CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD

Autor: Bruce Schneier
Editorial: W. W. Norton &Company Año: 2018 – 288 páginas
ISBN: 9780393608885 http://books.wwnorton.com

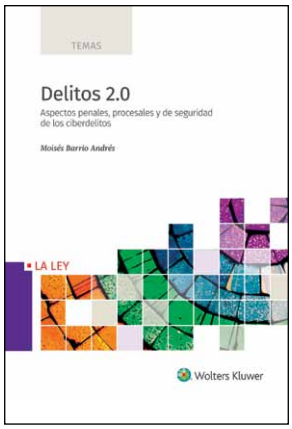
Bruce Schneier, el reconocido autor de *best-sellers* como 'Data and Goliath', desgrana bajo una nueva perspectiva la amenaza que plantea la exponencial conexión de prácticamente cualquier dispositivo a las redes y sistemas de empresas y gobiernos a través de internet.

Sin duda, todo este 'enjambre', conocido como Internet de las Cosas (IoT), tiene un efecto directo en el mundo físico: desde coches autónomos, *smartcities*, sistemas autónomos de negociación y drones equipados con sus propios algoritmos de comportamiento, hasta cafeteras o termostatos inteligentes. Y, si bien este futuro tan digitalizado conlleva un enorme potencial, a medida que estos objetos proliferan los riesgos cibernéticos también se multiplican.

En '**Click Here to Hill Everybody**', Schneier comienza sumergiendo al lector en una reflexión profunda sobre diversas cuestiones, como la efectividad del 'parcheo' como método ortodoxo para proteger las vulnerabilidades de los dispositivos IoT, poniendo en cuestión su función como "paradigma" de la seguridad. Junto a ello, analiza la creciente dificultad de conocer 'quién es quién' en el ciberespcio y proporciona un conjunto de soluciones dirigidas a empresas, gobiernos e individuos para disfrutar del IoT sin ser víctimas de sus ciberriesgos.

En un segundo bloque, Schneier identifica los principios básicos necesarios para crear una Internet de las Cosas de confianza y resiliente; elabora una receta para crear una regulación y supervisión sanas por parte del gobierno; y, explica de qué forma la administración pública puede priorizar los sistemas defensivos por encima de los ofensivos.

Para concluir, el autor pasa a resumir una posible solución al problema, unir tecnología y política, que no dejará indiferente al lector.



DELITOS 2.0. ASPECTOS PENALES, PROCESALES Y DE SEGURIDAD DE LOS CIBERDELITOS

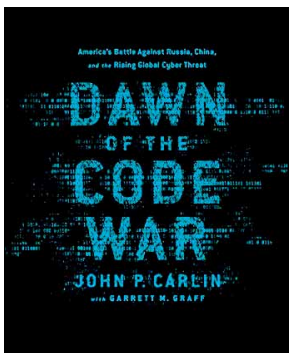
Autor: Moisés Barrio
Editorial: La Ley Año: 2018 – 310 páginas
ISBN: 9788490207437 https://tienda.wolterskluwer.es

Moisés Barrio, letrado del Consejo de Estado, es uno de los abogados españoles más prolíficos en obras sobre derecho y nuevas tecnologías. En este estudio analiza el problema que suponen los ciberdelitos para los planteamientos clásicos del Derecho. Para facilitar su entendimiento y repercusión, el autor detalla, de forma práctica y precisa, las características de la nueva delincuencia que se aprovecha del ciberespacio y su tipificación penal –prestando atención a la jurisprudencia más reciente–.

A lo largo de 16 capítulos, se analiza desde los delitos de descubrimiento y revelación de secretos hasta el intrusismo e interceptación de las comunicaciones (*hacking*), la protección de la intimidad, la revelación de secretos, la protección de datos y el derecho a la propia imagen, entre otros muchos.

También examina y compara la normativa española con la europea y extracomunitaria, así como las nuevas técnicas de investigación tecnológica que permite, desde 2015, la Ley de Enjuiciamiento Criminal –algunas de las cuales aún no son tan eficaces como se esperaba–. Y dedica un capítulo íntegro, el XV, a la ciberseguridad y las leyes que la circunscriben.

En definitiva, se trata de una obra de referencia para tener claros los conceptos jurídicos del 'ciberderecho', así como los retos que plantea cuando se usa lo último en tecnología en su modo más perverso.



DAWN OF THE CODE WAR: AMERICA'S BATTLE AGAINST RUSSIA, CHINA, AND THE RISING GLOBAL CYBER THREAT

Autores: John P. Carlines y Garrett M. Graff
Editorial: Public Affairs Año: 2018 – 480 páginas (incluye un audio libro)
ISBN: 9781541773837 www.publicaffairsbooks.com

El que fuera fiscal general adjunto con la Administración **Obama, John P. Carlin**, y **Garrett Graff**, periodista experto en Seguridad Nacional –colaborador habitual de Wired–, presentan una visión amplia –pero meticulosa y fascinante– de la evolución, los impactos y las implicaciones de la ciberguerra que vive el mundo desde la perspectiva estadounidense. "Con cada año que pasa, los ataques de Internet contra nuestros intereses han crecido en frecuencia y en gravedad. Países como Corea del Norte, China, Irán y Rusia nos han encontrado vulnerables en el ciberespacio", destaca Carlin en la obra. Por eso, recuerda que el '*CodeWar*' está sobre nosotros".

Así en este libro se muestra con rigor cómo funcionan las organizaciones de ciberterroristas, cibercriminales y los estados enemigos que pelean con EE.UU. por el ciberespacio. También hay varios apartados en los que se analiza la importancia de los datos personales y la lucha por los secretos industriales que den hegemonía en la economía de la próxima década. "El Departamento de Justicia y el FBI persiguen a piratas informáticos, reclutadores de terroristas en línea y espías", recuerdan los autores, que alertan de que la economía ya es digital y es uno de los pilares más atacados de la sociedad. "El ciberespacio es otro ejemplo más del doble filo de la tecnología: supone un gran beneficio para la humanidad por un lado, pero representa un gran riesgo por el otro", destaca en el libro **James Clapper,** ex Director Nacional de Inteligencia en el *New York Times,* que ha recordado que Carlin ha estado "en primera línea defendiéndonos contra ataques de China, Corea del Norte, Rusia, Siria y bandas criminales".