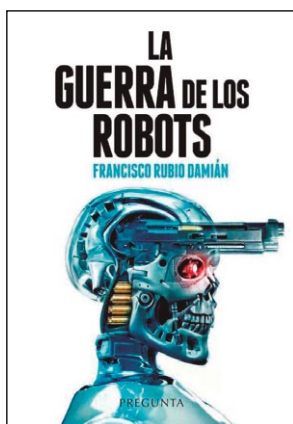


LA GUERRA DE LOS ROBOTS



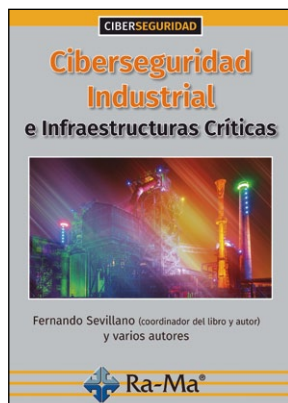
Autor: Francisco Rubio Damián
Editorial: Pregunta Ediciones
Año: 2021 – 242 páginas
ISBN: 9788417532611
<https://preguntaediciones.com>

ha movilizado a científicos y académicos, aunque aún no es muy debatido entre la población. “Sin embargo, no estamos frente a un debate científico, sino ante una realidad que nos afecta (y afectará) a todos”, destaca el autor en este libro prologado por el veterano periodista de Rtvé, **David Corral**.

En él ofrece una excelente visión del escenario inédito al que nos enfrentamos y en el que “las tecnologías son empleadas en contra de lo que se supone su esencia, aportar beneficio a la humanidad”. Un entorno en el que, lógicamente, la ciberseguridad se convierte en un aspecto clave para proteger de ciberataques los sistemas de armas robóticos. En definitiva, se trata de una obra en la que se plantean un buen número de preguntas, otras tantas respuestas y que resulta imprescindible para tener una opinión formada sobre un mundo nuevo que puede cambiarlo todo.

Con una prosa sencilla pero rica en información y referencias, el coronel, en la reserva, del Ejército de Tierra, **Francisco Rubio**, analiza cómo la robótica cambiará la sociedad del siglo XXI y también sus guerras, “que no desaparecerán: serán diferentes” por cuanto “las armas autónomas son capaces de matar y destruir sin necesidad de control humano”. Su punto de partida es la disrupción que provoca contar con sistemas ‘inteligentes’ capaces de “decidir sobre la vida de una persona”. Un aspecto que

CIBERSEGURIDAD INDUSTRIAL E INFRAESTRUCTURAS CRÍTICAS

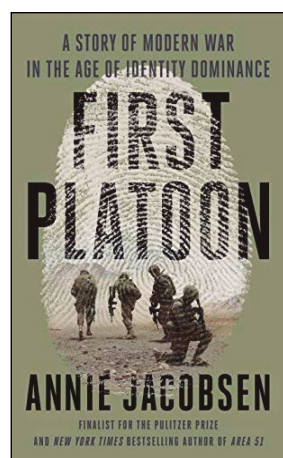


Autor: Coordina: Fernando Sevillano (Marta Beltrán, Antonio Rodríguez, Agustín Valencia, Edorta Echave, Susana Sánchez Mella, Elena Matilla, Erik de Pablo)
Editorial: Editorial Ra-Ma
Año: 2021 – 346 páginas
ISBN: 978-84-18551-36-9
www.ra-ma.es

principales amenazas y grupos APT, que pueden provocar un incidente de ciberseguridad. También, ofrece una exhaustiva referencia a marcos y estándares disponibles para gobernar y gestionar el ciberriesgo específico, así como las principales vulnerabilidades en un entorno crítico y las medidas que posibilitan la detección temprana y la correlación de eventos en estos entornos. Por último, se proponen numerosas prácticas para “diseñar una estrategia de continuidad de negocio que incluya planes de respuesta y recuperación ante incidentes en infraestructuras críticas”. En definitiva, una obra más que recomendable para tener una aproximación a la ciberseguridad industrial.

Nueva obra de la colección de ciberseguridad de la **Editorial Ra-Ma** en la que destacados especialistas en la materia ofrecen una completa síntesis de los aspectos que hay que contemplar para proteger estos entornos. Estructurada en diez capítulos, de fácil comprensión, y variada profundidad el lector encontrará, de forma práctica y didáctica, amplia información sobre los activos más comunes de los entornos industriales o de las infraestructuras críticas, así como sus

FIRST PLATOON: A STORY OF MODERN WAR IN THE AGE OF IDENTITY DOMINANCE



Autora: Annie Jacobsen
Editorial: Dutton
Año: 2021 – 400 páginas
ISBN: 978-1524746667
www.amazon.es

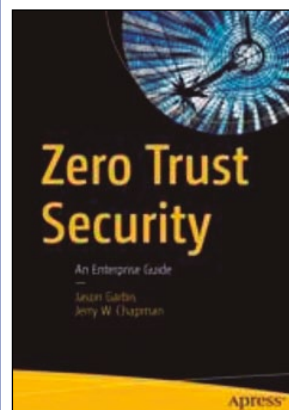
tres cuestiones de gran importancia en la actualidad: el desarrollo de la inteligencia de identidad, la recopilación y el uso de esos datos en las guerras modernas y su expansión a la sociedad civil; y la trágica historia de este Primer Pelotón.

La historia narrada de forma sagaz por **Annie Jacobsen** es, según algunos de sus críticos, “una advertencia para el resto de nosotros: una parábola del poder devastador que dicha inteligencia otorga al gobierno y a los legisladores”. “Se pone sobre la mesa cómo esta tecnología promete ser una defensa de los malhechores y, a la vez, cómo descubre el Primer Pelotón que la inteligencia de identidad es defectuosa porque hay personas que pueden manipular los datos y lo hacen”, puntualizan.

Aunque el argumento principal de este libro pueda parecer poco original: la experiencia de un pelotón de jóvenes, en su mayoría de diecinueve años, enviados a Afganistán, la trama esconde un gran debate sobre la identidad en la era de la identificación biométrica, que reduce a las personas a escaneos de iris, huellas dactilares, patrones de voz, detección a través del olor, etc.

Con ello, en la obra se entretrejen

ZERO TRUST SECURITY



Autores: Jason Garbis y Jerry W. Chapman
Editorial: Springer
Año: 2021 – 300 páginas
ISBN: 978-1-4842-6702-8
www.springer.com

ge los principios de seguridad que rigen este modelo y por qué resulta fundamental adoptarlos. Además, explica en detalle sus beneficios operativos y cómo pueden integrarse en una organización.

Proporciona, asimismo, orientación y requisitos realistas para apostar por este enfoque por parte de los equipos de seguridad, ayudándoles a planificar su implantación y defenderla ante la alta dirección. “Después de leer este libro, estará listo para diseñar una arquitectura de seguridad *Zero Trust* creíble y demostrable para su organización”, destacan sus autores que dan consejos para implementar este concepto. Por ello, la obra va destinada a CISOs, arquitectos de seguridad corporativa, de soluciones y de redes, así como a ingenieros de seguridad, entre otros.

El modelo de Confianza Cero se ha convertido en una tendencia que está teniendo gran aceptación entre las empresas para hacer frente a las nuevas ciberamenazas, aunque adoptarlo puede ser todo un desafío.

Con esta obra, sus autores quieren aportar luz sobre el cambio de filosofía que supone, ya que, fundamentalmente, deja atrás la protección tradicional para evolucionar hacia un enfoque dinámico, centrado en la identidad y basado en políticas. Para ello, el libro reco-