The Human Element and Defense Strategy: A Case Study of NotPetya

Proyecto Final – Information Security

Grupo 3

Tandazo Cobo, Xavier	00212431
Herrera Carrión, Pablo Andrés	00326431
Cantos Riera, Paulo Sebastian	00326682
López Ortiz, Ericson Daniel	00326945

Universidad San Francisco de Quito

Fecha 4/12/2025

Resumen

Este informe analiza *This Is How They Tell Me the World Ends* de Nicole Perlroth desde una perspectiva defensiva y centrada en el elemento humano. Tomamos como caso principal a NotPetya, porque en el libro aparece como un punto de quiebre: un ataque pensado dentro de un conflicto geopolítico, pero con consecuencias reales sobre infraestructura civil y operaciones empresariales a escala global. A partir de ese episodio, reconstruimos cómo una intrusión que empezó por una actualización de software en Ucrania terminó afectando redes corporativas completas, apoyándose tanto en fallas técnicas como en decisiones organizacionales acumuladas.

Además del análisis técnico (TTPs y cadena de ataque), el trabajo conecta el incidente con dos problemas que Perlroth repite a lo largo del texto. El primero es la fragilidad estructural de sistemas esenciales que operan con deuda técnica, proveedores críticos poco auditados y una cultura de "parchar después". El segundo es la brecha de talento en ciberseguridad: mientras el mercado ofensivo ofrece mejores incentivos y prestigio, la defensa queda subfinanciada y con menos capacidad de retención, lo que agrava el riesgo.

Finalmente, el informe argumenta una prioridad defensiva a nivel nacional coherente con la tesis del libro: reducir el incentivo a acumular vulnerabilidades y fortalecer la transparencia sobre el software que sostiene sectores sensibles. En conjunto, la lectura que proponemos es directa: los ataques no se vuelven catastróficos solo por la sofisticación del malware, sino porque encuentran organizaciones y Estados listos para fallar.

Índice

1. Introducción

La creciente dependencia entre sistemas digitales, infraestructura crítica y vida cotidiana ha hecho de la ciberseguridad un reto tan humano como tecnológico. En este contexto, nuestro grupo se propone analizar el papel clave que juegan las personas (usuarios, desarrolladores, defensores y atacantes) en la aparición, expansión y contención de ciberataques, basándose en el libro *This Is How They Tell Me the World Ends* de Nicole Perlroth. La autora subraya que el factor humano es el eslabón más débil de la cadena de seguridad. Errores mínimos pueden tener consecuencias enormes, decisiones mal enfocadas pueden abrir puertas invisibles al enemigo y una cultura que favorece la rapidez y la comodidad suele dejar la protección en segundo plano. Al mismo tiempo, Perlroth muestra cómo la defensa ha sido dejada atrás, mientras la ofensiva ha recibido fondos, incentivos y prestigio. Esto ha generado vulnerabilidades estructurales que actores como Rusia, China o Irán han sabido aprovechar.

Dentro de este panorama, NotPetya se convierte en el caso central del análisis. Este ataque resume lo peor de nuestras decisiones: errores humanos, negligencia organizacional y políticas ofensivas que terminaron volviéndose en contra de quienes las promovieron. Considerado el ataque cibernético más destructivo de la historia, NotPetya evidenció cómo una brecha en un proveedor de software aparentemente menor, sumada al uso de armas digitales desarrolladas por la NSA y luego filtradas, puede causar un daño económico global de escala masiva.

Este documento se estructura en cuatro partes. Primero, se presenta un repaso al caso NotPetya y las herramientas empleadas. Luego, se analiza la brecha de talento en ciberseguridad. Después, se describen las principales estrategias de mitigación y defensa. Finalmente, se ofrece una reflexión crítica sobre la necesidad de priorizar la ciberdefensa, a partir de los argumentos del libro. En conjunto, cada sección busca mostrar cómo el elemento humano, con sus aciertos y sus fallas, está en el centro de los desafíos actuales en seguridad digital, y por qué enfrentar estas amenazas exige más que soluciones técnicas: requiere voluntad, responsabilidad compartida y una nueva forma de pensar la protección digital.

2. Marco Teórico

El libro *This Is How They Tell Me the World Ends*, de Nicole Perlroth, sirve como base conceptual para entender cómo interactúan las vulnerabilidades técnicas, los incentivos ofensivos, los errores humanos y la fragilidad de nuestras infraestructuras digitales. Desde la acumulación de fallos no corregidos hasta la falta de responsabilidad institucional, la autora deja claro que la inseguridad global no es solo un problema tecnológico: es, sobre todo, un problema humano y estructural. Este marco teórico resume los conceptos esenciales que permiten analizar el caso NotPetya y plantear estrategias de defensa acordes con los desafíos actuales.

2.1. Zero-days y ciberarmas

Los zero-days son fallos desconocidos por los fabricantes, lo que significa que no existen parches disponibles para corregirlos. En su libro, Perlroth describe un mercado global multimillonario en el que gobiernos, intermediarios privados y actores ofensivos compran y

venden estas vulnerabilidades con fines de espionaje o guerra digital. Su alto valor radica en que permiten acceder a sistemas altamente protegidos sin dejar rastro. Las ciberarmas, es decir, exploits diseñados para aprovechar estos zero-days, se han vuelto herramientas estratégicas, pero su acumulación representa un riesgo enorme. Cuando se filtran, como ocurrió con los exploits de la NSA (EternalBlue y EternalRomance), las consecuencias pueden ser impredecibles y de escala global. NotPetya es el ejemplo más claro de cómo una ciberarma diseñada para fines ofensivos puede terminar causando estragos cuando cae en manos equivocadas.

2.2. TTPs (Tactics, Techniques and Procedures)

Las TTPs explican cómo se ejecuta un ataque: desde la intrusión inicial hasta su propagación e impacto. En el caso de NotPetya, y tal como lo detalla Perlroth, estas tácticas incluyeron la explotación de vulnerabilidades sin parchear, el uso de herramientas de movimiento lateral como PsExec y WMI, el robo de credenciales mediante Mimikatz, y la distribución automática del malware dentro de redes internas. Comprender las TTPs es clave para analizar el comportamiento de los atacantes, y permite construir modelos como MITRE ATT&CK que ayudan a anticipar, detectar y responder frente a amenazas complejas. El análisis técnico de NotPetya se basa en estas TTPs para reconstruir su cadena de ataque.

2.3. Infraestructura crítica y riesgos

Uno de los puntos más inquietantes del libro es la fragilidad de los servicios esenciales, como energía, salud, transporte, logística y finanzas, que dependen de sistemas digitales llenos de fallas históricas, escasa inversión en defensa y políticas más reactivas que preventivas. Muchas veces, estas infraestructuras están a cargo de proveedores externos con recursos limitados, prácticas inseguras o cadenas de suministro mal aseguradas. NotPetya expuso esa debilidad. Un software tributario ucraniano relativamente pequeño, M.E.Doc, fue el punto de entrada que permitió comprometer redes globales. La interconexión entre sectores agrava los riesgos, ya que lo que empieza como una falla local puede escalar en cuestión de minutos a una crisis internacional. Este marco explica cómo configuraciones deficientes o parches sin aplicar pueden provocar efectos en cascada.

2.4. Factores humanos en ciberseguridad

El componente humano está en el centro del problema. Según Perlroth, muchas de las fallas más críticas no son causadas por fallos técnicos, sino por decisiones humanas: malas prácticas operativas, errores de programación, falta de segmentación, clics en correos de phishing y una cultura generalizada de negligencia. A esto se suman problemas estructurales, como políticas que retienen vulnerabilidades (como NOBUS), entornos corporativos donde se privilegia la velocidad sobre la seguridad, escasa capacitación y una desconexión evidente entre equipos técnicos y directivos. NotPetya fue posible gracias a una serie de fallas humanas repartidas en distintos niveles, tanto en Ucrania como en organizaciones multinacionales. Este factor humano será clave para analizar la defensa, la brecha de talento y las propuestas que se presentan en las siguientes secciones.

3. Caso de Estudio: NotPetya (Prólogo; Capítulo 22: The Attacks)

3.1. Contexto del ataque

NotPetya llegó en un momento de gran tensión entre Ucrania y Rusia. Desde la revolución de 2014 que llevó a la salida del presidente prorruso Viktor Yanukóvich, Rusia había anexado Crimea y emprendió una agresiva campaña cibernética multidimensional contra Ucrania. Como Perlroth describió vívidamente en el prólogo de su libro, mucho antes del ataque global, Ucrania se convirtió en el "campo de pruebas" de las armas cibernéticas rusas. Durante varios años, Ucrania fue víctima de ataques coordinados a ministerios, campañas de desinformación y actos de sabotaje, incluidos los cortes de energía de 2015 y 2016. Lo que realmente ocurrió allí no fue solo un ataque, sino parte de una estrategia híbrida que combinaba ciberataques y presión política mediante acción militar. Según expertos locales, Ucrania estaba siendo utilizada como terreno de prueba para ensayos que posteriormente apuntarían a Occidente.

Fue en ese contexto que M.E.Doc, el software de contabilidad tributaria desarrollado por la empresa ucraniana Linkos Group, se convirtió en el punto de entrada del ataque. Aunque provenía de una firma pequeña, la aplicación era utilizada por la mayoría de las empresas e instituciones gubernamentales del país. Esa dependencia crítica resultó ser la grieta perfecta. Los atacantes tomaron el control de los servidores de actualización de la empresa y distribuyeron una actualización con malware. Miles de usuarios, al instalarla, abrieron sin saberlo las puertas de sus redes a NotPetya. La confianza en un proveedor clave transformó una pequeña debilidad en un desastre nacional y luego global.

3.2. Cadena de ataque (Kill Chain)

Todo comenzó con un vector de compromiso que, a primera vista, parecía rutinario: una actualización de software. Perlroth describe cómo los atacantes utilizaron a M.E.Doc —un sistema tributario ampliamente extendido en Ucrania— como punto de entrada mediante una actualización troyanizada. El simple acto de descargar e instalar ese paquete, en un equipo conectado a la red corporativa, fue suficiente para introducir el malware en entornos empresariales que luego servirían como puente hacia operaciones fuera del país. La autora enfatiza que el daño no dependió de una intrusión manual prolongada, sino de la combinación entre confianza en la cadena de suministro y redes interconectadas, donde una sola instalación podía convertirse en el detonante de una crisis transnacional (Perlroth, sección sobre NotPetya).

Una vez dentro, el ataque se desplegó con una lógica de propagación diseñada para maximizar velocidad y alcance. En el relato de Perlroth, NotPetya explotó vulnerabilidades de Windows mediante herramientas filtradas del arsenal de la NSA, en particular EternalBlue y EternalRomance, lo que permitió moverse de manera autónoma entre equipos vulnerables sin necesidad de intervención humana constante. En paralelo, incorporó el robo de credenciales como multiplicador: al extraer contraseñas y *hashes* desde memoria (por ejemplo, con Mimikatz), el malware pudo extenderse también a sistemas que ya estaban parchados para SMB, penetrando a través de accesos legítimos capturados dentro del entorno. Este com-

portamiento se vio amplificado por una condición organizacional recurrente: redes planas o pobremente segmentadas, donde la caída de un solo host no quedaba contenida en un segmento, sino que abría el camino hacia dominios completos y, con ello, hacia sedes y filiales conectadas globalmente. De ahí la observación de la autora sobre cómo "un solo empleado ucraniano trabajando de forma remota" podía poner en riesgo a una multinacional entera, no por sofisticación individual, sino por la arquitectura y la dependencia digital acumulada (Perlroth, capítulo "The Attacks").

3.3. TTPs técnicos utilizados

En términos tácticos, Perlroth presenta a NotPetya como un híbrido entre capacidad estatal y pragmatismo operativo: no se apoyó únicamente en *zero-days* exóticos, sino en herramientas eficaces, ya conocidas y, en varios casos, disponibles tras las filtraciones. El núcleo técnico del ataque fue la explotación de SMB a través de EternalBlue y EternalRomance, lo que le dio una capacidad "wormable" para replicarse y avanzar rápidamente por redes con equipos vulnerables. Esta capa de explotación se complementó con técnicas de escalamiento interno basadas en credenciales: Mimikatz, originalmente difundida como prueba de concepto, se convirtió en una pieza clave para capturar secretos en memoria y reutilizarlos para moverse lateralmente con autenticación válida. En la práctica, esto redujo la dependencia del atacante de encontrar más vulnerabilidades; bastaba con "caminar" la red con identidades robadas (Perlroth, capítulo "The Attacks").

Además, el malware aprovechó utilidades legítimas propias de administración en Windows, como PsExec y WMI, para ejecutar comandos de manera remota y distribuir la carga maliciosa como si se tratara de operación interna. Este detalle es importante porque borra la frontera entre actividad administrativa normal y actividad hostil, dificultando detección temprana en organizaciones sin telemetría ni monitoreo profundo. Finalmente, Perlroth subraya el carácter destructivo del incidente: aunque NotPetya se presentó como ransomware, su lógica real era la de un *wiper*. La nota de rescate funcionó como fachada, mientras el resultado práctico era la pérdida irreversible de datos y la inutilización masiva de sistemas, lo que explica el nivel de disrupción observado y la complejidad de la recuperación posterior (Perlroth, sección sobre NotPetya).

3.4. Impacto en infraestructura crítica

El impacto en Ucrania fue inmediato porque el ataque golpeó servicios que sostienen la vida cotidiana y la continuidad del Estado. Perlroth describe pantallas negras generalizadas y la interrupción de operaciones básicas: ciudadanos sin acceso a cajeros automáticos, fallas en pagos en estaciones de servicio, y parálisis de sistemas asociados a transporte, logística y servicios públicos. En el plano institucional, el incidente afectó redes de agencias gubernamentales y organizaciones críticas, generando un colapso digital que se sintió tanto en la administración pública como en el sector privado. El episodio de Chernóbil condensa el riesgo humano: con sistemas de monitoreo fuera de línea, ingenieros se vieron forzados a medir radiación manualmente, evidenciando cómo un ataque informático puede trasladarse, en minutos, a escenarios de seguridad física y ambiental (Perlroth, capítulo "The Backyard" / pasajes sobre NotPetya y Chernóbil).

El daño, sin embargo, no quedó confinado a Ucrania. Por diseño y por conectividad empresarial, NotPetya se propagó a compañías internacionales con operaciones, proveedores o empleados vinculados a redes ucranianas. Perlroth relata la afectación de gigantes como Maersk, con envíos globales detenidos mientras intentaban reconstruir sistemas de inventario; Merck, con interrupciones severas que impactaron producción; y FedEx/TNT, con parálisis logística y pérdidas millonarias. También menciona afectaciones en firmas y conglomerados como DLA Piper, Reckitt Benckiser y Mondelez, y destaca el efecto bumerán del ataque, que terminó impactando incluso a organizaciones rusas como Rosneft. En la evaluación que reconstruye la autora, las pérdidas globales superaron los diez mil millones de dólares, mostrando que el costo real de una ciberarma fuera de control se mide en disrupción sistémica y daño económico prolongado, no solo en equipos cifrados (Perlroth, capítulo "The Backyard" y capítulo "The Attacks").

3.5. Fallas humanas y organizacionales

Aunque NotPetya incorporó herramientas avanzadas, Perlroth insiste en que su devastación fue posible por una suma de fragilidades humanas y organizacionales acumuladas. El primer eslabón fue un problema de cadena de suministro: una dependencia crítica de M.E.Doc sin controles robustos de verificación, auditoría o aislamiento, lo que convirtió una actualización "confiable" en el vehículo perfecto para la intrusión inicial (Perlroth, sección sobre NotPetya). A esto se sumó la deuda técnica: sistemas desactualizados, entornos con parches pendientes y una cultura de postergación de actualizaciones que dejó abiertas superficies de ataque explotables por SMB. La autora también menciona cómo el uso de software no correctamente licenciado y, por tanto, no parchado en algunos contextos agravó la imposibilidad de aplicar correcciones a tiempo, ampliando el universo de máquinas vulnerables.

En el plano arquitectónico, la falta de segmentación transformó lo que pudo ser un incidente localizado en una propagación transversal. Redes "planas", credenciales privilegiadas expuestas y ausencia de controles de contención permitieron que el malware pasara de un equipo inicial a controladores de dominio y sistemas centrales. Y cuando llegó el momento de recuperarse, muchas organizaciones evidenciaron un vacío crítico: planes insuficientes de continuidad, respaldos no resilientes y capacidad limitada para reconstruir desde cero bajo presión. Finalmente, Perlroth vincula estas fallas con un problema estratégico mayor: la retención de vulnerabilidades bajo lógicas como NOBUS y los límites del VEP. La filtración de herramientas por *Shadow Brokers* mostró cómo la acumulación ofensiva puede terminar alimentando ataques de terceros, convirtiendo capacidades estatales en riesgo público. En ese sentido, NotPetya no fue solo un fallo de seguridad técnica: fue el resultado de decisiones humanas equivocadas, tomadas a distintos niveles, que dejaron el ecosistema listo para colapsar cuando el malware llegó (Perlroth, capítulos sobre Shadow Brokers/NOBUS y capítulo "The Attacks").

4. Brecha de Talento en Ciberseguridad (Capítulo 5 – Zero Day Charlie, Capítulo 11 – The Kurd, Capítulo 13 – Guns of Hire, Capítulo 17 – Cyber Gauchos)

La escasez de profesionales cualificados en ciberseguridad no es solo un problema de falta de formación académica, sino una consecuencia directa de las dinámicas económicas y geopolíticas del mercado de vulnerabilidades.

4.1. Incentivos ofensivos

El dinero está en el ataque y esta es una de las principales razones de la brecha de talento en ciberseguridad. Un caso puntual de la fuerte motivación del dinero es Charlie Miller, ex trabajador de la NSA, quién reveló públicamente la compra de exploits por parte de la NSA y además empezó con la ideología "No More Free Bugs" para que los trabajadores de ciberseguridad dejen de entregar exploits a empresas a cambio de prácticamente nada o forzados por amenazas. Charlie Miller no solo promovió esta idea, sino que también la aplicó en el caso de "Zero Day Charlie" donde vendió una vulnerabilidad de Linux por $50000.

Esta tendencia de ir hacia la ofensiva se agudizó más con la incapacidad de las empresas buscaban parchar una vulnerabilidad frente a la competencia y posible ganancia adicional de utilizar esa vulnerabilidad para obtener información confidencial e importante.

4.2. Mercado gris

La venta de exploits y zero days se encuentra en la delgada franja entre lo legal e ilegal. Si bien existen normativas y regulaciones relacionadas con el uso de información ajena, no existen (posiblemente jamás existan) regulaciones sobre derechos y propiedad intelectual relacionada al descubrimiento de vulnerabilidades y, por esta razón, las vulnerabilidades se consideran mercado gris al ser solo una herramienta que según como se la utilice puede ser legítimo (defensa/parchado de vulnerabilidades) o ilegal (ataque/espionaje e invasión de privacidad). La gran demanda de información, espionaje e intervención silenciosa de equipos tecnológicos junto con las recompensas adyacentes fue la semilla para que surja el mercado gris de la venta de exploits que sigue operando hasta la actualidad.
Desde contratos y transacciones directas y secretas el mercado gris se fue expandiendo a medida que esta demanda aumentaba y era solicitada por más países y agencias, incluso aquellas entidades que no poseían un conocimiento técnico o personal capacitado en ciberseguridad. Tal es el caso de la llegada al mercado de brokers como Zerodium, quienes ofrecían millones de dólares por exploits para Iphone que luego vendían a agencias gubernamentales u otras empresas; o el caso de NSO Group, una empresa israelí encargada de ofrecer servicios de espionaje directamente con software como Pegasus (Enrique Peña Nieto lo utilizó durante su gobierno en México) que amplió el mercado al ofrecer un servicio accesible para el cliente independientemente de si tenía conocimiento o no en la parte de vulnerabilidades.

4.3. Fuga de cerebros (DarkMatter, Emiratos, etc.)

Si bien el mercado gris fue el principal centro de comercio y dónde la mayoría de los expertos en el área pasaron del mercado defensivo hacia el ofensivo también existieron otras burbujas más separadas que incentivaron esta brecha de talento como el caso de la fuga de cerebros, donde empresas y entidades empezaron contratar a profesionales y expertos de agencias gubernamentales y entidades que tenían áreas dedicadas a la seguridad informática.

La fuga de cerebros se evidenció claramente con la empresa CyberPoint, posteriormente llamada DarkMatter (Project Raven), que empezó a reclutar a operadores de la NSA como David Evenden para trabajar en los Emiratos Árabes Unidos, quienes fácilmente aceptaros debido a los salarios libres de impuestos y la mayor remuneración otorgada por esta empresa. Sin embargo, CyberPoint no quería estancarse en el área defensiva. Aunque inicialmente se les presentó a los exoperadores de la NSA una misión defensiva (la çarpeta violeta", defender a EAU de ciberataques), la realidad operativa (la çarpeta negra") implicaba utilizar sus habilidades para ejecutar ofensivas avanzadas y lograr espiar a disidentes, rivales geopolíticos como Qatar e incluso ciudadanos estadounidenses. Estos operadores, sin tener posibilidad de dar marcha atrás indirectamente transicionaron de un uso ético y defensivo de vulnerabilidad a la utilización de exploits para otras actividades, abriendo más la brecha de talento.

4.4. Problemas al contratar defensores

Mientras el sector ofensivo y el mercado gris continuaban con una alta demanda, compensaciones millonarias y el atractivo de trabajar con herramientas de vanguardia, el sector defensivo, especialmente en el gobierno civil, luchaba por captar talento para cuestiones defensivas.

Lamentablemente, el capturar talento para la parte defensiva en seguridad era prácticamente imposible. La principal razón es económica: para las empresas y gobiernos el incentivar profesionales a la defensa supone un gasto que posiblemente no sea compensado respecto a las ganancias de la entidad; mientras tanto, el incentivo hacia la ofensiva genera dinero tanto para las empresas (uso de información) como para los hackers lo cuál es viable a largo plazo a diferencia de la captura de talentos para la defensa que involucra gastos internos.

Por otro lado, a medida que el mercado se expandía, el incentivo para ir hacia el lado ofensivo dejo de ser meramente económico: muchos profesionales preferían trabajar en nuevas tecnologías y procesos que dar soporte a sistemas, donde la mayoría eran obsoletos; además, el surgimiento de grupos hacktivistas como Anonymous indicó una nueva tendencia a realizar hacking ofensivo a manera de protesta y manifestación de ciertos ideales.

4.5. Consecuencias globales

La creciente demanda y expansión del mercado gris no solo afectó a empresas y agencias en términos del nacimiento de brokers y fugas de cerebros, el lado proveedor (hackers) fue también altamente influenciado. Muchos universitarios que cursaban carreras de tecnología estaban fuertemente influenciados a ir hacia trabajos de hacking ofensivo; por otro lado, en países con situaciones económicas problemáticas, como el caso de Argentina y su elevada inflación, nacieron grupos de hacking como los "Cyber gauchos" quienes se adentraron a tempranas edades al mundo del hacking por la necesidad y restricciones del país de acceder a las nuevas tecnologías, así como la necesidad económica similar al caso en América Latina de niños y adolescentes que se adentran en el mundo de armas y drogas por la necesidad y situación económica que viven.

Dentro del grupo de los Cyber Gauchos se puede destacar a Alfredo Ortega, quién había puesto toda su dedicación en encontrar vulnerabilidades y maneras de hackear sistemas, hasta al punto de realizar prototipos de emisores de ondas de radio con el fin de intervenir sistemas aislados. Este surgimiento de células de hacking por necesidad expandió el mercado en el ámbito de oferta, mostrando que no solo superpotencias como USA pueden enfocarse en el hacking ofensivo, teniendo menos control de exploits actualmente descubiertos a la vez que existen más vulnerabilidades disponibles en un instante de tiempo.

4.6. Cultura, Ética en la Formación y soluciones parciales al talent gap

Como se puede evidenciar del análisis previo, la problemática del hacking ofensivo es algo prácticamente imposible de solucionar, ya que mientras exista demanda de información, espionaje y control de sistemas ajenas va a existir inherentemente personas y grupos dispuestos a buscar vulnerabilidades y explotarlas ya sea por temas económicos, ideológicos o simplemente poder. A pesar de ello, existen ciertas soluciones parciales que mitigan la cantidad de hacking ofensivo más no lo eliminan. Una de ellas es el hecho de "combatir fuego con fuego" capturando talentos hacia el hacking defensivo ofreciendo compensaciones elevadas y renombre. Tal es el caso de iniciativas privadas como Project Zero de Google contratando a los mejores hackers del mundo (como el prodigio surcoreano Lokihardt).; sin embargo, los recursos y capacidad de inversión es un limitante para la mayoría de las empresas y agencias gubernamentales al optar por esta opción.

Por otro lado, está la legalización del hacking. Similar a la legalización de drogas y armas va a tener ventajas en el sentido de que las transacciones y una parte el mercado de exploits sea más visible; sin embargo, siempre va a existir la necesidad de transacciones secretas para ciertas necesidades.

Finalmente, la tercera solución parcial es el lado de éticas y normativas. Educar a los nuevos profesionales en colegios y universidad sobre el lado oscuro del hacking y vulnerabilidades donde vidas de personas pueden estar en riesgo cuando sistemas como hospitales,

centrales eléctricas o nucleares son comprometidos por vulnerabilidades descubiertas que talvez no fueron pensadas para ser armas o herramientas para actividades poco éticas e ilegales.

Si bien no se puede eliminar este mercado gris de exploits, cada persona y agencia tiene la decisión final sobre qué desean hacer con su información (física o digital), donde publicarla o exponerla y que debe ser estrictamente necesario expuesto en sitios de posible acceso no deseado como el internet.

5. Estrategias de Mitigación y Defensa (Capítulo 14: Aurora; Capítulo 19: The Grid; Epílogo)

5.1. Mitigaciones que habrían detenido NotPetya

El análisis técnico realizado del ataque, revela que NotPetya no era imparable como se presupone; fue la combinación relativamente pequeña de medidas básicas lo que habría reducido drásticamente su impacto o, y nos atrevemos a decir, que incluso impedido su propagación.

a) **Aplicación del parche MS17-010.** EternalBlue, ya había sido parchado por Microsoft tres meses antes del ataque según Greenberg, esto ya que ese mismo año había ocurrido el popular "WannaCry". La presencia de sistemas sin actualizar, incluyendo servidores que aún operaban con Windows 2000 y máquinas con backlog de parches de años, permitió que el exploit tuviera un potencial alcance.

b) **Segmentación de red adecuada.** La arquitectura plana que manejaban en Maersk, Merck o los bancos ucranianos hizo posible que la infección de una única máquina sea capaz de propagar el ataque a oficinas globales en cuestión de segundos, por ello, firewalls internos o una microsegmentación de red habrían limitado la catástrofe a un dominio local.

c) **Autenticación multifactor (MFA) y restricciones a credenciales privilegiadas.** Mimikatz, realmente, sólo fue devastador porque muchas organizaciones y empresas mantenían sus credenciales en memoria, por WDigest. Por esta razón, muchas cuentas administrativas fueron fácilmente vulnerables. Un sencillo proceso de MFA para usuarios privilegiados y vaults de credenciales habrían bloqueado la expansión automática del malware.

d) **Respaldos fuera de línea (air-gapped).** Está documentado que, uno de los factores más críticos del incidente fue la destrucción simultánea de todos los controladores de dominio globales de varias empresas, un ejemplo claro fue Maersk y su recuperación, que fue posible únicamente por un servidor que estaba apagado por accidente.

e) **Verificación reforzada de la cadena de suministro.** NotPetya utilizó actualizaciones oficiales de M.E.Doc, firmadas y distribuidas por un proveedor que ya había sido

comprometido; es necesario llevar a cabo procesos y controles de transparencia y revisión del código de actualizaciones habrían dificultado la inserción del malware.

5.2. Defensa en profundidad

Este caso particular de NotPetya, nos demuestra que las organizaciones no pueden depender de un único control de seguridad, pues la defensa en profundidad implica superponer capas de protección manera sucesiva, asumiendo que cada una de ellas podría fallar en cualquier momento. Es entonces que, a partir del análisis de este incidente, se identifican los siguientes pilares:

a) **Separación interna de la red.**
La red de una empresa, u organización de talla nacional, no debe bajo ningún concepto funcionar como una única autopista al que cualquier equipo puede llegar. Es vital entonces crear firewalls y servidores críticos, para ayudar a limitar la propagación de un ataque y evitar que una sola infección afecte a toda la organización, como pasó con NotPetya.

b) **Detección temprana y visibilidad.**
Es necesario contar con herramientas que alerten sobre comportamientos anómalos de manera inmediata, como accesos inusuales o conexiones inesperadas, que permitan a una empresa reaccionar antes de que el incidente se convierta en un desastre total.

c) **Despliegue seguro del software.** Cualquier cambio o actualización debe pasar por revisiones; se hablan de pruebas previas y un formidable monitoreo posterior. De esta forma no solo se reduce cualquier posibilidad de introducir errores a los servicios, sino que además, dificulta que software malicioso pase desapercibido.

5.3. Resiliencia en infraestructura

La resiliencia debería significar una garantía de que la organización pueda seguir operando incluso bajo condiciones adversas. El caso Maersk es una prueba más que ilustrativa: su reconstrucción total fue posible gracias a un único servidor en Ghana que sobrevivió accidentalmente.

A partir de esta observación, podríamos señalar tres principios claves y fundamentales:

a) **Arquitecturas diseñadas para fallos catastróficos.** La posibilidad de perder simultáneamente todos los controladores de dominio siempre debe ser parte del modelo de amenazas, ya que es el peor de los casos. En estos casos, por ejemplo, sería recomendable tener un respaldo desconectado de una aplicación crítica:

"Si todo el servidor principal desaparece, aún se puede reinstalar el sistema desde una copia segura que nunca tocó la red."

b) **Independencia de sistemas críticos.** Operaciones esenciales, digase por ejemplo los procesos de facturación o logística, deben poder funcionar (al menos temporalmente) sin depender de toda la infraestructura central, pues la idea en casos como Not Petya, es que las interrupciones totales no deberían paralizar la organización entera por completo.

c) **Planes operativos alternos.** Cuando el funcionamiento de Maersk se paralizó, el uso de WhatsApp, pizarras, facturación a mano y comunicación externa improvisada, demostraron la necesidad de canales previamente estabecidos para poder coordinar acciones cuando la red corporativa está caída.

d) **Capacitación para situaciones de riesgo.** Es pertinente la creación de programas continuos de formación para administradores, departamento de tecnología y personal operativo sobre detección temprana y protocolos de aislamiento; habría sido menos improvisada la reacción si se hubieran realizados simulacros regulares ante ataques informáticos.

5.4. Lecciones del libro y del caso

En el libro de de Perlroth, y varios análisis al caso NotPetya, se convergen en una sola conclusión común:

> La debilidad no está en el software solamente, sino también en las decisiones y responsabilidades humanas, políticas y organizacionales.

- **La seguridad no debe ser opcional o postergada.** Tal y como se contempla con Maersk o los bancos ucranianos, las organizaciones habían normalizado operar con vulnerabilidades conocidas, incluso después de incidentes similares, como WannaCry. La mentalidad de: "arreglarlo cuando se pueda" debe desaparecer, pues la seguridad es tan importante como un proceso de logística o facturación.

  En el libro, en el capítulo del ataque Aurora, Perloth menciona que las empresas no suelen tomarse la ciberseguridad como una prioridad hasta que algo de magnitudes catastróficas ocurre; el caso de Google siendo hackeada por China, fue el inicio de un estricto protocolo MFA para todos los empleados de la compañía, algo que hasta Aurora, solo era relegado a los altos cargos o personal con privilegios.

- **Las tensiones geopolíticas impactan directamente al sector privado.** Igual que en el caso Aurora descrito por Perlroth, NotPetya demuestra que los conflictos entre Estados pueden traducirse en daños colaterales multimillonarios para empresas sin relación directa con el conflicto.

  Perloth menciona, que situaciones políticas tan delicadas han requerido la intervención de informáticos para crear una defensa más óptima ante posibles ataques. En Estados Unidos por ejemplo, Perloth menciona que organizaciones nacionales importantes como el Pentágono, crearon e impulsaron programas para mejorar la infraestructura de seguridad de sus servicios.

  Aún así, tanto el libro como los estudios de incidentes destacan la dificultad de reclutar y retener personal de ciberseguridad capaz de diseñar arquitecturas robustas y responder a incidentes catastróficos. Esta brecha amplifica la vulnerabilidad de gobiernos e infraestructura crítica.

- **La seguridad debe ser gobernanza institucional, no solo tecnología.** Incentivos, KPIs, responsabilidades, auditorías y cultura interna son tan importantes como los parches o las herramientas que se pueden llegar a proporcionar. NotPetya funcionó, únicamente porque las organizaciones habían construido entornos donde un error podía escalar globalmente, y los mismos nunca fueron prioridad para ningún ministerio, aún y con la delicada relación Rusia.

6. Prioridad Defensiva Más Crítica (Capítulo 9: The Rubicon; Capítulo 16: Going Dark; Epílogo)

6.1. Propuesta de política nacional

Tras analizar la evidencia presentada por Perlroth, la postura central es que la medida defensiva más crítica no es únicamente técnica, sino política: reformar de raíz el *Vulnerabilities Equities Process* (VEP). El VEP es el mecanismo gubernamental mediante el cual Estados Unidos decide si una vulnerabilidad (por ejemplo, un *zero-day*) debe divulgarse al fabricante para ser parchada, o si debe retenerse para operaciones de inteligencia y capacidades ofensivas. En teoría, el proceso busca equilibrar la seguridad pública con las necesidades de espionaje; en la práctica, el libro muestra que ese equilibrio se ha inclinado históricamente hacia la retención, bajo supuestos que ya no sostienen el mundo actual.

Por ello, la política propuesta es priorizar la divulgación rápida y verificable de vulnerabilidades en tecnologías ampliamente utilizadas (sistemas operativos, protocolos, servicios críticos) para que los fabricantes parcheen antes de que esas fallas se conviertan en ciberarmas reutilizables. Esta reforma debe acompañarse de controles que hagan el proceso auditable, con plazos de retención limitados y métricas públicas agregadas, de modo que la lógica defensiva no dependa de confianza ciega en agencias cuyo incentivo natural es "guardar" herramientas.

6.2. Justificación basada en el libro: el problema de fondo (NOBUS)

La necesidad de reformar el VEP se entiende mejor a través de la doctrina **NOBUS** (*Nobody But Us*). Perlroth describe NOBUS como el cálculo interno que asume que "nadie más que nosotros" tiene la capacidad de descubrir o explotar ciertas vulnerabilidades, lo que justificaría retenerlas. El problema es que el propio relato del libro desmonta esa premisa: el mercado de *exploits* se ha expandido, se ha privatizado y se ha globalizado. Ya no existe un monopolio real de sofisticación técnica; adversarios estatales y actores criminales pueden comprar, replicar o redescubrir fallas similares.

Peor aún, el libro muestra cómo filtraciones como las de *Shadow Brokers* expusieron que la retención no era únicamente de fallas "NOBUS-level", sino también de vulnerabilidades plausibles de encontrar por múltiples actores. Ese contraste deja una conclusión incómoda: acaparar fallas en nombre de la ventaja ofensiva no solo no garantiza exclusividad, sino que amplía el riesgo sistémico para hospitales, redes eléctricas, gobiernos locales y empresas que

dependen de ese mismo software.

6.3. Cómo habría mitigado NotPetya: el caso EternalBlue como evidencia

NotPetya funciona en el libro como el ejemplo definitivo del "efecto bumerán". Su propagación masiva se apoyó en herramientas que aprovecharon vulnerabilidades críticas, entre ellas **EternalBlue**, un *exploit* asociado a fallas en Microsoft Windows. La historia que reconstruye Perlroth enfatiza un punto clave para esta sección: cuando una vulnerabilidad se retiene durante años en un sistema ampliamente desplegado, el costo potencial de una filtración o reutilización se vuelve catastrófico.

Si el VEP hubiese operado bajo una prioridad defensiva robusta (divulgación temprana en tecnología ubicua, límites de retención, y una cultura institucional que penalice la acumulación), el ecosistema habría tenido una ventana de protección más amplia: parches antes, adopción antes y, sobre todo, menos tiempo de exposición estructural. NotPetya no fue solo un malware destructivo; fue la demostración de que una decisión "racional" en clave ofensiva puede convertirse en una vulnerabilidad global cuando el código se filtra, se replica y se usa fuera de control.

6.4. Transparencia radical: exigir una Lista de Materiales de Ciberseguridad (SBOM)

La reforma del VEP reduce el riesgo "aguas arriba" (qué fallas se corrigen y cuándo), pero Perlroth insiste en otra fragilidad: la opacidad del software que sostiene infraestructura crítica. Operamos con dependencias, librerías y componentes de terceros como si fueran una caja negra; cuando aparece una vulnerabilidad grave, muchas organizaciones ni siquiera saben si están afectadas, dónde exactamente, y qué deben aislar primero.

Por ello, una segunda medida defensiva prioritaria es exigir una *Cybersecurity Bill of Materials* (SBOM) para software y sistemas utilizados en infraestructura crítica y sectores sensibles (por ejemplo, salud, energía, finanzas). La lógica es simple: del mismo modo que una etiqueta permite saber qué contiene un producto, un SBOM permite identificar componentes y dependencias para responder con rapidez ante vulnerabilidades, priorizar parches y ejecutar auditorías efectivas. Sin esta transparencia, la respuesta a incidentes se vuelve lenta, reactiva y costosa; con ella, se acelera la contención y se reduce el radio de explosión.

6.5. Implicaciones humanas: talento, ética y defensa como cultura

Perlroth deja claro que la seguridad no es abstracta. La discusión sobre zero-days, procesos burocráticos y *exploits* aterriza en consecuencias humanas: hospitales interrumpidos, servicios degradados, ciudades paralizadas y pérdidas que terminan afectando a poblaciones enteras. En ese marco, la defensa requiere más que controles técnicos: necesita personas, incentivos y cultura.

Aquí entra el componente humano que conecta con la "crisis de talento" descrita en el texto. La autora muestra cómo el mercado y la geopolítica empujan a muchos de los mejo-

res perfiles hacia lo ofensivo: mejores sueldos, herramientas más atractivas y menos fricción institucional. En paralelo, la defensa queda subfinanciada, burocratizada y normaliza operar con deuda técnica. Por ello, la política defensiva debe incluir incentivos para reportar vulnerabilidades de forma responsable (programas de *bug bounty* competitivos a nivel nacional, expansión de auditorías y apoyo a infraestructura crítica), y formación ética obligatoria para evitar la desensibilización: que el código se vea como un "puzzle" aislado de sus consecuencias.

En síntesis, la reforma del VEP y la transparencia vía SBOM funcionan si la defensa se dignifica: atraer y retener defensores, profesionalizar prácticas, y elevar la higiene digital como parte de la cultura organizacional y educativa.

7. Conclusiones

Este trabajo revisó NotPetya como algo más que un "gran malware". En el relato de Perlroth, el ataque sirve para mostrar cómo una cadena de decisiones, muchas de ellas normales en el día a día de una organización, puede terminar en un evento desproporcionado. Lo que vuelve al caso especialmente útil es que mezcla todo: dependencia de proveedores, vulnerabilidades técnicas, falta de segmentación, credenciales expuestas y una cultura de actualización tardía. El resultado fue una propagación que no respetó fronteras ni intenciones iniciales.

A lo largo del informe también quedó claro que el factor humano aparece en varios niveles. Está en la persona que confía en una actualización porque "siempre ha sido así", pero también en el directivo que posterga inversiones defensivas y en el Estado que prioriza capacidad ofensiva sin hacerse cargo del riesgo sistémico. Perlroth insiste en que la seguridad digital no falla solo por errores de programación; falla por incentivos, por burocracias y por decisiones que se toman sin ver el costo civil hasta que ya ocurrió.

La infraestructura crítica, en ese contexto, es el punto más sensible. La interconexión global hace que un incidente pensado para un objetivo específico tenga efectos en sectores que no estaban en la mira: salud, logística, finanzas o energía. Esa dependencia compartida es precisamente lo que vuelve frágil al ecosistema. Cuando el software es común y los procesos están acoplados, una vulnerabilidad retenida o un parche no aplicado se transforma en un problema colectivo.

Por eso, si se resume la tesis práctica del libro en una línea, sería esta: la defensa no puede ser el plan B. Reformar prioridades (qué vulnerabilidades se retienen y cuáles se corrigen), exigir más transparencia sobre el software que sostiene servicios esenciales, y fortalecer la cultura defensiva con talento e incentivos no son ideas "extra"; son condiciones mínimas para que los incidentes no terminen en parálisis social. NotPetya dejó una evidencia difícil de ignorar: en un mundo conectado, las ciberarmas y las malas decisiones tienden a regresar.

8. Bibliografía

Referencias

[1] Columbia University. (s.f.). *Case Study: "NotPetya"*. Informe y análisis sobre herramientas, vectores, impacto y recuperación.

[2] Cybersecurity and Infrastructure Security Agency. (s.f.). *Critical infrastructure sectors*. Department of Homeland Security. Recuperado el 2 de diciembre de 2025, de https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

[3] European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023: Prime threats*. Publications Office of the European Union. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[4] Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday. (Capítulo dedicado a Mimikatz y NotPetya).

[5] Joint Task Force. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

[6] National Institute of Standards and Technology. (s.f.-a). *Zero-day exploit*. Computer Security Resource Center Glossary. Recuperado el 2 de diciembre de 2025, de https://csrc.nist.gov/glossary/term/zero_day_exploit

[7] National Institute of Standards and Technology. (s.f.-b). *Zero-day vulnerability*. Computer Security Resource Center Glossary. Recuperado el 2 de diciembre de 2025, de https://csrc.nist.gov/glossary/term/zero_day_vulnerability

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

[9] Spitzner, L. (s.f.). *Security awareness maturity model*. SANS Institute. Recuperado el 2 de diciembre de 2025, de https://www.sans.org/security-awareness-training/maturity-model/

[10] The MITRE Corporation. (2024). *MITRE ATT&CK®: Design and philosophy*. https://attack.mitre.org/

[11] The White House. (2013, 12 de febrero). *Presidential policy directive – PPD-21: Critical infrastructure security and resilience*. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[12] Wilson, M., & Hash, J. (2003). *Building an information technology security awareness and training program* (NIST Special Publication 800-50). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50

[13] Electronic Privacy Information Center. (2016). *Vulnerabilities Equities Process*. https://archive.epic.org/privacy/cybersecurity/vep/