinado para Ucrania, pero acabó siendo mundial y costó como 10 billones de dólares en daños (Perlroth, 2021, pp. 331). Utilizó armas del arsenal de la NSA, como lo son EternalBlue y EternalRomance, usando también otro exploit llamado MimiKatz para robar contraseñas (Perlroth, 2021, pp. 329).

Estos son ejemplos que nos indican cuáles son los usos de estas capacidades que vienen desde la exportación de armas cibernéticas. Podemos ver ejemplos ya mencionados que entran en tres categorías, bajo nuestra perspectiva, que son sabotaje, espionaje y castigo o coerción. Primero, para sabotaje tenemos ataques como el de Stuxnet y Sandworm mencionados en el libro, con los que se atacaron mecanismos de otros países, como los centrifugadores de Irán. También se utilizan para espionaje, como el caso de la Unidad 61398 de China, que orquestó ataques hacia empresas estadounidenses como Coca-Cola o la RSA para ciberespionaje (Perlroth, 2021, pp. 267). Como también para un tipo de castigo, como el caso que ya se mencionó de Sony por parte de Corea del Norte, que en realidad solo fue venganza o castigo por una película con una escena que no les pareció.

Todos estos casos se han dado por un gran vacío normativo, y con esto nos referimos a la ausencia de reglas, porque aunque después de ataques enormes como WannaCry y NotPetya se quieren crear estos tipos de tratados donde no se puedan atacar hospitales, la red eléctrica, procesos políticos, etc., en realidad estos se vienen proponiendo por Europa y Rusia desde que pasó el ataque de Stuxnet (Perlroth, 2021, pp. 333). Pero Estados Unidos no aceptó estos tratados para mantener su arsenal de ataques guardados y usarlos para sus intereses de la ofensiva en ciberseguridad.

Y esto nos da paso a la discusión final, que es cómo esto en realidad desestabiliza la seguridad global. Y con todos los ejemplos que hemos podido analizar podemos ver que los países y criminales que pueden acceder a estas armas o este tipo de munición es cada vez más grande, con lo que existe menos control y más peligro para los mismos países y para las personas que viven en ellos.También hay varios ejemplos mencionados donde vemos que los efectos colaterales son enormes y, en ciertos casos, catastróficos, como ambos ataques después del leak de los Shadow Brokers, donde vimos que ni las mismas agencias que lanzan los ataques los pueden controlar al cien por ciento y no pueden medir sus consecuencias a nivel económico y personal. En el caso de Estados Unidos fue casi un caso perfecto de boomerang, en donde el país que tenía mayor ventaja ofensiva fue atacado por los mismos exploits que decidió no parchar para tener como arma, sin tomar en consideración que estos podrían ser usados en su contra, como al final pasó.

Esto también se puede observar cómo los países que más digitalizados y modernos están, son en realidad los que más peligro corren en sentido de ataques cibernéticos. Como nos indicó el libro, Ucrania sufrió ataques rusos que sí fueron catastróficos, pero no cómo podrían haber sido si hubieran sido contra USA o contra otros países que dependen de la tecnología (Perlroth, 2021, pp. 20).

Por último, como ya mencionamos, la falta de normas hace que los ataques no puedan ser medibles en sentido de reciprocidad al atacar de vuelta ni en los límites que estos deben respetar, lo que causa que el nivel de ataques vaya incrementando y pueda llegar a ser verdaderamente catastrófico o incluso mortal para muchas personas.

Simulación de escenario que detalla un importante conflicto geopolítico

Ahora vamos a detallar una simulación basada en los conceptos que hemos venido abordando. El objetivo es demostrar como la ausencia de reglas de engagement internacionales en el ciberespacio puede llevar a una escalación incontrolable de conflictos entre naciones.

El escenario que se propone se sitúa en el año 2027 y presenta un conflicto que involucra a China, Estados Unidos, Taiwán y Rusia. Todos los actores, capacidades técnicas y tácticas usadas en esta simulación están fundamentadas en casos reales documentados en el libro, incluyendo Stuxnet, NotPetya, revelaciones de Snowden y las filtraciones de Shadow Brokers.

Contexto Geopolítico del Escenario

El escenario se desarrolla en un contexto de tensiones máximas entre China y Taiwán. El gobierno chino está realizando ejercicios militares de bloqueo alrededor de Taiwán, simulando operaciones de asedio. Como respuesta a esta situación, Estados Unidos ha desplegado grupos de portaaviones en la región del Indo-Pacífico como muestra de apoyo a Taiwán y disuasión hacia China. Simultáneamente, Rusia observa la situación y evalúa oportunidades para aprovechar que la atención occidental está concentrada en Asia.

Actores Involucrados

Los actores estatales que participan en este escenario son los siguientes:

- **China:** Unidad 61398 del Ejército Popular de Liberación (PLA) y la Fuerza de Apoyo Estratégico, unidades cibernéticas militares documentadas extensamente por Perlroth en su análisis del ciberespionaje chino contra empresas occidentales.
- **Estados Unidos:** Agencia de Seguridad Nacional (NSA) con su división de Operaciones de Acceso Personalizado (TAO) y el Comando Cibernético de

Estados Unidos. Estas organizaciones desarrollaron el arsenal de ciberarmas revelado por Snowden y posteriormente filtrado por Shadow Brokers.

- **Rusia:** Unidad 74455, conocida como Sandworm, y Fancy Bear (APT28). Estos grupos son responsables de ataques documentados como NotPetya y los apagones en Ucrania que Perlroth describe en detalle.
- **Taiwán:** Ministerio de Defensa Nacional con capacidades defensivas limitadas en comparación con los actores principales.

Desarrollo del Escenario por Fases

Fase 1: Provocación Inicial (Día 1-3)

Evento Desencadenante

Un carguero chino reporta una falla crítica en sus sistemas de navegación GPS mientras transita cerca del estrecho de Taiwán, lo que casi ocasiona una colisión con un buque de guerra taiwanés. El gobierno chino acusa públicamente a Taiwán de realizar operaciones de guerra electrónica contra embarcaciones civiles chinas, utilizando este incidente como justificación para una respuesta.

Primera Respuesta Cibernética

China lanza un ataque cibernético coordinado a través de la Unidad 61398, dirigido contra infraestructura crítica taiwanesa. El ataque tiene tres componentes principales: primero, un ataque de denegación de servicio distribuido (DDoS) masivo contra los principales bancos taiwaneses, provocando el colapso de servicios bancarios en línea y cajeros automáticos durante varias horas. Segundo, infiltración en los sistemas de control de tráfico aéreo del Aeropuerto Internacional de Taipéi, generando alertas falsas y causando retrasos significativos en operaciones aéreas. Tercero, desfiguración (defacement) de sitios web gubernamentales, reemplazando su contenido con mensajes propagandísticos pro-reunificación.

Capacidades Técnicas Utilizadas

Las capacidades técnicas empleadas por China en esta fase están documentadas en el libro de Perlroth a través de casos reales. La Unidad 61398 ha perfeccionado técnicas de spear-phishing durante años, como se evidenció en los ataques documentados contra

empresas como RSA Security, Lockheed Martin y Coca-Cola. Además, explotan vulnerabilidades zero-day, fallas de software no publicadas que China ha acumulado en su arsenal cibernético a través del mercado gris de vulnerabilidades. Finalmente, emplean la técnica 'watering hole', que consiste en comprometer sitios web frecuentados por los objetivos para distribuir malware de manera selectiva.

Primera Manifestación de Ausencia de Reglas

Esta fase demuestra la primera problemática relacionada con la ausencia de reglas de engagement: ¿constituye este ataque cibernético un acto de guerra? No existe consenso internacional al respecto. Aunque la atribución técnica es clara y hay evidencia forense que señala a China, no existe un mecanismo internacional establecido para imponer consecuencias. Taiwán enfrenta un dilema: no puede responder militarmente porque eso escalaría a un conflicto convencional que no puede ganar, pero tampoco existe un marco legal internacional que le permita obtener reparación.

Fase 2: Escalación Controlada (Día 4-7)

Contraataque de Estados Unidos

Estados Unidos decide responder al ataque contra su aliado Taiwán. La NSA, operando a través de su división TAO (Tailored Access Operations), lanza un contraataque contra infraestructura militar china con tres componentes: sabotaje temporal de sistemas de radar costeros chinos, creando puntos ciegos en la vigilancia marítima de China en áreas estratégicas del Mar de China Oriental; infiltración en sistemas de comando y control (C2) del Ejército Popular de Liberación, permitiendo monitoreo de comunicaciones militares; y colocación de implantes persistentes en redes de comunicación militar china para capacidades de espionaje a largo plazo.

Herramientas Documentadas de la NSA

Las herramientas utilizadas por Estados Unidos están documentadas en el libro a través de las revelaciones de Snowden y las filtraciones de Shadow Brokers. QUANTUM INSERT es una técnica de man-in-the-middle desarrollada por la NSA que permite interceptar y modificar tráfico de internet en tiempo real. El arsenal incluye vulnerabilidades zero-day similares a las herramientas filtradas por Shadow Brokers, incluyendo exploits para sistemas operativos y firmware de equipos de red. Finalmente, se emplean implantes de

hardware, una técnica similar a la utilizada en Stuxnet, donde se insertan componentes maliciosos en hardware, aunque sin causar daño físico permanente en esta instancia.

Contraataque de China

La Fuerza de Apoyo Estratégico de China responde al contraataque estadounidense con operaciones dirigidas contra bases militares de Estados Unidos en Japón y Guam. El ataque incluye el despliegue de ransomware en sistemas administrativos (no operacionales) de las bases militares, enviando un mensaje sin cruzar el umbral de incapacitar capacidades operativas críticas. Simultáneamente, ejecutan un robo masivo de datos de personal militar estadounidense, incluyendo información sensible de seguridad, y causan interferencia con sistemas de comunicación satelital utilizados por fuerzas estadounidenses en la región.

Segundo Dilema: Proporcionalidad Indefinida

Esta fase demuestra la segunda problemática fundamental: la ausencia de métricas para determinar qué constituye una respuesta proporcional en el ciberespacio. ¿Es el sabotaje temporal de un sistema de radar equivalente a la destrucción de un tanque o avión? ¿El robo de datos clasificados justifica una respuesta física? No existen tratados internacionales que establezcan equivalencias, y ninguna de las partes desea escalar a un conflicto militar convencional, pero tampoco hay un marco que defina dónde está el límite de la respuesta cibernética aceptable.

Fase 3: Pérdida de Control y Daño Colateral (Día 8-12)

Entrada Oportunista de Rusia

Mientras Estados Unidos está concentrado en manejar la crisis en Asia, Rusia identifica una oportunidad estratégica. La Unidad 74455 (Sandworm) lanza una serie de ataques coordinados que incluyen el despliegue de NotPetya 2.0, una versión actualizada del malware destructivo utilizado en 2017, dirigido nuevamente contra infraestructura ucraniana. Simultáneamente, ejecutan ataques contra instalaciones de gasoductos en Europa del Este, aprovechando la distracción de las naciones occidentales. Lo más peligroso es el uso de operaciones de bandera falsa, haciendo que algunos ataques parezcan provenir de actores chinos para generar confusión y fricción entre aliados occidentales y asiáticos.

Propagación Incontrolable de Malware

El aspecto más peligroso de esta fase es la pérdida de control sobre el malware inicialmente diseñado para objetivos específicos. El código malicioso que China desarrolló específicamente para sistemas taiwaneses comienza a propagarse más allá de sus objetivos originales, extendiéndose a Japón y Corea del Sur debido a la integración de cadenas de suministro y conexiones comerciales con Taiwán. La propagación afecta gravemente la industria global de semiconductores, causando interrupciones en la producción de chips que abastecen a múltiples sectores económicos. Al final de esta fase, más de 15,000 empresas en 60 países reportan afectaciones, en un patrón similar al ataque NotPetya real documentado por Perlroth, que causó más de $10 mil millones en daños a nivel mundial.

Técnicas Documentadas en el Libro

Las técnicas utilizadas en esta fase están extensamente documentadas por Perlroth. NotPetya es un malware que se disfraza de ransomware pero es en realidad puramente destructivo, sin mecanismo real de recuperación de datos. El caso real afectó a empresas como Maersk, Merck y FedEx. EternalBlue, por su parte, es un exploit desarrollado por la NSA, robado por Shadow Brokers, y posteriormente utilizado en ataques masivos como WannaCry y el propio NotPetya, demostrando cómo las herramientas creadas por un estado pueden terminar siendo utilizadas por otros actores. Finalmente, el wiper malware es software diseñado específicamente para destruir datos de manera permanente, sin posibilidad de recuperación.

Tercera Problemática: Responsabilidad del Daño Colateral

Esta fase plantea la pregunta más compleja sobre responsabilidad legal internacional: ¿Quién es responsable cuando el daño colateral excede dramáticamente los objetivos originales? ¿China, por crear el malware? ¿Estados Unidos, por provocar el conflicto que llevó a su despliegue? ¿Rusia, por aprovechar oportunistamente la situación? La ausencia de un marco legal internacional deja estas preguntas sin respuesta, y las empresas afectadas no tienen recurso legal claro.

Fase 4: Desescalación Caótica (Día 13-20)

Presión Internacional

Las consecuencias económicas del conflicto cibernético comienzan a generar presión política significativa. Los mercados bursátiles globales experimentan caídas significativas

debido a la incertidumbre y la interrupción de cadenas de suministro. La escasez de componentes electrónicos afecta múltiples industrias, desde automotriz hasta electrónica de consumo. En este contexto, la Unión Europea y la Asociación de Naciones del Sudeste Asiático (ASEAN) presionan diplomáticamente por un 'alto al fuego digital'.

Ausencia de Mecanismos Formales

Un problema fundamental emerge: no existe un mecanismo formal establecido para declarar o negociar un cese al fuego cibernético. A diferencia de los conflictos militares convencionales, donde existen protocolos diplomáticos centenarios y organizaciones internacionales como las Naciones Unidas que pueden mediar, el ciberespacio carece completamente de estos marcos institucionales.

Desescalación Informal

Los intentos de desescalación son completamente informales y ad hoc. China y Estados Unidos establecen una línea de comunicación directa, similar al 'teléfono rojo' de la Guerra Fría, pero adaptada a la era digital. Ambas potencias acuerdan tácitamente una 'pausa' en operaciones ofensivas, aunque ninguna admite públicamente responsabilidad por sus acciones previas. Mientras tanto, Rusia continúa con operaciones menores sin enfrentar consecuencias, aprovechando la ambigüedad de atribución y la falta de voluntad occidental de abrir un segundo frente de confrontación.

Resultado Final Ambiguo

El conflicto termina sin resolución clara:

- No hay un ganador definido en términos estratégicos o tácticos.
- Los daños económicos acumulados suman decenas de miles de millones de dólares a nivel global.
- No se firma ningún tratado, acuerdo formal ni se establece ningún precedente legal.
- Las vulnerabilidades explotadas durante el conflicto permanecen en los arsenales de cada nación, listas para ser utilizadas en futuros enfrentamientos.

Esta conclusión ambigua ilustra una característica fundamental de la ciberguerra documentada por Perlroth: a diferencia de los conflictos militares convencionales que típicamente terminan con rendiciones formales, tratados de paz o acuerdos de armisticio, los

conflictos cibernéticos simplemente se desvanecen en pausas temporales hasta el próximo enfrentamiento.

Análisis Sistemático: Ausencia de Reglas de Engagement

El escenario presentado demuestra seis problemáticas fundamentales relacionadas con la ausencia de reglas de engagement claras en el ciberespacio. A continuación se analiza cada una sistemáticamente:

Indefinición de 'Ataque'

En la guerra convencional, la definición de ataque es relativamente clara: el uso de fuerza cinética contra objetivos físicos. Sin embargo, en el ciberespacio no existe consenso internacional sobre qué constituye un ataque. Surgen preguntas fundamentales: ¿Un ataque DDoS que interrumpe servicios bancarios es un acto de guerra, espionaje económico, o simplemente vandalismo digital? ¿El robo masivo de datos clasificados constituye un ataque armado bajo el derecho internacional? ¿La infiltración en sistemas sin causar daño inmediato pero manteniendo acceso persistente debe considerarse un acto hostil? Perlroth documenta cómo esta ambigüedad permite a los estados realizar operaciones que en el mundo físico serían claramente actos de guerra, mientras mantienen negación plausible en el ámbito diplomático.

Atribución Ambigua

La atribución técnica de ciberataques es inherentemente compleja. Aunque existen técnicas forenses que pueden identificar patrones de código, infraestructura utilizada y tácticas características, la prueba definitiva de autoría estatal es difícil de establecer. Los estados pueden operar a través de proxies, utilizando hackers mercenarios o grupos criminales, manteniendo distancia oficial. Además, las operaciones de bandera falsa son comunes, donde un actor se hace pasar por otro para generar fricción entre adversarios o confundir la investigación. El libro documenta múltiples casos donde, a pesar de evidencia técnica sólida, los estados acusados mantienen negación oficial, y no existe un tribunal internacional con autoridad para adjudicar estas disputas.

Proporcionalidad Indefinida

En la guerra convencional, existe cierta lógica de proporcionalidad: la destrucción de un activo militar generalmente justifica una respuesta equivalente. En el ciberespacio, no existen métricas establecidas para determinar qué constituye una respuesta proporcional. ¿Cómo se cuantifica el 'valor' de un ataque cibernético? ¿Por el daño económico causado? ¿Por la importancia estratégica del sistema comprometido? ¿Es la interrupción temporal de un sistema de radar equivalente a su destrucción física? ¿El daño económico a empresas privadas se equipara al daño a activos militares? Esta indefinición crea un riesgo de escalación, donde cada parte puede interpretar subjetivamente que su respuesta es 'proporcional', llevando a ciclos de represalias crecientes.

Ausencia de Distinción Civil-Militar

Las Convenciones de Ginebra establecen una distinción clara entre objetivos civiles y militares en guerra convencional. En el ciberespacio, esta distinción es prácticamente imposible. Internet es inherentemente 'dual-use': la misma infraestructura sirve propósitos civiles y militares. Los bancos procesan tanto transacciones civiles como pagos a contratistas militares. Las redes eléctricas alimentan simultáneamente hogares, hospitales y bases militares. Las cadenas de suministro industriales producen componentes tanto para uso civil como militar. Como documenta Perlroth con el caso NotPetya, el daño colateral a infraestructura civil no solo es inevitable, sino que puede exceder dramáticamente el daño a objetivos militares. No existe el equivalente digital de una 'zona desmilitarizada'.

Umbral Incierto para Respuesta Física

Una de las preguntas más críticas y sin resolver en el ciberespacio es: ¿Cuándo justifica un ciberataque una respuesta con armas convencionales? Si un ciberataque apaga la red eléctrica de una ciudad causando muertes, ¿justifica esto bombardear la instalación desde donde se lanzó el ataque? El Artículo 5 de la OTAN declara que un ataque a un miembro es un ataque a todos, pero ¿aplica esto a ciberataques? ¿Qué magnitud de ataque cibernético activaría esta cláusula? ¿Existe un equivalente digital del ataque a Pearl Harbor que justificaría una declaración formal de guerra? Cada nación mantiene sus propios criterios, no públicos, sobre este umbral, creando un peligroso espacio de incertidumbre donde una escalación accidental a conflicto físico es posible.

Escalación Impredecible

A diferencia de las armas convencionales o nucleares, las ciberarmas son inherentemente incontrolables una vez desplegadas. El malware puede propagarse más allá de sus objetivos originales, como NotPetya demostró cuando un ataque dirigido a Ucrania causó daños globales por más de $10 mil millones. Las herramientas pueden ser robadas por otros actores, como ocurrió cuando Shadow Brokers filtró el arsenal de la NSA, permitiendo que herramientas estadounidenses fueran utilizadas en ataques contra intereses estadounidenses. No existe forma de 'contener' un ataque digital una vez liberado en la red, a diferencia de un misil cuya trayectoria es predecible. Esta imprevisibilidad inherente significa que incluso ataques cibernéticos 'limitados' pueden tener consecuencias globales no intencionadas, un riesgo que Perlroth documenta extensamente a través de casos reales.

Lecciones Extraídas del Escenario

Mutually Assured Disruption vs. Mutually Assured Destruction

Durante la Guerra Fría, la doctrina de Destrucción Mutuamente Asegurada funcionó como disuasivo efectivo porque ninguna parte estaba dispuesta a iniciar un intercambio nuclear que resultaría en aniquilación mutua. En el ciberespacio, paradójicamente, la dinámica es inversa. Las naciones lanzan ciberataques precisamente porque el daño parece 'manejable' y limitado en comparación con armas convencionales. No existe una amenaza existencial inmediata que prevenga el uso de ciberarmas. Sin embargo, cuando se acumulan todos los ataques 'pequeños' y se contabiliza el daño colateral, el resultado es catastrófico para la economía global y la estabilidad internacional. Perlroth introduce el concepto de 'Mutually Assured Disruption' para describir esta dinámica donde todos atacan continuamente, causando disrupción acumulativa masiva sin que ninguna parte tenga incentivo para detenerse unilateralmente.

Proliferación Incontrolable de Ciberarmas

El caso de EternalBlue, documentado extensamente por Perlroth, ilustra perfectamente este problema. La NSA desarrolló EternalBlue como herramienta sofisticada de espionaje, invirtiendo recursos significativos. Shadow Brokers robó esta herramienta y la publicó en internet. Rusia la incorporó en NotPetya, causando daño masivo a empresas estadounidenses. Grupos criminales la utilizaron en WannaCry, afectando al Sistema Nacional de Salud británico y otras víctimas globales. Este ciclo demuestra que, a diferencia

de las armas nucleares que requieren infraestructura física masiva y materiales controlados, las ciberarmas son esencialmente código que puede copiarse infinitamente. Una vez que una capacidad existe, su proliferación es inevitable. No existe equivalente al Tratado de No Proliferación Nuclear para el ciberespacio.

Ausencia de Disuasión Efectiva

La disuasión en guerra convencional o nuclear funciona porque la atribución es clara y las consecuencias son seguras. En el ciberespacio, la atribución difusa permite negación plausible, reduciendo el costo político de ser descubierto. Las consecuencias son inconsistentes: algunos ataques resultan en sanciones económicas, otros en condenas diplomáticas vacías, y muchos no enfrentan respuesta alguna. El beneficio potencial, que incluye inteligencia robada, daño económico al adversario y ventaja estratégica, frecuentemente supera el riesgo de consecuencias. Sin consecuencias predecibles y significativas, no hay incentivo real para que los estados se abstengan de lanzar ciberataques. Perlroth documenta cómo esto ha llevado a una normalización de la ciberguerra como herramienta de política exterior.

Necesidad de Marco Legal Internacional

La Convención de Budapest sobre Cibercrimen, que actualmente representa el principal tratado internacional en esta área, es fundamentalmente insuficiente. Se enfoca en crimen cibernético, no en guerra cibernética entre estados. No establece reglas de engagement ni define qué constituye un acto de guerra en el ciberespacio. Además, carece de mecanismos de enforcement o consecuencias claras por violaciones. Se requiere un marco internacional equivalente al Tratado de No Proliferación Nuclear o a las Convenciones de Ginebra, pero adaptado a las realidades del ciberespacio.

Sin embargo, existe un obstáculo fundamental: el incentivo para desarrollar capacidades cibernéticas ofensivas es extremadamente alto. Son relativamente baratas comparadas con sistemas de armas convencionales, difíciles de detectar, fáciles de negar, y potencialmente muy efectivas. Ninguna potencia importante está dispuesta a renunciar unilateralmente a estas capacidades, creando un dilema del prisionero a nivel global.

Conclusión

El escenario 'Operación Estrecho Digital', aunque ficticio, está fundamentado completamente en capacidades reales, actores documentados y precedentes históricos presentados en el libro de Nicole Perlroth. Cada elemento del escenario tiene su contraparte en eventos reales: Stuxnet demostró que las ciberarmas pueden causar daño físico real en el mundo material; NotPetya demostró que el control sobre ciberarmas una vez desplegadas es una ilusión peligrosa; Shadow Brokers demostró que la proliferación de herramientas cibernéticas es inevitable; y los documentos de Snowden revelaron la escala masiva de los arsenales cibernéticos estatales.

La simulación presentada combina estos elementos para proyectar cómo podría desarrollarse un conflicto cibernético futuro en ausencia de reglas de engagement internacionales claras. Las seis problemáticas identificadas (indefinición de ataque, atribución ambigua, proporcionalidad indefinida, ausencia de distinción civil-militar, umbral incierto para respuesta física, y escalación impredecible) no son teóricas: son desafíos reales que los estados enfrentan actualmente.

La conclusión más significativa es que la comunidad internacional se encuentra en una carrera armamentista cibernética sin las salvaguardas institucionales, legales y normativas que eventualmente estabilizaron la carrera armamentista nuclear. A diferencia de la Guerra Fría, donde la amenaza existencial forzó el desarrollo de tratados, líneas directas y protocolos de reducción de armas, en el ciberespacio la amenaza es lo suficientemente difusa como para permitir ataques continuos, pero lo suficientemente real como para causar daño masivo acumulativo.

Podemos ver que la ventana para establecer normas internacionales efectivas se está cerrando rápidamente. Cada ataque cibernético que ocurre sin consecuencias significativas normaliza este comportamiento y hace más difícil establecer límites posteriormente. La pregunta no es si ocurrirá un conflicto cibernético mayor, sino cuándo, y si la comunidad internacional habrá desarrollado los marcos necesarios para prevenirlo o al menos limitarlo antes de que cause daño irreparable a la infraestructura global de la cual depende la civilización moderna.

Referencias

Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race.* Bloomsbury Publishing.