LA ECONOMÍA Y ÉTICA DEL MERCADO ZERO-DAY

Análisis del ecosistema oculto de vulnerabilidades: De la Carrera Armamentista al Dilema Regulatorio

INTRODUCCIÓN

En las últimas dos décadas, las vulnerabilidades zero-day han evolucionado de ser anomalías técnicas aisladas a constituir el núcleo de una industria armamentista global multimillonaria. Un zero-day es una vulnerabilidad de software desconocida por el fabricante y sin parche disponible, denominada así porque los usuarios tienen literalmente cero días para defenderse una vez que es explotada. Nicole Perlroth documenta cómo este mercado opera en una zona gris completamente desprovisto de regulación internacional efectiva, donde convergen hackers independientes, brokers especializados como Zerodium, empresas de spyware, contratistas de defensa y agencias de inteligencia, como relata la autora en los capítulos 3, 4 y 5, donde expone cómo agencias de inteligencia y brokers privados construyeron un mercado paralelo de exploits sin supervisión alguna. Los incentivos económicos son extraordinarios: mientras programas defensivos como iDefense históricamente pagaban $100 dólares por vulnerabilidad, el mercado ofensivo ofrece regularmente cientos de miles o incluso millones de dólares por los mismos exploits, creando un diferencial que ha impulsado el crecimiento explosivo de este ecosistema oculto.

Desde este punto, esta investigación examina el mercado zero-day desde tres perspectivas complementarias. Primero, analiza la cadena de suministro completa desde el descubrimiento inicial hasta la armamentización operacional, mapeando actores, flujos económicos y dinámicas de poder en cada etapa. Segundo, desarrolla un marco económico para cuantificar los costos de oportunidad del dilema central "parchear versus acumular" que enfrentan gobiernos y empresas tecnológicas: revelar vulnerabilidades para proteger usuarios o retenerlas para capacidades ofensivas. Tercero, presenta una propuesta de política regulatoria que aborda las cuestiones éticas cuando investigadores, agencias gubernamentales y empresas deben elegir entre divulgación responsable o retención estratégica. A continuación, se procederá a explicar los temas complementarios.

EVOLUCIÓN DEL MERCADO: LAS CINCO FASES CRÍTICAS

Fase 1: El Despertar

Todo cambió con Operation Aurora en 2010, un ataque contra Google que dejó claro que ya no se estaba hablando de hackers aficionados, sino de estados nacionales con recursos masivos, como explica la autora en el capítulo 14, donde Google descubre la magnitud del ataque chino y reconoce la necesidad de reforzar defensas y programas de bug bounty. Google respondió

reforzando su infraestructura, desarrollando fuzzing masivo e incrementando sus bug bounties. Sin embargo, las agencias de inteligencia comenzaron a acumular zero-days en lugar de reportarlos para que fueran parcheados. Este choque entre parchear para proteger versus acumular para atacar es lo que impulsa la carrera armamentista cibernética que se explica a gran escala en el libro. El dilema se conoce como el Vulnerabilities Equities Process (VEP), donde los gobiernos deben decidir si revelar o retener las vulnerabilidades que descubren técnicamente.

Fase 2: El Dilema Económico

La segunda fase se caracteriza por la emergencia de una brecha económica masiva. El mercado defensivo como iDefense pagaba apenas $100 dólares por vulnerabilidad, mientras el mercado ofensivo pagaba miles o decenas de miles por el mismo fallo, como relata Perlroth en el capítulo 3, donde expone las diferencias abismales entre los mercados defensivos y ofensivos que atraían a los investigadores hacia la venta clandestina. Google intentó competir aumentando sus recompensas hasta $1.5 millones de dólares para Android, pero los precios del mercado ofensivo eran de 10 a 50 veces más altos. Este diferencial económico gigantesco fue clave para entender por qué prosperó el mercado gris y negro. Los investigadores de seguridad enfrentaban un dilema: reportar responsablemente por recompensas modestas o monetizar lucrativamente en el mercado ofensivo con implicaciones éticas complejas.

Fase 3: De la Ética al Mercado Gris - El Caso Netragard

Adriel Desautels fundó Netragard tras descubrir un fallo en software de HP en 2002 y enfrentar amenazas legales al reportarlo, como detalla la autora en el capítulo 4, explicando cómo la falta de incentivos defensivos y las amenazas empujaron a los investigadores hacia el mercado ofensivo. Con apoyo de la EFF, entró al mercado de exploits. Vendió su primer zero-day en formato MP3 por $16,000 dólares, luego otros por más de $90,000, mientras iDefense seguía pagando solo $100. Netragard estableció estándares profesionales rigurosos: exigía 98-99% de éxito, "clean fail" sin rastros detectables, y vendía exclusividad al triple del precio. Crucialmente, Desautels solo vendía a entidades estadounidenses por razones éticas.

De igual forma, Netragard no solo vendía exploits técnicos; ofrecía penetration testing realista que incluía falsificación de documentos, intrusión física en edificios, obtención de llaves y tarjetas de acceso, e infiltración en bancos, casinos y laboratorios. Su lema era provocador: "We protect you from people like us" (Te protegemos de gente como nosotros). Este modelo estableció la primera cadena clara del mercado: investigador descubre vulnerabilidad, la valida bajo estándares rigurosos, la vende a un broker con filtros éticos, quien vende a agencias gubernamentales estadounidenses. Sin embargo, este modelo relativamente ético sentó las bases para brokers globales sin restricciones.

Fase 4: Globalización del Mercado

Chaouki Bekrar marca la verdadera globalización del mercado y la eliminación de restricciones éticas, según se relata en el capítulo 5, donde Bekrar rechaza el premio de Google y declara que su exploit vale mucho más en el mercado estatal ofensivo. En Pwn2Own 2012, Bekrar ganó la competencia cuando rompió la seguridad de Google Chrome, pero rechazó el premio porque debía revelar el exploit. Declaró contundentemente que no compartiría su zero-day "ni por 1 millón de dólares". La razón por su afirmación se debía por el hecho de que estaba vendiendo a la NSA, al BSI alemán y otros gobiernos por cifras muy superiores. A diferencia de Netragard, Bekrar vendía globalmente a cualquier gobierno con suficiente dinero, sin filtros éticos. Esto marcó la verdadera globalización del mercado y eliminó las restricciones éticas que existían antes, significando que regímenes autoritarios y gobiernos sin supervisión democrática robusta podían ahora acceder a las mismas armas digitales.

Fase 5: Zerodium y la Explosión del Mercado

Finalmente, Bekrar fundó Zerodium e hizo algo revolucionario: publicó listas de precios públicamente. Hasta ese momento todo era negociación privada en las sombras. Bekrar publicó abiertamente: $80,000 por Chrome, $100,000 por Android, $500,000 por iPhone, hasta $1 millón en 2015 por jailbreak remoto de iPhone. Para 2020, los exploits zero-click móviles llegaron a valer $1.5-$2.5 millones de dólares. Esta transparencia estableció precios de mercado claros por primera vez, permitió a investigadores saber exactamente cuánto valían sus descubrimientos, creó presión competitiva sobre programas de bug bounty corporativos y legitimó públicamente un mercado que antes operaba en secreto. Cuando perdió su licencia de exportación en Europa, simplemente movió operaciones a Washington D.C. donde había menos regulaciones. Este movimiento disparó una verdadera carrera de precios y consolidó el mercado ofensivo como industria multimillonaria, como explica Perlroth en los capítulos 5 y 15, donde se detalla cómo esta empresa institucionalizó precios públicos y aceleró la carrera armamentista.

LA CADENA DE SUMINISTRO: PRIMERAS ETAPAS

Basándonos en la evolución descrita, la cadena de suministro en sus etapas iniciales funciona de la siguiente manera. En la etapa de descubrimiento, investigadores de seguridad independientes, equipos corporativos o hackers patrocinados por estados identifican vulnerabilidades mediante fuzzing, análisis de código o ingeniería reversa. La decisión crítica en este punto es si reportar responsablemente o monetizar en el mercado ofensivo, una elección determinada principalmente por los incentivos económicos masivos del mercado gris y negro.

La segunda etapa es el desarrollo y validación. El investigador original o equipos especializados convierten la vulnerabilidad en un exploit funcional y confiable bajo criterios

estrictos: tasa de éxito de 98-99%, capacidad de "clean fail" sin dejar rastros, persistencia en el sistema objetivo y evasión efectiva de defensas, criterios mencionados por Perlroth en el capítulo 4, cuando describe los estándares que Netragard aplicaba antes de vender exploits a agencias estadounidenses. Esta fase es crucial porque determina el valor final del exploit en el mercado.

La tercera etapa crítica es la intermediación a través de brokers. Aquí es donde empresas como Netragard (con filtros éticos) o Vupen/Zerodium (sin filtros geográficos) conectan vendedores con compradores, validan la calidad técnica del exploit, garantizan exclusividad y proporcionan protección legal para vendedores. El valor agregado de estos intermediarios incluye la gestión de transacciones complejas, la validación técnica rigurosa y el acceso a compradores de alto nivel. La evolución de estos brokers muestra una transición clara: de intermediarios éticos y regionales como Netragard que solo vendían a entidades estadounidenses, a mercados globales completamente abiertos como Zerodium que venden a cualquier comprador con capacidad de pago, sin restricciones geográficas ni éticas.

Fase 6: La Industrialización del Espionaje — El Auge del Spyware Comercial

Tras la consolidación del mercado ofensivo con Zerodium, una nueva etapa descrita por Perlroth en los capítulos 11–13 muestra cómo el espionaje digital se industrializa a través de empresas privadas como Hacking Team y NSO Group. Estas compañías tomaron la infraestructura creada por brokers y la transformaron en servicios completos de vigilancia para gobiernos. En palabras de Perlroth, este periodo marca la transición del mercado zero-day desde un intercambio técnico de exploits hacia “una industria de espionaje llave en mano” controlada por actores privados. La autora detalla cómo estos proveedores integraban zero-days de Android, iOS y Windows en paquetes de spyware capaces de tomar control total de dispositivos, lo que redujo drásticamente las barreras para que gobiernos de todo tipo accedieran a capacidades ofensivas avanzadas. Este proceso permitió que regímenes autoritarios adquirieran herramientas que antes solo estaban disponibles para superpotencias como Estados Unidos, creando un nuevo nivel de riesgo global.

Fase 7: Proliferación Global y Normalización del Abuso Estatal

La siguiente fase, documentada en los capítulos 12 y 13, se caracteriza por la proliferación masiva de estas capacidades. Perlroth muestra cómo países con antecedentes de represión interna como Emiratos Árabes Unidos, Arabia Saudita, Sudán, Uzbekistán o Etiopía comenzaron a adquirir zero-days y spyware para vigilar periodistas, activistas y opositores políticos. Casos como el de Ahmed Mansoor, quien recibió repetidos mensajes con exploits de iPhone adquiridos de NSO Group, ilustran cómo estas herramientas se convertían en instrumentos directos de persecución. Esta proliferación no solo aumentó el volumen de abusos, sino que normalizó el uso ofensivo de zero-days como política estatal rutinaria. En esta etapa, la “ventaja competitiva” tecnológica se transformó en una herramienta para consolidar poder interno y silenciar disidencia, desplazando cualquier noción de seguridad colectiva o responsabilidad ética.

Fase 8: La Subcontratación del Ciberpoder, Project Raven y el Outsourcing Ofensivo

En los capítulos 11–13, Perlroth introduce otro fenómeno crítico: la subcontratación de capacidades ofensivas. A través del caso de Project Raven en Emiratos Árabes Unidos, la autora explica cómo exagentes de la NSA fueron reclutados para construir programas de vigilancia dirigidos inicialmente a amenazas externas, pero que pronto derivaron en operaciones contra periodistas, activistas y gobiernos rivales. Esta fase simboliza un cambio estructural: el ciberpoder deja de ser monopolio estatal y empieza a ser tercerizado hacia expertos privados con entrenamiento militar, lo que diluye la rendición de cuentas. Como narran los propios participantes entrevistados por Perlroth, muchos se dieron cuenta demasiado tarde de que sus conocimientos estaban siendo utilizados para reforzar aparatos represivos, un riesgo que se intensificó por la ausencia total de regulación internacional.

Fase 9: El Colapso del Secreto, Shadow Brokers y la Pérdida del Control Operacional

Una vez que el mercado se globalizó y se privatizó, la siguiente fase crítica ocurre cuando los arsenales digitales acumulados por potencias como Estados Unidos se vuelven imposibles de proteger. En los capítulos 20–22, Perlroth describe cómo el grupo Shadow Brokers filtró herramientas de la NSA, incluyendo el exploit EternalBlue, lo que reveló la fragilidad inherente a la estrategia de acumular zero-days ("hoarding"). El impacto fue inmediato: Corea del Norte lo utilizó para lanzar WannaCry y Rusia para ejecutar NotPetya, ataques que afectaron hospitales británicos, redes de transporte, plantas nucleares como Chernóbil y empresas globales como Maersk y Merck. Esta fase demuestra que ningún estado puede garantizar el control de sus armas digitales, y que la acumulación secreta de vulnerabilidades produce riesgos sistémicos que trascienden fronteras, sectores y poblaciones.

Modelo Económico "Patch vs Hoard"El libro *This Is How They Tell Me the World Ends* describe el crecimiento de un mercado clandestino de vulnerabilidades zero-day y cómo este mercado alteró profundamente la seguridad global. A lo largo del texto, la autora muestra cómo los gobiernos, especialmente el NSA, han acumulado ciberarmas en secreto, creando riesgos sistémicos cuando estas herramientas salen de su control.

Según la autora en la sección “The Shadow Brokers”, se detalla que un conjunto altamente sensible de herramientas del NSA fue robado y posteriormente publicado, demostrando que incluso las agencias más poderosas pueden perder el control de los exploits que deciden acumular.

Este hecho fundamenta el dilema que analizamos en este informe:

¿Qué sale más caro a largo plazo: parchar una vulnerabilidad o acumularla para explotarla?

Según la autora en la sección “Tailored Access Operations”, el NSA desarrolló un programa masivo de intrusión digital basado en la adquisición, desarrollo y uso secreto de vulnerabilidades zero-day. Allí se explica que la agencia gestionaba un flujo constante de exploits que le permitían infiltrarse en sistemas de alto valor estratégico.

A su vez, la sección “A Growing Market” detalla cómo se creó toda una economía en torno a estas vulnerabilidades, alimentada por intermediarios, contratos confidenciales y un ecosistema de brokers que conectaban a hackers con agencias gubernamentales. Este mercado, como señala la autora, operaba casi por completo en la sombra.

Según la autora en la sección “The Price of Vulnerabilities”, los zero-days solo mantienen su valor mientras permanecen sin revelar. Una vez divulgados, son asignados a bases de datos como CVE, parchados por los fabricantes y pierden su utilidad ofensiva. Esto crea un incentivo directo para que las agencias no revelen la existencia de una vulnerabilidad, aun cuando afecta a millones de usuarios.

Ello conduce al dilema ético que atraviesa el libro:

¿Priorizar la seguridad colectiva o priorizar el valor ofensivo?

En la sección “The Shadow Brokers”, la autora describe uno de los eventos más significativos de la historia cibernética moderna: el robo y publicación de herramientas del NSA por parte de un grupo desconocido. La autora enfatiza que estas herramientas no estaban diseñadas para hacerse públicas y que su divulgación representó un riesgo sin precedentes.

En “Another Confidential Leak”, se analiza cómo estas filtraciones revelan la vulnerabilidad intrínseca del enfoque de acumulación: si un arsenal de ciberarmas es robado, el daño se propaga globalmente, y nada impide que otros actores reutilicen los exploits contra objetivos civiles o gubernamentales. Esto demuestra que la probabilidad de que un exploit acumulado se filtre no es cero, y que sus consecuencias pueden ser catastróficas.

Dado el contexto del libro, proponemos un modelo de decisión entre:

- Parchar (patch)
- Acumular (hoard)

Variables del modelo:

Estas variables reflejan lo que la autora describe en las secciones anteriores:

- V: Valor operativo que obtiene una agencia al explotar un zero-day

(inteligencia, infiltración, ventaja estratégica).

- P: Probabilidad de que el exploit sea descubierto o robado por un tercero.
- D: Daño económico-social si la vulnerabilidad se usa en ataques masivos.
- C: Costo asociado a que el fabricante parchee la vulnerabilidad.
- R: Costo político/reputacional si se descubre que un gobierno retuvo la vulnerabilidad.

Para evaluar las decisiones, utilizamos funciones de bienestar social, estándar en economía pública.

Si el gobierno decide parchar

$W_{patch} = - C$

Se elimina el riesgo global, pero se pierde el valor ofensivo que el gobierno podría haber explotado.

Si el gobierno decide acumular

$W_{hoard} = V - P * D - R$

V: beneficio táctico.

P · D: riesgo de una filtración o descubrimiento, tal como ocurrió con la publicación de las herramientas del NSA.

R: costo político si se revela que la agencia retuvo la vulnerabilidad.

Parchear es preferible cuando:

W_patch > W_hoard

Es decir:

P * D > V + C - R

Si el daño esperado supera el beneficio ofensivo, es racional parchar.

Cuando una agencia opta por acumular, incurre en un costo esperado:

CO_nopatch = P * D + R

Este concepto refleja exactamente lo que la autora describe en *"The Shadow Brokers"* y *"Another Confidential Leak",* el daño posible de perder el control sobre un exploit puede ser inmenso y propagarse globalmente.

El libro detalla en *"The Shadow Brokers"* que herramientas extremadamente poderosas desarrolladas por el NSA fueron publicadas y utilizadas en ataques posteriores por actores extranjeros. Si imaginamos un daño potencial elevado y una probabilidad moderada de filtración (como demuestran los eventos descritos), podemos observar que P · D puede superar fácilmente el valor ofensivo V.

Por ejemplo. si una agencia considera que una vulnerabilidad podría causar daños masivos si se filtra y existe un riesgo real de que ocurra una filtración, como evidencia *"The Shadow Brokers"*, entonces el costo de oportunidad de no parchar puede alcanzar niveles inaceptables.

El mercado de zero-days ha crecido sin transparencia, generando incentivos para acumular ciberarmas a pesar de los riesgos que estas representan cuando salen de control.

El modelo económico demuestra que acumular ofrece beneficios tácticos, pero implica riesgos catastróficos si la vulnerabilidad se filtra. El costo de oportunidad de no parchar puede ser enorme, afectando no solo a gobiernos sino a empresas y a la población civil. Por lo tanto, en muchos casos, desde una perspectiva económica y social, parchar es la opción óptima.

Ética, Regulación y Propuesta de Política

El libro *This Is How They Tell Me the World Ends*, de Nicole Perlroth, revela que el mercado de vulnerabilidades de día cero dejó de ser un espacio técnico de investigación y pasó a convertirse en un sistema global de ciberarmas alimentado por gobiernos, corredores privados y empresas de spyware. A través de entrevistas, documentos filtrados y testimonios de exagentes, la autora muestra cómo este ecosistema creció de manera descontrolada, impulsado por la demanda de exploits capaces de penetrar teléfonos, computadoras, servidores e infraestructura crítica sin dejar rastro, como se detalla en los capítulos 3 (The Cowbo) y 4 The First Broker"), donde se narra el nacimiento de este mercado con empresas como iDefense y los primeros intermediarios gubernamentales.

Lo más relevante es que, mientras el mundo dependía cada vez más del software, el mercado zero-day se expandía sin ninguna regulación significativa. Agencias como la NSA en Estados Unidos, el GCHQ británico, la Unidad 8200 israelí y servicios de inteligencia de diversos estados autoritarios comenzaron a competir por comprar vulnerabilidades antes que los propios fabricantes pudieran corregirlas, una dinámica explorada a fondo en la Parte III (The Spies), específicamente en los capítulos 8 (The Omnivore) y 10 (The Factory), que describen la expansión masiva de la recolección de datos y la industrialización del desarrollo de exploits.

Uno de los problemas centrales expuestos por Perlroth es el fracaso de los intentos de regulación internacional. Aunque existieron iniciativas como el Arreglo de Wassenaar para controlar la exportación de spyware, la presión de empresas tecnológicas, grupos de investigación y compañías de ciberinteligencia logró frenar cualquier avance real. Estados Unidos, a pesar de reconocer el riesgo, decidió no imponer controles estrictos, lo que consolidó a su territorio como uno de los centros globales del comercio de exploits. En el capítulo 11 (The Kurd), la autora explica cómo el gobierno estadounidense evitó adoptar las restricciones más severas de Wassenaar, permitiendo que empresas de vigilancia digital vendieran a clientes con historiales graves de abusos.

Este vacío regulatorio permitió que el mercado zero-day se vinculara directamente a violaciones de derechos humanos, como documenta Perlroth en el capítulo 12 (Dirty Business), donde muestra cómo la filtración de Hacking Team reveló ventas a Sudán, Etiopía, Egipto y otros regímenes represivos. Perlroth presenta casos emblemáticos: la filtración de la empresa italiana Hacking Team reveló que su spyware era utilizado por gobiernos represivos para vigilar y detener activistas, periodistas y opositores. Posteriormente, la historia de NSO Group y Pegasus mostró una evolución aún más sofisticada: herramientas capaces de infectar dispositivos iPhone mediante exploits de altísimo valor se empleaban para perseguir a defensores de derechos humanos como Ahmed Mansoor, quien fue blanco de repetidos intentos de espionaje digital antes de ser arrestado, según se expone en los capítulos 12 y 13 (Guns for Hire), donde la autora explica cómo Mansoor recibió repetidos mensajes con zero-days de iPhone vendidos por NSO a gobiernos del Golfo.

La autora profundiza también en el caso de Project Raven, un programa dirigido por exagentes de la NSA en Emiratos Árabes Unidos. Inicialmente presentado como un esfuerzo para combatir terrorismo, derivó rápidamente en operaciones clandestinas para hackear periodistas, activistas y gobiernos rivales. En el capítulo 11, la autora detalla la historia de David Evenden y otros exoperadores de la NSA que trabajaron para CyberPoint (y luego DarkMatter) en los Emiratos, dándose cuenta demasiado tarde de que sus capacidades estaban siendo utilizadas para reforzar la represión estatal.

Pero el aspecto más grave señalado por Perlroth no es solo el abuso directo, sino el riesgo sistémico global que surge cuando los gobiernos acumulan vulnerabilidades sin reportarlas. El dilema ético central del libro se resume en la pregunta: ¿es correcto retener una vulnerabilidad crítica para usarla en operaciones ofensivas, incluso si eso deja a millones de usuarios en riesgo?

La respuesta, según los hechos narrados, es contundente. El ejemplo de Shadow Brokers demuestra que ningún estado, por poderoso que sea, puede garantizar el control absoluto de sus arsenales digitales. Cuando este grupo filtró una colección de herramientas de la NSA, entre ellas EternalBlue, quedó expuesto el fracaso de la estrategia del "hoard": una vulnerabilidad mantenida en secreto durante años se convirtió de inmediato en un arma disponible para actores hostiles en todo el mundo, como se narra en el capítulo 21 (The Shadow Brokers). EternalBlue fue utilizado por Corea del Norte en WannaCry y por Rusia en NotPetya, como se expone en el capítulo 22 (The Attacks), donde Perlroth describe los ataques como devastadores: parálisis de hospitales, interrupciones en redes de transporte, caída de sistemas de radiación en Chernóbil, pérdidas millonarias para empresas como Maersk, FedEx y Merck, y un impacto global estimado en más de 10.000 millones de dólares.

Este episodio ilustra que retener vulnerabilidades no solo pone en riesgo a adversarios, sino también a aliados, empresas, infraestructura y ciudadanos comunes. La autora deja claro que acumular exploits sin divulgarlos se ha convertido en una amenaza que supera el ámbito militar: una sola filtración puede detonar una crisis internacional en cuestión de horas. A partir de estas evidencias, resulta evidente que la seguridad colectiva requiere un cambio profundo. Una política pública coherente con las lecciones del libro debería incluir tres elementos esenciales:

1. Regulación internacional estricta del mercado zero-day. Es necesario un marco que limite la venta de exploits y herramientas de intrusión, especialmente a gobiernos con historial de abusos. El modelo actual, basado en acuerdos voluntarios y débiles, ha demostrado ser insuficiente.
2. Un estándar global de divulgación responsable. Los estados deberían estar obligados a reportar vulnerabilidades críticas a los fabricantes en un plazo máximo definido. Mantener fallas abiertas por razones ofensivas solo amplifica el riesgo de que terminen reutilizadas contra la población global.

3. Priorizar el "patch" sobre el "hoard". El libro deja claro que el enfoque ofensivo ha sobrepasado los límites razonables y que la defensa tecnológica debe convertirse en la prioridad. Programas de bug bounty, auditorías abiertas y alianzas entre gobiernos y empresas pueden fortalecer la protección antes de que nuevas filtraciones provoquen daños irreversibles.

La conclusión que se desprende del análisis de Perlroth es que el mercado zero-day, tal como funciona hoy, pone en peligro la estabilidad digital mundial. Mientras las vulnerabilidades sigan considerándose armas para acumular en secreto, el riesgo de otro episodio como Shadow Brokers seguirá latente. La evidencia presentada en el libro muestra que la humanidad depende más de la corrección rápida de fallos que de la acumulación de herramientas ofensivas.

Después de los ataques narrados, especialmente NotPetya, resulta difícil justificar que gobiernos democráticos continúen participando en un mercado que ha demostrado ser imposible de controlar. Regular estrictamente, divulgar vulnerabilidades críticas y priorizar el parche sobre el arsenal no son medidas idealistas, sino la única respuesta responsable frente a un ecosistema donde cualquier error puede desencadenar una catástrofe global.

Las primeras etapas de la cadena de suministro de zero-days revelan un ecosistema que ha evolucionado dramáticamente de un mercado defensivo modesto a una industria armamentista multimillonaria global. Las cinco fases descritas ilustran cómo factores económicos y decisiones estratégicas han moldeado este mercado: desde el reconocimiento de amenazas estatales con Operation Aurora, descrito en el capítulo 14 (Aurora) , pasando por el establecimiento de diferenciales de precios insostenibles entre mercados defensivos y ofensivos detallado en el capítulo 15 (Bounty Hunters), la profesionalización del mercado con estándares técnicos, pero filtros éticos limitados, hasta la globalización completa sin restricciones y la normalización mediante transparencia de precios. Las tensiones fundamentales entre seguridad colectiva y capacidades ofensivas, entre incentivos económicos y responsabilidad ética, permanecen sin resolver mientras el mercado continúa expandiéndose. Esta base estructural y económica del mercado informa tanto el análisis cuantitativo de costos de oportunidad del dilema "parchear versus acumular" como las propuestas de política regulatoria, por ejemplo.