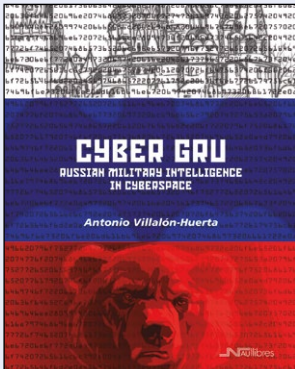


CYBER GRU: RUSSIAN MILITARY INTELLIGENCE IN CYBERSPACE



Autor: Antonio Villalón-Huerta
Editorial: Nau Llibres
Año: 2025 – 390 páginas
ISBN: 978-8-419-75567-4
<https://naullibres.com>

llevar a cabo una amplia gama de operaciones, desde sabotaje y espionaje hasta guerra psicológica. La complejidad de algunas de ellas, sumada a su alta pensión al riesgo y su mentalidad similar a la de los Spetsnaz –los comandos de las fuerzas especiales de élite del país–, la convierte en uno de los actores de ciberamenazas más formidables y sofisticados a los que nos enfrentamos”, destaca Villalón-Huerta.

A lo largo de sus 15 capítulos, tres apéndices y abundante bibliografía, el libro ofrece desde sus principales técnicas de ataque conocidas, hasta una excelente visión de las diferentes unidades de inteligencia rusas (FSB, Fapsi, SVR, FSO y GRU), así como el organigrama del GRU que ha dado pie a muchos de los grupos que mayor notoriedad han alcanzado en el ciberespacio, en los últimos años, por el éxito e impacto de sus ataques persistentes avanzados (APT), así como sus, como era de prever, devaneos por los ámbitos españoles.

El reconocido experto de S2 Grupo, CSO de la compañía, ofrece en este libro de su fecunda bibliografía –en esta ocasión de primeras en inglés, para facilitar su difusión internacional– una lúcida visión del GRU, la agencia de inteligencia militar rusa para el ciberespacio más activa del país. Prologado por el teniente general del Ejército Rafael Comas, el volumen es, sin duda, una lectura obligada para conocer los entramados de una de las unidades más secretas, y que más operaciones de impacto ha realizado, tanto en el ámbito cinético como en el ciberespacio. “El GRU ha desarrollado potentes ciber capacidades a través de diversas unidades militares y un completo espectro de técnicas. Estas le permiten

LA REGULACIÓN DE LAS TECNOLOGÍAS CUÁNTICAS: UNA CUESTIÓN DE SEGURIDAD NACIONAL

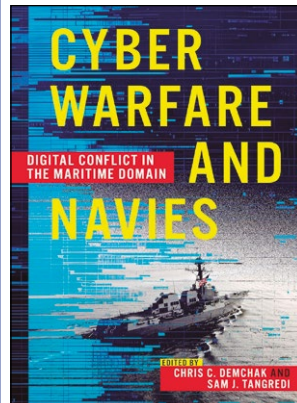


Autor: Francisco Pérez Bes
Editorial: Publicación independiente
Año: 2025 –211 páginas
ISBN: 979-8-287-30649-6
www.amazon.es

afecta a esta materia además de proponer un marco regulatorio adecuado “que dé respuesta a los nuevos retos tecnológicos que plantea esta nueva disrupción”. En definitiva, el lector puede adquirir una primera visión de calado sobre cuál es el panorama legislativo actual e identificar qué carencias requieren comenzar a ser resueltas de cara a regular de manera adecuada esta tecnología aún incipiente, pero cada vez más cercana y cuyo impacto será muy relevante en muchos aspectos de la sociedad, confidencialidad incluida.

El Adjunto de la Agencia Española de Protección de Datos (AEPD) –también fue antaño secretario general y DPO del Incibe–, **Francisco Pérez Bes**, es un abogado de máxima referencia en asuntos tecnológicos, y en este nuevo libro aborda las diferentes regulaciones, en España y la UE, que competen a las tecnologías cuánticas, un tema de especial relevancia “ya que la ONU ha proclamado este año como el Internacional de la Ciencia y las Tecnologías Cuánticas”, recuerda. Frente a ello, este libro permite conocer la legislación actual que

CYBER WARFARE AND NAVIES: DIGITAL CONFLICT IN THE MARITIME DOMAIN



Autores: Chris C. Demchak, Sam J. Tangredi
Editorial: Naval Institute Press
Año: 2025 – 416 páginas
ISBN: 978-1-682-47585-0
<https://www.usni.org/press/books>

marítimos y otras industrias marítimas pueden paralizar las industrias manufactureras y los negocios minoristas a nivel mundial.

Interesantísima obra que analiza en profundidad las amenazas que plantea la ciber guerra a las operaciones en el entorno marítimo y los medios para defenderse de los ciberataques. “Las armadas son blancos obvios de ciberataques hostiles, tanto nacionales como no estatales”, destacan los autores recordando que, en la actualidad, el 85% del comercio mundial y el 70% de todos los combustibles líquidos se transportan por mar. Por ello, consideran que el impacto contra lo cibernético en los buques, los equipos de portuarios, las compañías navieras, los proveedores

Así, esta obra aporta información abundante de las diversas amenazas que la ciber guerra representa para este ámbito, así como la capacidad de las armadas modernas para defenderse de ellas. Además, explica cómo se organizan y equipan las armadas para las ciberoperaciones, además de los conceptos y la doctrina adoptados por ellas, y ofrece recomendaciones para mejorar las ciberactuaciones marítimas. Por supuesto, el libro abarca no solo la Armada, el Cuerpo de Marines y la Guardia Costera de los EE.UU., sino también las armadas de aliados, países adversarios (como China y Rusia).

HACKING & PENTESTING CON INTELIGENCIA ARTIFICIAL



Autores: Pablo González, Fran Ramirez, Rafael Troncoso, Javier del Pino y Chema Alonso
Editorial: OxWord
Año: 2025 – 300 páginas
ISBN: 978-8-409-70056-1
Oxword.com

Pocos expertos técnicos tan reputados suelen coincidir en un mismo libro y ese es uno de los grandes valores de este volumen plural que aglutina a referentes de la ciberseguridad y la IA sobre uno de sus aspectos más críticos: las pruebas de intrusión automatizadas. “Desde la llegada de la IA Generativa (GenAI), con las GANs, los modelos de Difusión, los LLM multimodales y los modelos de *Deep Reasoning* como *Deep Research* o *DeepThink*, el trabajo de un experto en ciberprotección ha cambiado radicalmente”, destacan los autores que recuerdan la importancia de “entender las capacidades de estos modelos que tienen razonamiento visual, con Memory, con aumento de capacidades al usar

MoE (Mixture of Experts) en su diseño, y que desplegados en arquitecturas RAG (Retrieval-Augmented Generation), con destilación de modelos, Agentes de IA (Agentic AI) y la extensión de sus capacidades mediante MCP (Model Context Protocol) han demostrado un poder extraordinario para resolver el día a día en proceso de *pentesting* y *hacking*”.

Así, durante sus 12 capítulos se puede aprender, de forma práctica, a usar la IA para la búsqueda de vulnerabilidades, automatización de ataques con agentes, análisis forenses de imágenes, salto de *captchas*, *webscraping*, ofuscación de código, codificación esteganográfica o criptoanálisis de textos, entre otros aspectos.

VIVIR CONECTADOS: EN FAMILIA



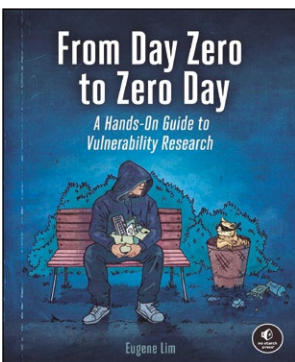
Autora: Jennifer Sesmero,
Jordi Estruch Hill (Ilustrador)
Editorial: Publicación
independiente
Año: 2025 – 42 páginas
ISBN: 979-8-311-15017-0
www.jenniferesesmero.com

a navegar de forma segura. “Desde el papá adicto al móvil, hasta la abuela con su instinto infalible, cada miembro tiene algo que aprender (y enseñar!) sobre ciberseguridad”, explica la autora.

Así pues, es una obra perfecta para disfrutar en familia y, también, para regalar ya que se muestra como un cuento ideal para todos, con abundantes consejos prácticos, situaciones reales y un enfoque ameno que hará reflexionar al lector sobre tus propios hábitos digitales. “Este libro es para vosotros, para todas las familias que desean estar conectadas de forma inteligente y responsable”, destaca Sesmero. “Si usas internet, este cuento es para ti. ¡Haz clic y empieza a protegerte hoy mismo!”, añade con una amplia sonrisa.

Ingeniera en informática y experta en ciberseguridad y desarrollo de talento tecnológico en una de las multinacionales financieras españolas de máxima referencia en ciberprotección, **Jennifer Sesmero** plasma en este libro divulgativo cómo poner en marcha consejos de ciberhigiene básica pensando en los que están más alejados de la ciberprotección en el entorno familiar y educativo. Para ello, usa como gancho a los ‘Pérez’, una familia que podría ser la de cualquiera, pero que tiene el reto de aprender

FROM DAY ZERO TO ZERO DAY:



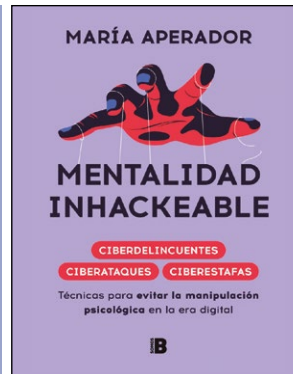
A HANDS-ON GUIDE TO VULNERABILITY RESEARCH

Autor: Eugene Lim
Editorial: No Starch Press
Año: 2025 – 344 páginas
ISBN: 978-1-718-50394-6
<https://nostarch.com>

con CVE (las que se han reportado), así como las principales herramientas y técnicas para dar con ellas en bases de código, protocolos y formatos de archivos, además de mostrar cómo crear un flujo de trabajo repetible para descubrir fallos críticos en el código o rastrear rutas de código con análisis de contaminación y mapear superficies de ataque con precisión. También, ofrece información detallada y abundante para aprender a realizar ingeniería inversa de binarios utilizando Ghidra, Frida y angr, entre otros aspectos. Incluso dedica espacio a cómo desarrollar y validar *exploits*, de prueba de concepto, para demostrar el impacto en el mundo real.

El reconocido investigador de seguridad y hacker de sombrero blanco, **Eugene Lim** (aka ‘Space-raccoon’), ofrece una interesante obra técnica fruto de su experiencia en este ámbito tras haber reportado cientos de vulnerabilidades en software, hardware y servicios en la nube empresariales. De hecho, en 2021, fue uno de los cinco investigadores seleccionados entre un grupo de más de un millón, para el Salón de la Fama Elite de HackerOne.

Así, en este libro, de carácter técnico, el lector podrá adentrarse en el proceso para reconocer e identificar vulnerabilidades, partiendo del conocimiento de las bases de datos



MENTALIDAD INHACKEABLE

Autora: María Aperaturador
Editorial: Ediciones B
Año: 2025 – 200 páginas
ISBN: 978-8-466-68175-9
www.penguinlibros.com

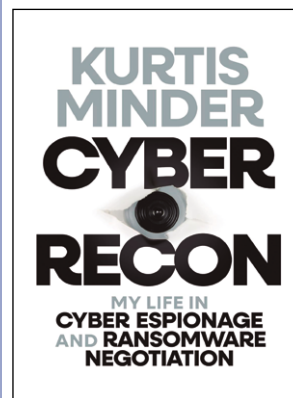
actuar, protegerse y reducir el impacto de las amenazas digitales. Dada su trayectoria en el ámbito de la búsqueda de información en fuentes abiertas (OSINT), dedica amplios apartados a mostrar desde las técnicas más comunes de manipulación hasta los ciberdelitos más sofisticados, así como muchas de las herramientas más eficaces para defenderse.

Con una prosa amena y fácil de leer, se trata, en definitiva, de “un manual esencial para identificar los engaños, cuestionar la desinformación, proteger tu privacidad y, lo más importante, cultivar hábitos digitales saludables que te permitan navegar con confianza”, explica la autora.

“Vivimos en una era en la que la tecnología avanza a pasos agigantados, pero también, lo hacen las amenazas invisibles que acechan en la red”, explica la reconocida criminóloga **María Aperaturador**, CEO de la App de concienciación VeWalk. Como parte de su incansable labor en pro de una cultura de ciberseguridad, ahora ha publicado este libro para un público no técnico buscando que cada persona sea “inhackeable”.

En sus capítulos se puede aprender a detectar los riesgos más comunes que nos rodean en el ciberespacio, así como

CYBER RECON: MY LIFE IN CYBER



ESPIONAGE AND RANSOMWARE NEGOTIATION

Autor: Kurtis Minder
Editorial: Wiley
Año: 2025 – 272 páginas
ISBN: 978-1-394-33461-2
www.wiley.com

de los incidentes en línea más dramáticos de las últimas décadas.

Así, Cyber Recon se ofrece a modo de ‘guía de campo’ para cualquier persona interesada en el espionaje, la tecnología, la piratería o el emprendimiento digital, incluyendo la referencia a interesantes entrevistas de profesionales del ciberespionaje y la negociación, como Jax Scott, Jon DiMaggio, Jason Ingalls, Beau Woods y Brye Ravattin, además de ofrecer amplia información de “cómo se relaciona la intersección de la negociación comercial y la negociación de rehenes con las negociaciones de *ransomware* de alto riesgo”, destaca su autor y de “cómo se está usando la rápida evolución de la IA generativa para ciberataques y su defensa”.

Con más de 30 años de experiencia, **Kurtis Minder** ofrece una fascinante exploración del ciberespionaje en algunos de los entornos más peligrosos de internet. Explica cómo se lleva a cabo, las herramientas y habilidades que personas como él usan constantemente, y las consecuencias de interactuar con ciberdelincuentes a diario.

El lector podrá adentrarse en este mundo ‘en la sombra’, donde las organizaciones privadas espían a los delincuentes y cómo negocian con los cibercriminales para intentar recuperar los datos robados. También, descubrirá lecciones cruciales que Minder ha aprendido al liderar su empresa de riesgo digital, GroupSense, en muchos