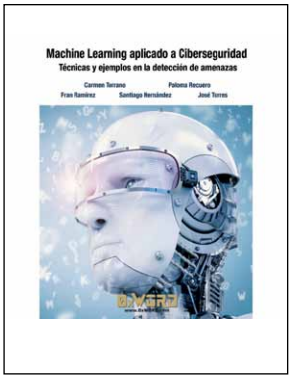


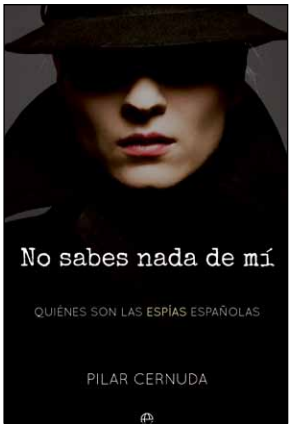
MACHINE LEARNING APLICADO A CIBERSEGURIDAD (TÉCNICAS Y EJEMPLOS EN LA DETECCIÓN DE AMENAZAS)

Autores: Carmen Torrano, Fran Ramírez, Santiago Hernández, Paloma Recuero, José Torres
Editorial: 0xWord Año: 2019 – 248 páginas
ISBN: 978-8409069187 www.oxword.com

Dedicado a un público experto o que quiera saber más de este tema, esta guía ofrece una excelente perspectiva de lo que es el aprendizaje automatizado (*machine learning*), de por qué está revolucionando el mundo de la empresa y de sus aplicaciones a sistemas predictivos, de soporte de decisión y recomendación, vehículos de conducción autónoma, agentes inteligentes de conversación, asistentes personales, visión artificial, detección de anomalías, procesamiento inteligente de textos, etc.

Este tipo de técnicas, que consisten en automatizar, mediante algoritmos, la búsqueda de patrones y tendencias en grandes cantidades de datos permiten entrenar a sistemas de inteligencia artificial para detectar, por ejemplo, diferentes ciberamenazas que afectan a particulares y, por supuesto, empresas. Por eso, en este libro, de fácil lectura y con un nivel técnico medio, se puede conocer cómo funcionan diferentes sistemas de *machine learning* para detectar y evitar fugas de información, robo y publicación de credenciales de clientes, uso no autorizado de marcas, noticias falsas, etc.

Con abundante información técnica y práctica, el libro comienza presentando qué es esta tecnología, cómo funciona y en base a qué datos y algoritmos y tendrá una visión clara de cómo dar los primeros pasos para modelar este tipo de sistemas conforme a unos datos procesados y que estos cuenten "su historia". De hecho, uno de los grandes atractivos de esta obra respecto a otras de este campo es que permite "desarrollar varios casos prácticos, con el paso a paso del proceso de analítica de datos, según el modelo denominado CRISP, para terminar construyendo un modelo predictivo de calidad", destacan sus autores. Un sistema que se muestra cómo aplicar para la "detección de tráfico de red no deseado, rechazar *spam*, identificar ficheros RTF maliciosos o detectar un *ransomware* mediante una técnica de detección de anomalías. En definitiva, un buen libro para iniciarse, de forma sencilla, en lo que es el *machine learning* y todas las aplicaciones que está teniendo.



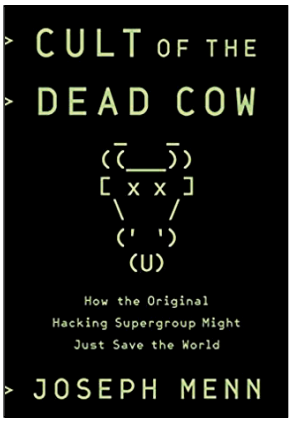
NO SABES NADA DE MÍ: QUIÉNES SON LAS ESPÍAS ESPAÑOLAS

Autora: Pilar Cernuda
Editorial: La Esfera de los libros Año: 2019 – 256 páginas
ISBN: 978-8491645603 www.esferalibros.com

Trabajar para una Agencia como el Centro Nacional de Inteligencia conlleva pasar al anonimato en la mayor parte de las ocasiones, sobre todo si en vez de analista eres agente de campo. Para poner en valor el ingente e incansable trabajo de las mujeres que han ingresado en el CNI, la periodista Pilar Cernuda, ha escrito una obra que recoge los testimonios en primera personas de algunas de las grandes protagonistas de las últimas décadas del Centro tras entrevistar a más de 30 integrantes. Y, en definitiva un complejo mosaico del complicado y arriesgado trabajo que muchas de ellas han realizado, en la sombra, en la lucha incansable que lleva el CNI contra las amenazas que afectan a nuestra Seguridad Nacional.

Un relato en primera persona de "mujeres con un sexto sentido que han conocido, desde dentro, la lucha contra el terrorismo de ETA y el yihadismo y que han participado en operaciones de riesgo y de contraespionaje, entrenadas para preservar el anonimato en un mundo de hombres", destaca su autora. En esta obra con "testimonios de primera mano" intenta romper tópicos y desvelar algunos secretos de su trabajo nunca destacado.

No falta un capítulo dedicado al trabajo de las mujeres relacionados con los "Cambios tecnológicos y la ciberseguridad". En él, se muestran los retos de algunas expertas del CNI para conseguir información a través las radiocomunicaciones por satélite así como el desarrollo de diferentes herramientas de software para los analistas. Cernuda también presenta a 'Elena' y 'Susana' que trabajan para el Centro Criptológico Nacional (CCN), el organismo de ciberseguridad del CNI, y encargadas de realizar auditorías de seguridad en organismos de la Administración y velar por la aplicación de la normativa "en el ámbito de los sistemas clasificados". Quizá por ser una *rara avis* o por desmitificar muchas creencias la nueva obra de Cernuda no dejará a nadie indiferente. Por último, cabe igualmente reseñar que una de las principales protagonistas del libro, Beatriz Méndez de Vigo, fue entrevistada por SIC, en calidad de Secretaria General de la 'casa', en la edición de junio de 2015.



CULT OF THE DEAD COW: HOW THE ORIGINAL HACKING SUPERGROUP MIGHT JUST SAVE THE WORLD

Autor: Joseph Menn
Editorial: Public Affairs Año: 2019 – 272 páginas
ISBN: 978-1541762381 www.publicaffairsbooks.com

Apasionante relato sobe el grupo de *hacking* más antiguo de EE.UU., el '***Cult of the Dead Cow***'. Una verdadera leyenda en el mundo de la ciberseguridad por haber inspirado el concepto de 'hacktivismo' en los años 80 y por el anonimato de sus integrantes a pesar de los años. Entre sus hitos figuran desde el desarrollo de herramientas para contar con claves seguras hasta para controlar dispositivos en remoto –RAT– y muchas acciones que pusieron en valor, a costa de su espíritu justiciero, la ciberseguridad. Una historia de la que hay muchos claros y oscuros pero en la que todos los expertos dan un papel importante a este grupo que también colaboró con el desarrollo de la red TOR y se dice que con los servicios de seguridad de los EE.UU. en ciertas iniciativas.

Curiosamente, algunos de sus primeros integrantes se han dado a conocer en la última década, ya que ocupan cargos de responsabilidad tanto en Washington como en Silicon Valley. ¿El último? El ex congresista de Texas y actual candidato a la presidencia del país, **Beto O'Rourke.**

Actualmente, el grupo hacktivista tiene una actividad ligada a la lucha contra la desinformación electoral. '*Cult of the Dead Cow*' muestra cómo los gobiernos, las corporaciones y los criminales llegaron a tener un poder inmenso sobre los individuos y cómo podemos luchar contra ellos", explica su autor, el periodista de la agencia Reuters, **Joseph Menn.** En definitiva, esta obra es una interesante "historia de cómo los primeros hackers de Internet aprendieron a manejar sus enormes capacidades y que puede ayudarnos a controlar el poder de los titanes de la tecnología de hoy", resaltó el conocido experto **Bruce Schneier**.