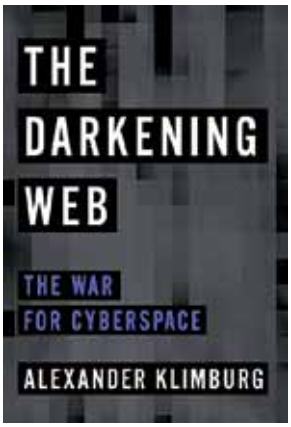


THE DARKENING WEB: THE WAR FOR CYBERSPACE

Autor: Alexander Klimburg
Editorial: Penguin Publishing Group Año: 2017 – 432 páginas
ISBN: 9781594206665 http://www.penguin.com

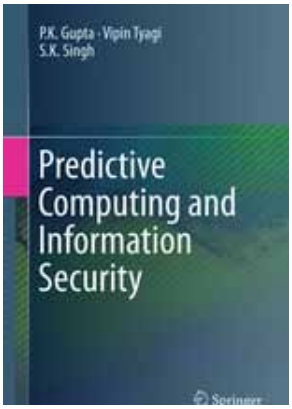
La guerra por el ciberespacio, como reza su subtítulo, es el principal *leitmotiv* de este nuevo libro escrito por **Alexander Klimburg,** quien alerta de los peligros de minusvalorar el dominio cibernético y advierte de la pasividad de la inmensa mayoría de la comunidad internacional.

El ciberespacio, según sostiene Klimburg y muchos otros escritores, analistas y doctos en la materia, ya es el escenario principal de la confrontación mundial de este siglo, donde el debate sobre cómo las naciones, de forma individual, y la comunidad global definirán este nuevo dominio de interacción es más apremiante y divisivo que nunca.

En este contexto, Klimburg alerta de la subestimación de las consecuencias a largo plazo de las aspiraciones de los estados por proyectar su poder en el ciberespacio. Este experto internacional en ciberseguridad ahonda en **The Darkening Web** en las cibercapacidades que están construyendo y utilizando las principales potencias mundiales con objeto de ejercer una superioridad no solo tecnológica sino, también, de cara a controlar la informacion para conseguir más poder e influencia.

Con una buena mezcla de anécdotas y argumentos, y un enfoque específico en los Estados Unidos por un lado, y Rusia y China, por el otro, el libro deja entrever que el debate sobre las diferentes aspiraciones en el ciberespacio es básicamente una guerra sobre nuestros valores globales.

Asimismo, el autor enfrenta al lector cara a cara con el amplio abanico de amenazas que abre la lucha por el espacio cibernético, revela las posibilidades de un siglo XXI dominado por la guerra de la información y explica cómo la promesa original para la que se concibió internet como medio para promover las libertades, aún puede recuperarse.



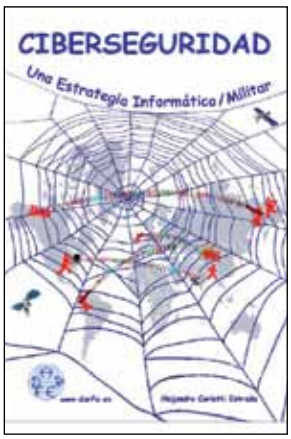
PREDICTIVE COMPUTING AND INFORMATION SECURITY

Autores: PK Gupta, Vipin Tyagi y Sanjay Kumar Singh
Editorial: Springer Año: 2017 – 155 páginas
ISBN: 9789811051074 http://www.springer.com

Este libro describe algunos de los métodos y avances más recientes en el ámbito de la informática predictiva y la seguridad de la información, a través de las últimas investigaciones, algoritmos y marcos de trabajo basados, especialmente, en Internet de las Cosas (IoT) y en la computación en la nube.

Sus autores, profesores y expertos en ingeniería y tecnologías de la información, han elaborado este ejemplar destacando las implementaciones del mundo real de este tipo de técnicas, además de abordar otros procedimientos de vanguardia, así como el diseño, desarrollo y uso innovador de ciertas tecnologías para mejorar la computación predictiva y la seguridad de la información.

Como tal, el libro se presenta como un valioso recurso para investigadores o todo aquel interesado en explorar las técnicas y arquitecturas de modelado predictivo para resolver problemas de seguridad de la información, privacidad y protección en las comunicaciones futuras, a tenor de los avances en el mundo de la computación, que están generando un cambio significativo en el paradigma de la programación. Y es que, la integración de Internet de las cosas, la computación en la nube y las redes inalámbricas de sensores ha hecho posible la predicción en tiempo real en diferentes áreas de aplicación, que van desde el sector de la salud, al transporte, el hogar inteligente, el coche conectado y un largo etcétera pero que, de forma inherente, también está generando verdaderos desafíos en el terreno de la seguridad de la información, especialmente para mantener la confianza, privacidad y confidencialidad de los datos durante la comunicación, el almacenamiento y el acceso a los mismos.



CIBERSEGURIDAD: UNA ESTRATEGIA INFORMÁTICO/MILITAR

Autor: Alejandro Corletti Estrada
Editorial: DarFe Learning Consulting Año: 2017 – 245 páginas
ISBN: 9788469772058 http://www.darfe.es

Tras los ejemplares 'Seguridad por Niveles' y 'Seguridad en Redes', **Alejandro Corletti** vuelve a dar forma a una obra centrada en la ciberseguridad en la que, en esta ocasión, propone un novedoso enfoque relacionando ciertos temas militares y su forma de implementarlos a través de los diferentes protocolos de telecomunicaciones para lograr una adecuada estrategia de "ciberdefensa". Y es que, para el autor, a diferencia de los cuatro dominios tradicionales –tierra, mar, aire y espacio-, donde la capacidad bélica de las partes era un claro factor de éxito, en el nuevo dominio del ciberespacio, la misma no guarda absolutamente ninguna relación. "Hoy, la más grande potencia bélica mundial puede ser desbordada por una nación que no tenga ni ejército", manifiesta.

Abanderada por esta premisa, la obra, con un volumen de 245 páginas y prologada por **Julio Ardita**, se estructura en 12 capítulos que recorren la problemática actual a la que todos los estados se enfrentan en el ciberespacio, a través de la descripción clara de conceptos, metodologías, herramientas e ideas que ayudarán a estar más preparados para prevenir y contener las nuevas amenazas. En este sentido, ya en la presentación de este libro, Corletti intenta llamar a "la unión de esfuerzos sobre ciberseguridad", defendiendo que si no se es capaz de seguir una línea de acción de este tipo, lo que haga cada país de forma aislada no producirá el más mínimo impacto sobre su propia ciberdefensa, "solo se logrará apagar algún que otro fuego menor".

Como ya se hiciera con las anteriores, esta obra se publica bajo licencia *copyleft* para su descarga gratuita en formato electrónico y libre uso en actividades docentes sin fines de lucro. En su versión impresa, la obra tiene un coste y es posible adquirirla solicitándola a la dirección info@darFe.es o directamente desde la página web de DarFE.