Sistemas de comunicación seguros para operaciones militares modernas

Este libro ofrece un examen exhaustivo de los sistemas de comunicaciones seguras para las operaciones militares modernas, abordando los retos tecnológicos y operativos del intercambio de información en los campos de batalla contemporáneos y futuros. Traza la evolución de las comunicaciones militares desde los sistemas analógicos y digitales hasta las arquitecturas cifradas, definidas por software y mejoradas con IA, haciendo hincapié en la interoperabilidad de la OTAN, las amenazas a la ciberseguridad y la guerra electrónica. Se analizan principios básicos como la transmisión de señales, el cifrado, la autenticación, las técnicas anti-interferencia y las redes de radio tácticas resistentes. Entre los temas avanzados se incluyen las comunicaciones seguras entre vehículos aéreos no tripulados y centros de mando, el enrutamiento y la gestión del espectro basados en IA, los sistemas por satélite, las aplicaciones militares 5G/6G, la comunicación cuántica y las redes de radio cognitivas. El libro también propone un marco de comunicaciones seguras orientado al futuro e integrado con sistemas C4ISR, apoyado por estudios de casos prácticos, incluida la investigación doctoral del autor. Está dirigido a investigadores, profesionales militares, ingenieros y responsables políticos que busquen soluciones de comunicaciones de defensa resistentes e inteligentes.

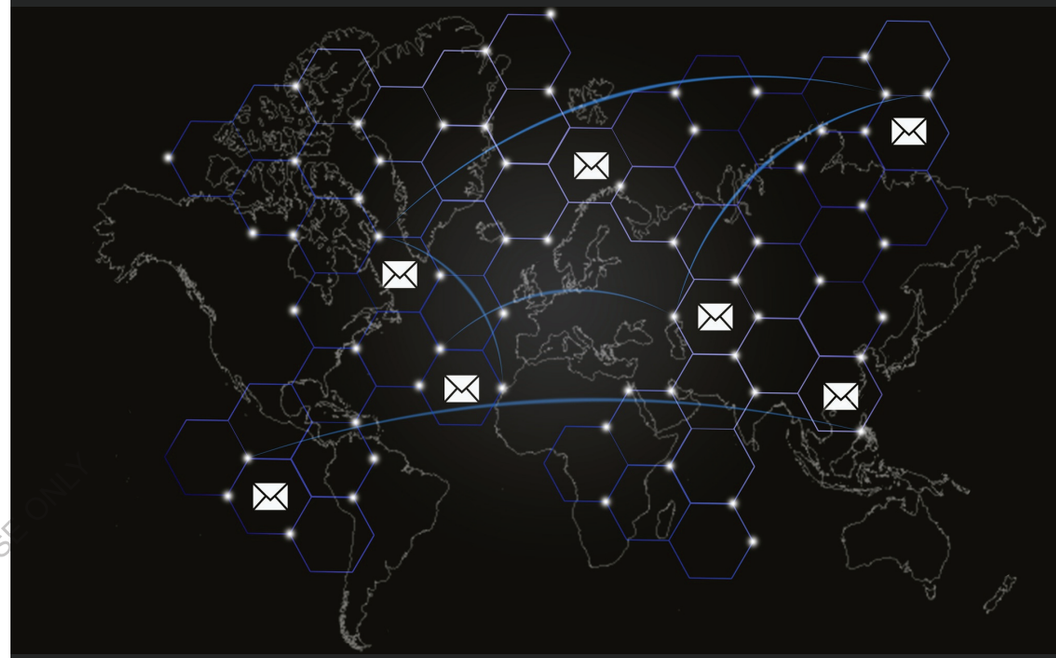
Rexhep Mustafovski, MSc, es oficial de señales e investigador en comunicaciones militares. Es licenciado por la Academia Militar "General Mihailo Apostolski" de Skopje y máster en Tecnologías de la Comunicación y la Información por la Universidad "Ss. Cirilo y Metodio".

9 786209 567889

EDICIONES NUESTRO CONOCIMIENTO

Rexhep Mustafovski

EDICIONES NUESTRO CONOCIMIENTO



Sistemas de comunicación seguros para operaciones militares modernas

Fundamentos, tecnologías y perspectivas de futuro

Rexhep Mustafovski

Rexhep Mustafovski

Sistemas de comunicación seguros para operaciones militares modernas

Rexhep Mustafovski

Sistemas de comunicación seguros para operaciones militares modernas

Fundamentos, tecnologías y perspectivas de futuro

ScienciaScripts

Imprint

Cover image: www.ingimage.com

This book is a translation from the original published under ISBN 978-620-9-27053-6.

Publisher:
Sciencia Scripts
is a trademark of
Dodo Books Indian Ocean Ltd. and OmniScriptum S.R.L publishing group

120 High Road, East Finchley, London, N2 9ED, United Kingdom
Str. Armeneasca 28/1, office 1, Chisinau MD-2012, Republic of Moldova, Europe
Managing Directors: Ieva Konstantinova, Victoria Ursu
info@omniscriptum.com

Printed at: see last page
ISBN: 978-620-9-56788-9

Sistemas de comunicación seguros para operaciones militares modernas: fundamentos, tecnologías y orientaciones futuras

Índice

Prefacio

Soy Rexhep Mustafovski, máster en Ciencias, y este libro es el resultado de mi compromiso académico, profesional y de investigación en el campo de los sistemas de comunicación modernos, con especial atención a las aplicaciones seguras orientadas a la defensa y el ámbito militar. La motivación para escribir este libro surge de la creciente importancia de las tecnologías avanzadas en la configuración de la sociedad contemporánea y, más concretamente, en la transformación de la forma en que las fuerzas militares se comunican, coordinan y operan en entornos complejos y conflictivos.

En el mundo moderno, la tecnología ya no es un elemento periférico de la actividad humana, sino un motor central del cambio en los ámbitos económico, social y de seguridad. Las tecnologías de la comunicación, en particular, se han convertido en fundamentales para la forma en que se genera, transmite, protege y explota la información. En el contexto militar, la comunicación segura no es solo un requisito técnico, sino una necesidad estratégica. La capacidad de intercambiar información de forma segura, fiable y en tiempo real influye directamente en la eficacia operativa, la toma de decisiones y la protección de las fuerzas. Este libro se ha escrito con la intención de presentar estas realidades a un público académico y profesional más amplio, tendiendo un puente entre los fundamentos teóricos y las aplicaciones militares prácticas.

Mi formación académica en tecnologías de la comunicación y la información, combinada con mi compromiso profesional en la educación y la investigación militares, ha dado forma a la perspectiva adoptada en este trabajo. A lo largo de mis estudios y actividades de investigación, observé una brecha recurrente entre las tecnologías de comunicación en rápido avance y su integración estructurada a nivel de sistema dentro de los marcos militares. Si bien muchos trabajos se centran en tecnologías aisladas o soluciones técnicas específicas, son pocos los que intentan presentar una visión integral e integrada de los sistemas de comunicación militar segura como arquitecturas en evolución. Este libro busca abordar esa brecha ofreciendo un examen coherente y estructurado de las tecnologías, los mecanismos de seguridad y los principios arquitectónicos que sustentan las comunicaciones militares modernas y futuras.

El libro también se basa en mi investigación doctoral en curso, que se centra en los marcos de comunicación segura y las plataformas de comunicación avanzadas para aplicaciones de defensa. Una parte de esta investigación se incorpora al libro en forma de un estudio de caso específico, que presenta un ejemplo práctico de cómo los conceptos teóricos y los principios arquitectónicos pueden aplicarse a un sistema real. Este estudio de caso, derivado de mi trabajo de doctorado, se incluye

para demostrar la transición del análisis conceptual al diseño y la implementación del sistema. Su propósito no es proporcionar una solución definitiva, sino ilustrar cómo se pueden estructurar las plataformas de comunicación segura para abordar los requisitos operativos , tales como la seguridad, la fiabilidad, la latencia y la interoperabilidad.

Al escribir este libro, mi objetivo era mantener un equilibrio entre el rigor académico y la relevancia práctica. El contenido se basa en principios establecidos de ingeniería de comunicaciones, ciberseguridad y sistemas militares, al tiempo que refleja las tendencias tecnológicas actuales, como la inteligencia artificial, las radios definidas por software, los sistemas no tripulados, las comunicaciones por satélite y los mecanismos de seguridad emergentes. La intención no era producir un texto puramente teórico, ni un manual estrictamente técnico, sino un trabajo académico estructurado que pudiera servir de referencia para estudiantes, investigadores, ingenieros y profesionales militares interesados en el diseño y la evolución de los sistemas de comunicación seguros.

Por lo tanto, el público destinatario de este libro es intencionadamente amplio, ya que abarca a estudiantes de grado y posgrado en ingeniería y disciplinas relacionadas con la defensa, investigadores que trabajan en los ámbitos de la comunicación y la seguridad, y profesionales que participan en la planificación de las comunicaciones militares, el desarrollo de sistemas y el despliegue operativo. Al mismo tiempo, el libro está escrito con suficiente profundidad y enfoque analítico para apoyar los estudios académicos avanzados y contribuir a los debates en curso dentro de la comunidad investigadora.

Por último, este libro representa un paso en un largo recorrido académico y profesional. Refleja tanto la investigación completada como la investigación en curso, reconociendo que el campo de las comunicaciones militares es dinámico y está en continua evolución. Las tecnologías, arquitecturas y marcos que se analizan en esta obra sin duda seguirán desarrollándose en respuesta a los nuevos requisitos operativos y las amenazas emergentes. Espero que este libro contribuya a una comprensión más profunda de los sistemas de comunicación seguros y fomente la investigación, el debate y la innovación en este ámbito tan importante.

Introducción

Los sistemas de comunicación militar siempre han desempeñado un papel decisivo en la conducción de la guerra, determinando la forma en que las fuerzas se coordinan, deciden y actúan en los entornos operativos. Desde las primeras formas de señalización en el campo de batalla hasta las arquitecturas actuales, conectadas a nivel mundial y basadas en datos, las comunicaciones han seguido siendo un elemento central para el mando, el control y la eficacia operativa. Sin embargo, en las operaciones militares contemporáneas, los sistemas de comunicaciones han evolucionado más allá de su tradicional función de apoyo y ahora constituyen una capacidad estratégica por derecho propio. Las infraestructuras de comunicaciones seguras, resilientes y adaptables son fundamentales para lograr la superioridad informativa, mantener el ritmo operativo y garantizar la supervivencia de las fuerzas en entornos cada vez más complejos y disputados.

La transformación de la guerra en el siglo XXI ha introducido nuevos retos que alteran fundamentalmente los requisitos que se exigen a los sistemas de comunicación militar. Las operaciones modernas se caracterizan por una alta movilidad, un compromiso multidominio y la integración de actividades de guerra convencional, cibernética e informática. Las fuerzas operan en los dominios terrestre, aéreo, marítimo, espacial y cibernético, a menudo de forma simultánea y en coordinación con socios conjuntos y de coalición. En tales condiciones, la capacidad de intercambiar información precisa, oportuna y protegida determina no solo el éxito táctico, sino también los resultados estratégicos. Por lo tanto, los sistemas de comunicación deben funcionar de manera fiable en condiciones de incertidumbre, interrupción e interferencia activa del adversario.

Una de las características definitorias de las comunicaciones militares modernas es la importancia central de la seguridad. A medida que las redes de comunicación se interconectan más y se basan cada vez más en el software, están cada vez más expuestas a ciberataques, guerra electrónica y explotación por parte de adversarios. La confidencialidad, la integridad, la disponibilidad y la autenticidad de la información ya no son conceptos técnicos abstractos, sino necesidades operativas. Los sistemas de comunicación comprometidos pueden dar lugar a desinformación, pérdida de autoridad de mando, fracaso de la misión o escalada no deseada. Por consiguiente, las consideraciones de seguridad deben integrarse en todos los niveles del diseño de los sistemas de comunicación, desde los mecanismos físicos de transmisión hasta las arquitecturas de red y los servicios a nivel de aplicación.

Al mismo tiempo, la innovación tecnológica se está acelerando a un ritmo sin precedentes. Los avances en las comunicaciones digitales, la criptografía, la inteligencia artificial, los sistemas satelitales y las tecnologías emergentes, como la

comunicación cuántica, están remodelando rápidamente el panorama de las comunicaciones militares. Estos avances ofrecen importantes oportunidades para mejorar el rendimiento, la resiliencia y la adaptabilidad, pero también introducen nuevas vulnerabilidades y complejidades. Por lo tanto, las instituciones militares deben equilibrar la adopción de tecnologías avanzadas con un diseño arquitectónico riguroso, disciplina operativa y responsabilidad ética.

Este libro surge de la necesidad de ofrecer un examen exhaustivo e integrado de los sistemas de comunicaciones militares seguras en el contexto de las operaciones de defensa modernas y futuras. En lugar de centrarse en tecnologías aisladas o problemas técnicos concretos, el libro adopta una perspectiva a nivel de sistema que considera las comunicaciones como un marco interconectado que involucra hardware, software, mecanismos de seguridad, doctrina operativa y toma de decisiones humanas. El objetivo es presentar una comprensión coherente de cómo se diseñan, implementan y evolucionan los sistemas de comunicaciones seguras para satisfacer las demandas de la guerra contemporánea.

Los primeros capítulos establecen el contexto fundamental para el debate. Las comunicaciones militares modernas se examinan a través de su evolución histórica, desde los sistemas analógicos y punto a punto hasta las arquitecturas digitales, cifradas y en red. Esta evolución refleja cambios más amplios en la doctrina militar, el ritmo operativo y los requisitos de información. Se destaca la importancia de las comunicaciones seguras no solo en términos de protección de la información, sino también para permitir una acción militar coordinada y legal. Se hace hincapié en el papel de la normalización, en particular en el marco de las alianzas, como factor crítico para garantizar la interoperabilidad y la cohesión operativa entre las fuerzas aliadas.

A continuación, el libro explora los principios fundamentales que subyacen a los sistemas de comunicación segura. Se examinan la transmisión y propagación de señales, así como los retos asociados a la comunicación con y sin línea de visión, con el fin de establecer una base técnica. Estos principios siguen siendo relevantes a pesar de los avances tecnológicos, ya que las limitaciones físicas y los factores ambientales siguen determinando el rendimiento de las comunicaciones. Partiendo de esta base, el libro analiza los mecanismos de seguridad fundamentales, como el cifrado, la autenticación, el control de acceso y las técnicas antiinterferencias. Estos elementos constituyen la columna vertebral de las arquitecturas de comunicación segura y son esenciales para mantener la fiabilidad y la confianza en entornos conflictivos.

La ciberseguridad surge como tema central en los capítulos siguientes. Las redes de comunicación militares son cada vez más objeto de sofisticadas amenazas cibernéticas que buscan interrumpir las operaciones, filtrar información

confidencial o manipular los procesos de toma de decisiones. El libro examina la naturaleza de estas amenazas y las estrategias utilizadas para mitigarlas, incluyendo el refuerzo de las redes, la selección de protocolos criptográficos, las arquitecturas de confianza cero y los mecanismos de respuesta a incidentes. Al abordar la ciberseguridad tanto a nivel técnico como arquitectónico, el libro hace hincapié en la importancia de la resiliencia y la adaptabilidad frente a amenazas persistentes y en constante evolución.

Los sistemas de comunicación por radio siguen siendo una piedra angular de las operaciones tácticas, y su papel se examina en profundidad. Los sistemas tradicionales de VHF, UHF y HF siguen proporcionando capacidades esenciales, especialmente en entornos en los que la infraestructura es limitada o está degradada. La integración de estos sistemas con radios definidas por software y técnicas de redes en malla ilustra cómo las tecnologías heredadas pueden mejorarse mediante enfoques arquitectónicos modernos. La interoperabilidad con las fuerzas aliadas se considera un requisito clave, lo que refleja la realidad de las operaciones conjuntas y de coalición en los escenarios de conflicto contemporáneos.

El uso cada vez mayor de sistemas aéreos no tripulados introduce nuevas dimensiones en las comunicaciones militares. Los UAV sirven como recopiladores de datos, repetidores de comunicaciones y plataformas operativas que amplían el alcance y la flexibilidad de las redes militares. El libro analiza los retos de seguridad asociados a la comunicación entre los UAV y los centros de mando, incluyendo el cifrado, la autenticación, la protección de la capa de enlace y las limitaciones de rendimiento, como la latencia y la fiabilidad. Un estudio de caso específico presenta una plataforma de comunicación segura integrada, que ilustra cómo los conceptos teóricos pueden aplicarse en la práctica para abordar los requisitos operativos del mundo real.

La inteligencia artificial representa una fuerza transformadora en los sistemas de comunicación militar. El libro explora cómo las técnicas de IA pueden mejorar la eficiencia del enrutamiento, la detección de intrusiones, la asignación del espectro y la gestión de redes en entornos de campo de batalla. Al permitir que los sistemas detecten, aprendan y se adapten, las arquitecturas de comunicación impulsadas por la IA ofrecen nuevos niveles de resiliencia y eficiencia operativa. Al mismo tiempo, la integración de la IA plantea importantes cuestiones relacionadas con la transparencia, la rendición de cuentas y el control, que se abordan mediante un análisis equilibrado y crítico.

Las tecnologías emergentes constituyen otro punto central del libro. Se examinan las redes celulares de próxima generación, las comunicaciones por satélite, la distribución de claves cuánticas y las redes de radio cognitivas como facilitadoras de las futuras capacidades de comunicación militar. Estas tecnologías amplían el

ámbito operativo al admitir mayores velocidades de datos, conectividad global, mayor seguridad y uso inteligente del espectro. Su integración en los sistemas militares refleja un cambio hacia una arquitectura híbrida que combina componentes terrestres, aéreos, marítimos y espaciales en un marco de comunicación unificado.

Los capítulos finales sintetizan estos avances tecnológicos y conceptuales en un debate más amplio sobre cómo se pueden construir marcos de comunicación seguros para el ejército del futuro. Se analizan los requisitos de las fuerzas modernas en términos de resiliencia, interoperabilidad, escalabilidad y seguridad. Se presentan principios arquitectónicos para ilustrar cómo se pueden diseñar sistemas de comunicación táctica seguros para apoyar operaciones complejas y distribuidas. Se hace hincapié en la integración con los sistemas C4ISR como factor crítico para lograr la conciencia situacional y la superioridad en la toma de decisiones. Se abordan consideraciones éticas y legales para garantizar que la innovación tecnológica se ajuste a las normas y responsabilidades establecidas. El debate sobre las tendencias futuras ofrece una perspectiva de futuro sobre cómo es probable que evolucionen los sistemas de comunicación militar en respuesta a las amenazas emergentes y las oportunidades tecnológicas.

El público al que va dirigido este libro incluye a profesionales militares, ingenieros de defensa, investigadores y estudiantes de posgrado dedicados al estudio y desarrollo de sistemas de comunicación seguros. El libro también es relevante para los responsables políticos y los encargados de la toma de decisiones que participan en la planificación de la defensa y el desarrollo de capacidades. Al combinar el análisis técnico con perspectivas arquitectónicas y operativas, el libro busca salvar la brecha entre la teoría y la práctica en las comunicaciones militares.

Este libro pretende contribuir a la comprensión y el desarrollo de sistemas de comunicaciones militares seguros, presentando una perspectiva integrada y orientada al futuro. A medida que la guerra sigue evolucionando en complejidad y alcance, la capacidad de comunicarse de forma segura, fiable e inteligente seguirá siendo un factor decisivo para la eficacia militar. A través de su examen exhaustivo de las tecnologías, la arquitectura y los principios, esta obra pretende sentar las bases para la creación de sistemas de comunicaciones que respalden el éxito operativo, al tiempo que se mantiene la seguridad, la resiliencia y la responsabilidad en las operaciones militares modernas y futuras.

Conclusión

Este libro ha examinado la evolución, la estructura y la dirección futura de los sistemas de comunicaciones militares seguras en el contexto de las operaciones de defensa modernas y emergentes. A lo largo de sus capítulos, la obra ha demostrado que las comunicaciones militares ya no son meras tecnologías de apoyo, sino que constituyen un pilar central de la eficacia operativa, la toma de decisiones estratégicas y la superioridad informativa. La creciente complejidad del entorno de seguridad, combinada con el rápido avance tecnológico, requiere marcos de comunicación que sean resilientes, inteligentes, interoperables y con una base ética.

Los primeros capítulos establecieron la importancia fundamental de las comunicaciones seguras en las operaciones militares. Las fuerzas armadas modernas operan en condiciones de incertidumbre, movilidad y amenaza persistente, en las que la capacidad de intercambiar información precisa y oportuna determina el éxito o el fracaso de la misión. La transición de sistemas analógicos y aislados a arquitecturas de comunicación digitales, cifradas y en red refleja un cambio más amplio hacia la guerra centrada en la información. Esta evolución ha transformado los sistemas de comunicación en facilitadores activos del mando, el control y la coordinación en todos los ámbitos de operación.

Un tema central a lo largo del libro ha sido la relación inseparable entre la comunicación y la seguridad. A medida que las redes militares se vuelven más interconectadas y dependientes del software, están cada vez más expuestas a las amenazas cibernéticas, la guerra electrónica y la explotación adversaria. El análisis del cifrado, la autenticación, el control de acceso y el refuerzo de las redes puso de relieve la necesidad de incorporar mecanismos de seguridad en todas las capas de las arquitecturas de comunicación. En lugar de tratar la seguridad como un complemento, los sistemas militares modernos deben adoptar un enfoque de seguridad desde el diseño que garantice la confidencialidad, la integridad, la autenticidad y la disponibilidad en condiciones conflictivas.

El debate sobre los sistemas de comunicación por radio para unidades tácticas demostró que las tecnologías heredadas siguen siendo operativamente relevantes cuando se integran en la arquitectura moderna. Los sistemas VHF, UHF y HF siguen proporcionando capacidades de comunicación robustas, especialmente en entornos degradados o denegados. Cuando se combinan con radios definidas por software y principios de redes en malla, estas tecnologías ofrecen la flexibilidad y la resiliencia que son esenciales para las operaciones tácticas. La capacidad de adaptar las formas de onda, las frecuencias y las estrategias de enrutamiento permite a las fuerzas mantener la conectividad a pesar de la movilidad, las limitaciones del terreno y las interferencias hostiles.

Se examinaron los sistemas aéreos no tripulados y su integración en marcos de comunicación seguros como una característica definitoria de las operaciones militares contemporáneas. Los UAV funcionan no solo como plataformas de detección, sino también como nodos de comunicación e es dinámicos que amplían el alcance de la red y mejoran el conocimiento de la situación. El análisis de la comunicación entre los UAV y el centro de mando hizo hincapié en la importancia del cifrado, la autenticación, la seguridad de la capa de enlace y la optimización del rendimiento. El estudio de caso presentado ilustró cómo una plataforma de comunicación integrada y segura puede apoyar el intercambio de datos en tiempo real, al tiempo que aborda las limitaciones de latencia, fiabilidad y rendimiento en entornos operativos.

La inteligencia artificial surgió como una fuerza transformadora en los sistemas de comunicación militar. La exploración del enrutamiento impulsado por la IA, la detección de intrusiones, la asignación de espectro y las redes de campo de batalla demostró cómo los algoritmos inteligentes pueden mejorar la adaptabilidad y la resiliencia. La IA permite a los sistemas de comunicación responder dinámicamente a los cambios ambientales y a las acciones adversas, reduciendo la carga cognitiva de los operadores humanos y mejorando el ritmo operativo. Al mismo tiempo, la integración de la IA plantea importantes cuestiones relacionadas con la transparencia, la rendición de cuentas y el control, lo que refuerza la necesidad de una implementación responsable y bien gobernada.

Se analizaron tecnologías emergentes como las redes celulares de próxima generación, las comunicaciones por satélite, la distribución de claves cuánticas y las redes de radio cognitivas como facilitadoras de las futuras capacidades de comunicación militar. Estas tecnologías amplían el ámbito operativo al admitir mayores velocidades de datos, conectividad global, mayor seguridad y uso inteligente del espectro. Su integración en los sistemas militares refleja un cambio hacia arquitecturas híbridas que combinan componentes terrestres, aéreos, marítimos y espaciales. Esta convergencia permite operaciones multidominio, al tiempo que introduce nuevos retos arquitectónicos y de seguridad que deben abordarse de manera holística.

Los capítulos finales se centraron en la construcción de un marco de comunicación seguro para el ejército del futuro. El análisis hizo hincapié en que el avance tecnológico por sí solo es insuficiente sin un diseño arquitectónico coherente, la integración con los sistemas C4ISR y la consideración de las implicaciones éticas y legales. Los futuros marcos de comunicación deben apoyar la interoperabilidad, la escalabilidad y la resiliencia, al tiempo que se ajustan al derecho internacional y a los principios éticos. La inclusión de consideraciones de gobernanza, rendición de cuentas y sostenibilidad garantiza que los sistemas de comunicación contribuyan

a la seguridad y la estabilidad a largo plazo, en lugar de limitarse a proporcionar una ventaja táctica a corto plazo.

Una idea clave de este trabajo es que los futuros sistemas de comunicación militar deben ser ecosistemas adaptables en lugar de infraestructuras estáticas. La naturaleza dinámica de los conflictos modernos exige sistemas que puedan reconfigurarse en respuesta a los cambios en los requisitos de las misiones, las condiciones ambientales y los vectores de amenaza. Esta adaptabilidad requiere una estrecha integración entre las tecnologías de comunicación, los mecanismos de seguridad, los sistemas de control inteligente y los responsables de la toma de decisiones humanas. El éxito e e de estos sistemas depende no solo de la excelencia técnica, sino también de la alineación doctrinal y la preparación organizativa.

Otra conclusión importante es la creciente importancia de la interoperabilidad y las operaciones de coalición. Las misiones militares modernas se llevan a cabo cada vez más en contextos multinacionales, lo que requiere sistemas de comunicación que permitan compartir información de forma controlada, preservando al mismo tiempo los intereses de seguridad nacional. La estandarización, los marcos de seguridad compartidos y los mecanismos flexibles de control de acceso son esenciales para una colaboración eficaz. Las arquitecturas de comunicación que apoyan la interoperabilidad por diseño proporcionan una base para la confianza y la coherencia operativa entre las fuerzas aliadas.

Las dimensiones éticas y jurídicas de la tecnología de las comunicaciones militares representan un área crítica de responsabilidad para los diseñadores, operadores y responsables políticos. A medida que los sistemas de comunicación se vuelven más autónomos y se integran con funciones de apoyo a la toma de decisiones, aumentan las posibles consecuencias de los fallos o el uso indebido de los sistemas. La incorporación de consideraciones éticas y el cumplimiento de la legislación en el diseño de los sistemas garantiza que la superioridad tecnológica no socave la legitimidad o la rendición de cuentas. La innovación responsable en las comunicaciones militares debe equilibrar la eficacia operativa con el cumplimiento de las normas y valores establecidos.

Este libro contribuye al campo al proporcionar una perspectiva integral y completa sobre los sistemas de comunicación militar seguros. En lugar de centrarse en tecnologías aisladas, hace hincapié en la coherencia arquitectónica, la integración de la seguridad y el diseño orientado al futuro. La combinación de análisis teórico, consideraciones prácticas y examen de casos prácticos ofrece un marco estructurado para comprender y desarrollar infraestructuras de comunicación militar modernas.

Desde un punto de vista académico, esta obra sienta las bases para futuras

investigaciones sobre arquitecturas de comunicación adaptativas, gestión de redes impulsada por la inteligencia artificial y sistemas cuánticos seguros. Desde una perspectiva operativa, ofrece información sobre los retos y oportunidades asociados al despliegue de tecnologías de comunicación seguras en entornos complejos. Los conceptos presentados pueden servir de base para el desarrollo de doctrinas, el diseño de sistemas y la formulación de políticas en las instituciones de defensa.

En conclusión, los sistemas de comunicación militar seguros son un factor decisivo en la guerra moderna y futura. A medida que las fuerzas armadas se enfrentan a entornos operativos cada vez más complejos y disputados, la capacidad de intercambiar información de forma segura, fiable e inteligente seguirá siendo un imperativo estratégico. Mediante la adopción de marcos de comunicación integrados, adaptativos y basados en la ética, los ejércitos del futuro podrán alcanzar la superioridad informativa, al tiempo que mantienen la resiliencia, la legitimidad y la eficacia operativa. Este libro pretende contribuir a ese objetivo ofreciendo un examen estructurado y con visión de futuro de las tecnologías, la arquitectura y los principios e es que darán forma al futuro de las comunicaciones militares.

Referencias

1. Defence Strategic Communications, *revista oficial del Centro de Excelencia para la Comunicación Estratégica de la OTAN,* vol. 10, primavera-otoño de 2021, NATO StratCom COE, Riga, Letonia.
2. Polovic, J., «Challenges of Global Communication: Strategic Competition and Escalation of Tensions in International Relations», *Collected Papers of the Faculty of Philosophy,* vol. 48, n.º 1, 2024, pp. 51-57. https://doi.org/10.5671/ca.48.1.7
3. Mustafovski, R., «El uso de plataformas de comunicación en operaciones militares: mejora de la eficacia estratégica y táctica», *Database Systems Journal,* vol. XVI, 2025, Facultad de Ingeniería Eléctrica y Tecnologías de la Información, Universidad Ss. Cyril and Methodius, Skopje, República de Macedonia del Norte.
4. Rienzi, T. M., *Comunicaciones-Electrónica 1962-1970,* Serie de Estudios sobre Vietnam, Departamento del Ejército, Washington, DC, EE. UU., 2002.
5. Mazzenga, F., Landry, R. y Young, K., «Comunicaciones militares», *IEEE Communications Magazine,* octubre de 2020, pp. 50-56.
6. Organización del Tratado del Atlántico Norte (OTAN), *Doctrina Conjunta Aliada para Sistemas de Comunicación e Información (AJP-6),* Edición B, Versión 1, Oficina de Normalización de la OTAN (NSO), abril de 2024.
7. Departamento de Defensa de los Estados Unidos, *Estrategia de modernización C3: mando, control y comunicaciones,* Washington, DC, EE. UU., septiembre de 2020.
8. Monteiro Marques, M., «STANAG 4586 - Interfaces estándar del sistema de control de UAV (UCS) para la interoperabilidad de los UAV de la OTAN», Documento técnico de la OTAN, Escola Naval - Afeite, Portugal.
9. Yarnell, A. M., Dullea, C. y Grunberg, N. E., «Comunicación militar», en *Comunicación militar y médica,* capítulo 11, Comando de Investigación y Desarrollo Médico del Ejército de los Estados Unidos, EE. UU.
10. Timofte, G., «Modernización de los sistemas de comunicaciones militares de acuerdo con los nuevos requisitos operativos, informativos y técnicos del campo de batalla», *Boletín científico de la Academia de Científicos Rumanos,* Bucarest, Rumanía.
11. Hayes, C., *Acuerdos de Normalización de la OTAN (STANAG) para comandantes y personal,* Noticias desde el frente, Centro de Lecciones Aprendidas del Ejército (CALL), Ejército de los Estados Unidos, abril de 2019.
12. Sánchez, R., Evans, J. y Minden, G., «Networking on the Battlefield: Challenges in Highly Dynamic Multi-hop Wireless Networks» (Redes en el campo de batalla: retos en redes inalámbricas multisalto altamente dinámicas), *Actas de IEEE MILCOM 1999,* Atlantic City, Nueva Jersey, EE. UU., octubre de 1999.

13. Kumar, D., «Challenges of a Digitised Battlefield» (Retos de un campo de batalla digitalizado), *Journal of the United Service Institution of India,* vol. CXLII, n.º 590, octubre-diciembre de 2012.
14. Lipscomb, P., «The Evolution of Communications in the Military as it Relates to Leadership» (La evolución de las comunicaciones en el ejército en relación con el liderazgo), *Estudios integrados*, documento n.º 90, Murray State University, 2017. Disponible en: https://digitalcommons.murraystate.edu/bis437/90
15. Amin, M. G., Lindsey, A. R., Zhao, L. y Zhang, Y., *«Técnicas antiinterferencias para receptores GPS»,* Informe técnico final AFRL-IF-RS-TR-2001-186, Laboratorio de Investigación de la Fuerza Aérea, Centro de Investigación de Roma, Nueva York, EE. UU., septiembre de 2001.
16. Bardis, N. G., Doukas, N. y Ntaikos, K., «Diseño y desarrollo de una comunicación militar segura basada en el prototipo de algoritmo criptográfico AES y un esquema avanzado de gestión de claves», *WSEAS Transactions on Information Science and Applications,* Universidad de Educación Militar, Academia del Ejército Helénico, Grecia.
17. Colbeck, M. J. L., «Cifrado cuántico en las comunicaciones militares», *Actas de la conferencia de la EAAW,* 28-29 de noviembre de 2023.
18. Evans, J., Sánchez, R. y Minden, G., «Networking on the Battlefield: Challenges in Highly Dynamic Multi-hop Wireless Networks» (Redes en el campo de batalla: retos en redes inalámbricas multisalto altamente dinámicas), *Actas de IEEEMILCOM,* Atlantic City, Nueva Jersey, EE. UU., octubre de 1999.
19. Hayes, C., «Acuerdos de normalización de la OTAN (STANAG) para comandantes y personal», *Noticias desde el frente,* Centro de Lecciones Aprendidas del Ejército (CALL), abril de 2019.
20. Kang, J. S., «Protocolo de autenticación independiente en entornos de redes tácticas utilizando el enfoque Hash Lock», *International Journal of Machine Learning and Computing,* vol. 5, n.º 5, octubre de 2015.
21. Kovács, L., «Guerra electrónica y los retos asimétricos», *Bolyai Szemle,* n.º 3, 2009, pp. 135-151, ISSN 1416-1443.
22. Kumar, D., «Challenges of a Digitised Battlefield» (Retos de un campo de batalla digitalizado), *Journal of the United Service Institution of India,* vol. CXLII, n.º 590, octubre-diciembre de 2012.
23. Lipscomb, P., «The Evolution of Communications in the Military as it Relates to Leadership» (La evolución de las comunicaciones en el ejército en relación con el liderazgo), *Integrated Studies*, n.º 90, Murray State University, 2017.
24. Sayyed, S. Y., Gurap, S. L., Devadhe, J. L. y Gat, K. R., «A Review on Secure Wireless Communication for Military Application» (Revisión *de* las

comunicaciones inalámbricas seguras para aplicaciones militares), *International Journal of Electrical, Electronics and Data Communication,* vol. 5, n.º 11, noviembre de 2017.
25. Shinde, V., Kulkarni, S. y Malekar, M. R., «Sistema de comunicaciones seguras», *Revista Internacional de Innovaciones en Investigación y Tecnología de Ingeniería (IJIERT),* Actas de la conferencia TECHNO-2K17.
26. Timofte, G., «Modernización de los sistemas de comunicaciones militares de acuerdo con los nuevos requisitos operativos, informativos y técnicos del espacio de batalla de la era de la información ( )», Academia de Científicos Rumanos, Bucarest, Rumanía.
27. Departamento del Ejército de los Estados Unidos, *Doctrina de Comunicaciones de Señales (FM 100-11),* Departamento del Ejército, Washington, DC, julio de 1948.
28. Alnifie, G. y Simon, R., «Una defensa multicanal contra los ataques de interferencia en redes de sensores inalámbricos», en *Actas del 3.er Taller ACM sobre Calidad de Servicio y Seguridad para Redes Inalámbricas y Móviles,* 2007, pp. 95-104.
29. Alnifie, G., y Simon, R., «MULEPRO: Una respuesta multicanal a los ataques de interferencia en redes de sensores inalámbricos», *Comunicaciones inalámbricas y computación móvil,* 2010.
30. Bayraktaroglu, E., King, C., Liu, X., Noubir, G., Rajaraman, R. y Thapa, B., «On the Performance of IEEE 802.11 Under Jamming» (Sobre el rendimiento de IEEE 802.11 bajo interferencias), en *Actas de la 27.ª Conferencia IEEE sobre Comunicaciones Informáticas,* 2008, pp. 1265-1273.
31. Bellardo, J., y Savage, S., «802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions» (Ataques de denegación de servicio 802.11: vulnerabilidades reales y soluciones prácticas), en *Actas del XII Simposio sobre Seguridad de USENIX,* 2003, pp. 15-28.
32. Broustis, I., Pelechrinis, K., Syrivelis, D., Krishnamurthy, S. V., y Tassiulas, L., «FIJI: Fighting Implicit Jamming in 802.11 WLANs» (FIJI: lucha contra las interferencias implícitas en redes WLAN 802.11), *Seguridad y privacidad en redes de comunicación,* vol. 19, 2009, pp. 21-40.
33. Chiang, J. T. y Hu, Y. C., «Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks» (Detección y mitigación de interferencias entre capas en redes de transmisión inalámbrica), *IEEE/ACM Transactions on Networking,* vol. 19, n.º 1, 2011, pp. 286-298.
34. Commander, C. W., Pardalos, P. M., Ryabchenko, V., Shylo, O. V, Uryasev, S. y Zrazhevsky, G., «Jamming Communication Networks Under Complete Uncertainty» (Interferencia en redes de comunicación en condiciones de incertidumbre total), *Optimization Letters*, vol. 2, n.º 1, 2008, pp. 53-70.

35. Gencer, C., Aydogan, E. K. y Celik, C., «A Decision Support System for Locating VHF/UHF Radio Jammer Systems on the Terrain» (Un sistema de apoyo a la toma de decisiones para localizar sistemas de interferencia de radio VHF/UHF en el terreno)*, Information Systems Frontiers,* vol. 10, n.º 1, 2008, pp. 111-124.
36. Gummadi, R., Wetherall, D., Greenstein, B. y Seshan, S., «Comprensión y mitigación del impacto de las interferencias de radiofrecuencia en las redes 802.11», en *Actas de la Conferencia ACM SIGCOMM sobre aplicaciones, tecnologías, arquitecturas y protocolos para comunicaciones informáticas,* 2007, pp. 385-396.
37. Huang, H., Ahmed, N. y Pulluru, S., «On Limited Range Strategic and Random Jamming Attacks in Wireless Ad Hoc Networks» (Sobre los ataques de interferencia estratégicos y aleatorios de alcance limitado en redes inalámbricas ad hoc), *en Actas de la 34.ª Conferencia IEEE sobre redes informáticas locales*, 2010, pp. 1-8.
38. Jain, S. K. y Garg, K., «A Hybrid Model of Defense Techniques Against Base Station Jamming Attack in Wireless Sensor Networks» (Un modelo híbrido de técnicas de defensa contra ataques de interferencia en estaciones base en redes de sensores inalámbricas), *en Actas de la Primera Conferencia Internacional sobre Inteligencia Computacional, Sistemas de Comunicación y Redes*, 2009, pp. 102-107.
39. Kerkez, B., Watteyne, T., Magliocco, M., Glaser, S. y Pister, K., « » (Análisis de viabilidad del diseño de controladores para el salto de canal adaptativo), en *Actas de la IV Conferencia Internacional ICST sobre Metodologías y Herramientas de Evaluación del Rendimiento*, 2009, pp. 76:1-76:6.
40. Khattab, S., Mosse, D. y Melhem, R., «Jamming Mitigation in Multi-Radio Wireless Networks: Reactive or Proactive?» (Mitigación de interferencias en redes inalámbricas multirradio: ¿reactiva o proactiva?), en *Actas de la 4.ª Conferencia Internacional sobre Seguridad y Privacidad en Redes de Comunicación,* 2008, pp. 27:1-27:10.
41. Khattab, S., Mosse, D. y Melhem, R., «Modelización de la defensa contra interferencias mediante salto de canal en redes inalámbricas multirradio», en *Actas de la 5.ª Conferencia Internacional Anual sobre Sistemas Móviles y Ubicuos: Informática, Redes y Servicios,* 2008, pp. 25:1-25:10.
42. Lazos, L., Liu, S. y Krunz, M., «Mitigación de los ataques de interferencia en el canal de control en redes ad hoc multicanal», en *Actas de la 2.ª Conferencia ACM sobre Seguridad de Redes Inalámbricas,* 2009, pp. 169-180.
43. Li, M., Koutsopoulos, I. y Poovendran, R., «Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks» (Ataques de interferencia óptimos y políticas de defensa de redes en redes de sensores inalámbricos), en *Actas de la 26.ª Conferencia Internacional IEEE sobre Comunicaciones Informáticas,*

2007, pp. 1307-1315.
44. Liu, H., Liu, Z., Chen, Y. y Xu, W., «Determining the Position of a Jammer Using a Virtual-Force Iterative Approach» (Determinación de la posición de un interferidor mediante un enfoque iterativo de fuerza virtual), *Wireless Networks,* vol. 17, n.º 2, 2011, pp. 531-547.
45. Liu, Z., Liu, H., Xu, W. y Chen, Y., «Aprovechamiento de los cambios en los vecinos causados por el interferidor para la localización del interferidor», *IEEE Transactions on Parallel and Distributed Systems,* 2011.
46. Misra, S., Singh, R. y Mohan, S. V. R., «Mecanismo de detección de ataques de interferencia aptos para la guerra de la información para redes de sensores inalámbricos utilizando un sistema de inferencia difusa», *Sensors,* vol. 10, 2010, pp. 3444-3479.
47. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C. y Pantziou, G., «Estudio sobre ataques de interferencia y contramedidas en redes de sensores inalámbricos», *IEEE Communications Surveys and Tutorials*, vol. 11, n.º 4, 2009, pp. 42-56.
48. Muraleedharan, R., y Osadciw, L. A., «Detección de ataques de interferencia y contramedidas en redes de sensores inalámbricos utilizando el sistema Ant», en *Actas de SPIE - Sociedad Internacional de Ingeniería Óptica,* vol. 6248, 2006, artículo 62480G.
49. Navda, V, Bohra, A., Ganguly, S., y Rubenstein, D., «Uso del salto de canal para aumentar la resistencia del 802.11 a los ataques de interferencia», en *Actas de la 26.ª Conferencia Internacional IEEE sobre Comunicaciones Informáticas*, 2007, pp. 2526-2530.
50. Panyim, K., Hayajneh, T., Krishnamurthy, P. y Tipper, D., «Jamming Dust: A Low Power Distributed Jammer Network» (Interferencia de polvo: una red de interferencias distribuida de baja potencia), en *Actas de la 27.ª Conferencia Científica del Ejército de los Estados Unidos ( )*, 2009, pp. 922-929.
51. Pelechrinis, K., Koufogiannakis, C. y Krishnamurthy, S. V., «Gaming the Jammer: Is Frequency Hopping Effective?» (Jugando con el interferidor: ¿es eficaz el salto de frecuencia?), en *Actas de la 7.ª Conferencia Internacional sobre Modelización y Optimización en Redes Móviles, AdHoc e Inalámbricas,* 2009, pp. 187-196.
52. Pelechrinis, K., Koutsopoulos, I., Broustis, I. y Krishnamurthy, S. V., «Lightweight Jammer Localization in Wireless Networks: System Design and Implementation», en *Actas de la Conferencia Global de Telecomunicaciones del IEEE,* 2009, pp. 1-6.
53. Pelechrinis, K., Iliofotou, M. y Krishnamurthy, S. V., «Denial of Service Attacks in Wireless Networks: The Case of Jammers» (Ataques de denegación de servicio en redes inalámbricas: el caso de los inhibidores), *IEEE Communications*

Surveys and Tutorials, vol. 13, n.º 2, 2011, pp. 245-257.
54. Shin, I., Shen, Y., Xuan, Y., Thai, M. T. y Znati, T., «Ataques de interferencia reactiva en redes de sensores inalámbricos multirradio: una medida de mitigación eficaz mediante la identificación de nodos desencadenantes», en *Actas del 2.º Taller Internacional ACM sobre Fundamentos de Redes y Computación Inalámbricas Ad Hoc y de Sensores,* 2009, pp. 87-96.
55. Strasser, M., Danev, B. y Capkun, S., «Detección de interferencias reactivas en redes de sensores», *ACM Transactions on Sensor Networks*, vol. 7, n.º 2, 2010, artículo 16.
56. Sun, Y. y Wang, X., «Jammer Localization in Wireless Sensor Networks» (Localización de interferencias en redes de sensores inalámbricas), en *Actas de la 5.ª Conferencia Internacional sobre Comunicaciones Inalámbricas, Redes y Computación Móvil,* 2009, pp. 1-4.
57. Tague, P., Slater, D., Poovendran, R. y Noubir, G., «Linear Programming Models for Jamming Attacks on Network Traffic Flows» (Modelos de programación lineal para ataques de interferencia en flujos de tráfico de red), en *Actas del 6.º Simposio Internacional sobre Modelización y Optimización en Redes Móviles, Ad Hoc e Inalámbricas y Talleres,* 2008, pp. 207-216.
58. Thamilarasu, G. y Sridhar, R., «Game Theoretic Modeling of Jamming Attacks in Ad Hoc Networks» (Modelización teórica de juegos de ataques de interferencia en redes ad hoc), en *Actas de la 18.ª Conferencia Internacional sobre Comunicaciones y Redes Informáticas*, 2009, pp. 1-6.
59. Wang, H., Zhang, L., Li, T. y Tugnait, J., «Spectrally Efficient Jamming Mitigation Based on Code-Controlled Frequency Hopping» (Mitigación de interferencias espectralmente eficiente basada en el salto de frecuencia controlado por código)*, IEEE Transactions on Wireless Communications,* vol. 10, n.º 3, 2011, pp. 728-732.
60. Wilhelm, M., Martinovic, I., Schmitt, J. B. y Lenders, V., «Reactive Jamming in Wireless Networks: How Realistic Is the Threat?» (Interferencias reactivas en redes inalámbricas: ¿hasta qué punto es realista la amenaza?), en *Actas de la IV Conferencia ACM sobre Seguridad de Redes Inalámbricas,* 2011, pp. 47-52.
61. Wood, A., Stankovic, J. y Son, S., «JAM: un servicio de mapeo de áreas interferidas para redes de sensores», en *Actas del 24.º Simposio IEEE sobre Sistemas en Tiempo Real,* 2003, pp. 286-297.
62. Wood, A., Stankovic, J. y Zhou, G., «DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-Based Wireless Networks» (DEEJAM: cómo derrotar el bloqueo eficiente en términos de energía y espectro en redes inalámbricas basadas en IEEE 802.15.4), *en Actas de la 4.ª Conferencia Anual de la Sociedad de Comunicaciones IEEE sobre Sensores, Redes en Malla y*

Comunicaciones y Redes Ad Hoc, 2007, pp. 60-69.
63. Xu, W., Wood, T., Trappe, W. y Zhang, Y., «Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service», en *Actas del 3.º Taller ACM sobre Seguridad Inalámbrica*, 2004, pp. 80-89.
64. Xu, W., Trappe, W., Zhang, Y. y Wood, T., «The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks» (La viabilidad de lanzar y detectar ataques de interferencia en redes inalámbricas), en *Actas del 6.º Simposio Internacional ACM sobre Redes y Computación AdHoc Móviles,* 2005, pp. 46-57.
65. Yoon, S. U., Murawski, R., Ekici, E., Park, S. y Mir, Z., «Adaptive Channel Hopping for Interference-Robust Wireless Sensor Networks» (Salto de canal adaptativo para redes de sensores inalámbricos resistentes a las interferencias), en *Actas de la Conferencia Internacional IEEE sobre Comunicaciones*, 2010, pp. 1-5.
66. Estado Mayor del Ejército Italiano - Oficina de Seguridad, *Sistemas de Software, Telecomunicaciones y Seguridad - Documentos no clasificados,* Roma, Italia, 2008.
67. Estado Mayor del Ejército Italiano - Oficina de Seguridad, *Sistemas de Software, Telecomunicaciones y Seguridad - Documentos clasificados,* Roma, Italia, 2008.
68. ISO/IEC 15408-1, *Tecnología de la información - Técnicas de seguridad - Criterios de evaluación para la seguridad de la tecnología de la información - Parte 1: Introducción y modelo general,* Organización Internacional de Normalización, Ginebra, 2009.
69. ISO/IEC 15408-2, *Tecnología de la información. Técnicas de seguridad. Criterios de evaluación para la seguridad de la tecnología de la información. Parte 2: Componentes funcionales de seguridad,* Organización Internacional de Normalización, Ginebra, 2008.
70. ISO/IEC 15408-3, *Tecnología de la información. Técnicas de seguridad. Criterios de evaluación para la seguridad de la tecnología de la información. Parte 3: Componentes de garantía de la seguridad,* Organización Internacional de Normalización, Ginebra, 2008.
71. Departamento de Defensa de los Estados Unidos, *Criterios de evaluación de sistemas informáticos fiables,* DoDD 5200.28-STD, Washington, DC, diciembre de 1985.
72. Departamento de Defensa de los Estados Unidos, *Directiva: Garantía de la información,* DoDD 8500.01E, Washington, DC, octubre de 2002.
73. Oficina Federal Alemana de Seguridad de la Información, *Notas de aplicación e interpretación del esquema (AIS): ITSEC a Criterios Comunes con potencial de ataque específico,* Bonn, Alemania, 2010. Disponible en línea: https://www.bsi.bund.de
74. ISO/IEC 27000, *Tecnología de la información. Técnicas de seguridad.*

Sistemas de gestión de la seguridad de la información. Visión general y vocabulario, Organización Internacional de Normalización, Ginebra, 2009.
75. Hare, F., «La amenaza cibernética para la seguridad nacional: ¿por qué no nos ponemos de acuerdo?», en *Actas de la Conferencia sobre Conflictos Cibernéticos,* Tallin, Estonia, 2010, pp. 211-225.
76. Liles, S., «La guerra cibernética: como forma de conflicto de baja intensidad e insurgencia», en *Actas de la Conferencia sobre Conflictos Cibernéticos*, Tallin, Estonia, 2010, pp. 47-57.
77. Kotenko, I. V., «Multi-Agent Modeling and Simulation of Cyber-Attacks and Cyber Defense for Homeland Security», en *Actas del Taller Internacional IEEE sobre Adquisición Inteligente de Datos y Sistemas Informáticos Avanzados: Tecnología y Aplicaciones,* Dortmund, Alemania, 6-8 de septiembre de 2008.
78. Kotenko, I. V. y Ulanov, A. V., «Simulación basada en agentes de ataques DDoS y mecanismos de defensa», *Journal of Computing,* vol. 4, n.º 2, 2005.
79. Gasser, L., «Criptografía poscuántica», en V. Mulder, A. Mermoud, V. Lenders y B. Tellenbach (eds.), *Tendencias en tecnologías de protección y cifrado de datos,* Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33386-6. 10
80. Radanliev, P., «Artificial Intelligence and Quantum Cryptography», *Journal of Analytical Science and Technology,* vol. 15, artículo 4, 2024. https://doi.org/10.1186/s40543-024- 00416-6
81. Atutxa, A., Sanz, A., Sasiain, J., Astorga, J. y Jacob, E., «Hacia un 5G cuánticamente seguro: distribución de claves cuánticas en redes centrales», *Computer Communications*, vol. 224, 2024, pp. 145-158. https://doi.org/10.1016Zj.comcom.2024.06.005
82. Ricci, S., Dobias, P., Malina, L., Hajny, J. y Jedlicka, P., «Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography» (Claves híbridas en la práctica: combinación de criptografía clásica, cuántica y poscuántica), *IEEE Access,* vol. 12, 2024, pp. 23206-23219. https://doi.org/10.1109/ACCESS.2024.3364520
83. Shim, K.-S., Kim, B. y Lee, W., «Investigación sobre protocolos aplicados de claves cuánticas, claves de distribución y claves de criptografía poscuántica para la ciencia de datos y la seguridad web», *Journal of Web Engineering,* vol. 23, n.º 6, septiembre de 2024, pp. 813-830. https://doi.org/10.13052/jwe1540-9589.2365
84. Dhar, S., Khare, A., Dwivedi, A. D. y Singh, R., «Securing IoT Devices: A Novel Approach Using Blockchain and Quantum Cryptography» (*Protección de dispositivos IoT: un enfoque* novedoso mediante el uso de *blockchain y* criptografía cuántica), *Internet of Things,* vol. 25, 2024, artículo 101019. https:ZZdoi.org/10.1016Zj.iot.2023.101019
85. Schneier, B., «Criptosistemas basados en redes y criptoanálisis cuántico», *Communications of the ACM,* Online First, junio de 2024.

https://doi.org/10.1145/3665224
86. Bozzio, M., Vyvlecka, M., Cosacchi, M., et al., «Enhancing Quantum Cryptography with Quantum Dot Single-Photon Sources» (Mejora de la criptografía cuántica con fuentes de fotones únicos de puntos cuánticos), *npj Quantum Information,* vol. 8, artículo 104, 2022. https://doi.org/10.1038/s41534-022-00626-z
87. Akçay, L., y Yalçın, B. Ö., «Diseño ASIP ligero para algoritmos de criptografía poscuántica basados en redes de puntos cuánticos ( )», *Arabian Journal for Science and Engineering*, 2024. https://doi.org/10.1007/s13369-024-08976-w
88. Oliva del Moral, J., de Marti i Olius, A., Vidal, G., Crespo, P. M., y Etxezarreta Martinez, J., «Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective», *IEEE Internet of Things Journal,* vol. 11, n.º 18, 15 de septiembre de 2024, pp. 30217-30244. https://doi.org/10.1109/JIOT.2024.3410702
89. Rubio García, C., Rommel, S., Takarabt, S., Vegas Olmos, J. J., Guilley, S., Nguyen, P.,
y Tafur Monroy, I., «Quantum-Resistant Transport Layer Security», *Computer Communications*, vol. 213, 2024, pp. 345-358.
https://doi.org/10.1016/j.comcom.2023.11.010
90. Alhakami, H., «Enhancing IoT Security: Quantum-Level Resilience Against Threats» (Mejora de la seguridad del IoT: resiliencia a nivel cuántico frente a las amenazas), *Computers, Materials and Continua,* vol. 78, n.º 1, 2024, pp. 329-356. https://doi.org/10.32604/cmc.2023.043439
91. Chawla, D. y Mehra, P. S., «A Survey on Quantum Computing for Internet of Things Security» (Estudio sobre la computación cuántica para la seguridad del Internet de las cosas), *Procedia Computer Science*, vol. 218, 2023, pp. 2191-2200. https://doi.org/10.1016Zj.procs.2023.01.195
92. Hekkala, J., Muurman, M., Halunen, K., et al., «Implementing Post-Quantum Cryptography for Developers» (Implementación de la criptografía poscuántica para desarrolladores), *SN Computer Science*, vol. 4, artículo 365, 2023. https://doi.org/10.1007/s42979-023-01724-1
93. Ji, X., Wang, B., Hu, F., Wang, C. y Zhang, H., «Nueva arquitectura informática avanzada
para el diseño y análisis criptográfico mediante el annealer cuántico D-Wave», *Tsinghua Science and Technology,* vol. 27, n.º 4, agosto de 2022, pp. 751-759.
https://doi.org/10.26599/TST.2021.9010022
94. Hasan, K. F., et al., «Un marco para la migración a la criptografía poscuántica: análisis de la dependencia de la seguridad y estudios de casos», *IEEE Access,* vol. 12, 2024, pp. 23427-23450. https://doi.org/10.1109/ACCESS.2024.3360412

95. Kong, I., Janssen, M. y Bharosa, N., «Realizing Quantum-Safe Information Sharing: Implementation and Adoption Challenges and Policy Recommendations for Quantum-Safe Transitions» (Cómo lograr un intercambio de información seguro desde el punto de vista cuántico: retos de implementación y adopción y recomendaciones políticas para transiciones seguras desde el punto de vista cuántico), *Government Information Quarterly*, vol. 41, n.º 1, 2024, artículo 101884. https://doi.Org/10.1016/j.giq.2023.101884
96. Pan, D., et al., «The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet» (La evolución de la *comunicación directa cuántica segura: hacia la* Qinternet), *IEEE Communications Surveys and Tutorials,* vol. 26, n.º 3, 2024, pp. 1898-1949. https://doi.org/10.1109/COMST.2024.3367535
97. Hoque, S., Aydeger, A. y Zeydan, E., «Exploring Post-Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design» (Exploración de la criptografía poscuántica con distribución de claves cuánticas para el diseño de una arquitectura de red *móvil sostenible*), en *Actas del 4.º Taller sobre Rendimiento y Eficiencia Energética de los Sistemas Concurrentes y Distribuidos (PECS '24),* ACM, Nueva York, 2024, pp. 9-16. https://doi.org/10.1145/3659997.3660033
98. Piatkowski, J. y Szymoniak, S., «Trivializing Verification of Cryptographic Protocols» (Trivialización de la verificación de protocolos criptográficos), *Computer Assisted Methods in Engineering and Science*, vol. 30, n.º 4, 2023, pp. 389-406. https://doi.org/10.24423/cames.869
99. Basin, D. A., Cremers, C. y Meadows, C. A., «Model Checking Security Protocols» (Comprobación de modelos de protocolos de seguridad), en E. Clarke, T. Henzinger, H. Veith y R. Bloem (eds.), *Handbook of Model Checking (Manual de comprobación de modelos),* Springer, Cham, 2018, pp. 727-762. https://doi.org/10.1007/978-3-319-10575-8_22
100. Blanchet, B., «Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif», *Foundations and Trends in Privacy and Security*, vol. 1, n.º 12, 2016, pp. 1-135. https://doi.org/10.1561/3300000004
101. Blanchet, B., Cheval, V. y Cortier, V., «ProVerif con lemas, inducción, subsunción rápida y mucho más», en *Actas del Simposio IEEE sobre Seguridad y Privacidad (S&P 2022),* IEEE Computer Society, San Francisco, California, 2022, pp. 205-222. https://hal.inria.fr/hal-03366962/
102. Bouroulet, R., Devillers, R., Klaudel, H., Pelz, E. y Pommereau, F., «Modelado y análisis de protocolos de seguridad utilizando especificaciones basadas en roles y redes de Petri», en K. M. van Hee y R. Valk (eds.), *Aplicaciones y teoría de las redes de Petri,* Springer, Berlín y Heidelberg, 2008, pp. 72-91.
103. Burrows, M., Abadi, M. y Needham, R., «Una lógica de autenticación», *ACM*

Transactions on Computer Systems, vol. 8, n.º 1, 1990, pp. 18-36. https://doi.org/10.1145/77648.77649

104. Chevalier, Y., et al., «A High Level Protocol Specification Language for Industrial Security Sensitive Protocols», en *Actas del taller sobre especificación y procesamiento automatizado de requisitos de seguridad (SAPS 2004),* Sociedad Austriaca de Informática, Linz, Austria, 2004, p. 13.

105. Cortier, V., Delaune, S. y Dreier, J., «Automatic Generation of Source Lemmas in Tamarin: Towards Automatic Proofs of Security Protocols» (Generación automática de lemas fuente en Tamarin: hacia pruebas automáticas de protocolos de seguridad), en L. Chen, N. Li, K. Liang y S. Schneider (eds.), *Computer Security - ESORICS 2020,* Springer, Cham, 2020, pp. 3-22.

106. David, A., Larsen, K. G., Legay, A., Mikucionis, M. y Poulsen, D. B., «UPPAAL SMC Tutorial», *International Journal on Software Tools for Technology Transfer,* vol. 17, n.º 4, 2015, pp. 397-415. https://doi.org/10.1007/s10009-014-0361-y

107. Dolev, D. y Yao, A. C., «On the Security of Public Key Protocols», en *Actas del 22.º Simposio Anual sobre Fundamentos de la Informática (SFCS '81),* IEEE Computer Society, Washington, DC, 1981, pp. 350-357.

108. Gregor, D., Järvi, J., Siek, J., Reis, G., Stroustrup, B., y Lumsdaine, A., « » (Conceptos: soporte lingüístico para la programación genérica en C++), *ACM SIGPLAN Notices,* vol. 41, n.º 10, 2006, pp. 291-310. https://doi.org/10.1145/1167515.1167499

109. Grosser, A., Kurkowski, M., Piatkowski, J. y Szymoniak, S., «ProToc: un lenguaje universal para especificaciones de protocolos de seguridad», en A. Wilinski, I. E. Fray y J. Pejas (eds.), *Soft Computing in Computer and Information Science,* Advances in Intelligent Systems and Computing, vol. 342, Springer, Cham, 2014, pp. 237-248. https://doi.org/10.1007/978-3-319-15147-2_20

110. Hercog, D., *Communication Protocols: Principles, Methods and Specifications*, Springer, 2020. https://doi.org/10.1007/978-3-030-50405-2

111. Hess, A. y Modersheim, S., «A Typing Result for Stateful Protocols», en *Actas del 31.º Simposio sobre Fundamentos de Seguridad Informática (CSF 2018) del IEEE,* IEEE, 2018, pp. 374-388. https://doi.org/10.1109/CSF.2018.00034

112. Järvi, J., Gregor, D., Willcock, J., Lumsdaine, A. y Siek, J., «Algorithm en programación genérica: retos de los genéricos restringidos en C++», *ACM SIGPLAN Notices*, vol. 41, n.º 6, 2006, pp. 272-282. https://doi.org/10.1145/1133255.1134014

113. Kassem, A., Lafourcade, P., Lakhnech, Y. y Modersheim, S., «Multiple Independent Lazy Intruders», en *Actas del 1.er Taller sobre Temas Candentes en Principios de Seguridad y Confianza (HotSpot 2013)*, 2013, 15 páginas.

114. Kordy, B., Mauw, S., Radomirovic, S. y Schweitzer, P., «Fundamentos de

los árboles de ataque-defensa», en P. Degano, S. Etalle y J. Guttman (eds.), *Aspectos formales en seguridad y confianza (FAST 2010),* Lecture Notes in Computer Science, vol. 6561, Springer, Berlín y Heidelberg, 2010, pp. 80-95. https://doi.org/10.1007/978-3-642-19751-2_6

115. Kruse, R. L. y Ryba, A. J., *Data Structures and Program Design in C++,* Prentice-Hall, EE. UU., 1998.

116. Kurkowski, M., *Métodos formales para la verificación de las propiedades de los protocolos de seguridad en redes informáticas* (en polaco), Akademicka Oficyna Wydawnicza Exit, Varsovia, 2013.

117. Liang, J., Nguyen, Q., Simoff, S., Huang, M., «Divide and Conquer Treemaps: Visualizing Large Trees with Various Shapes», *Journal of Visual Languages and Computing,* vol. 31, 2015, pp. 104-127. https://doi.org/10.1016/jjvlc.2015.10.009

118. Liu, S., Xiao, T., Liu, J., Wang, X., Wu, J. y Zhu, J., «Visual Diagnosis of Tree Boosting Methods» (Diagnóstico visual de métodos de refuerzo de árboles), *IEEE Transactions on Visualization and Computer Graphics,* vol. 24, n.º 1, 2017, pp. 163-173. https://doi.org/10.1109/TVCG.2017.2744378

119. Mauw, S. y Oostdijk, M., «Fundamentos de los árboles de ataque», en *Conferencia Internacional sobre Seguridad de la Información y Criptología,* Springer, 2005, pp. 186-198. https://doi.org/10.1007/11734727_17

120. Millen, J. K., «CAPSL: Common Authentication Protocol Specification Language», en *Actas del Taller sobre Nuevos Paradigmas de Seguridad (NSPW '96),* 1996. https://doi.org/10.1145/304851.304879

121. Morin, P., *Open Data Structures (en C++),* 2013. https://opendatastructures.org/

122. Modersheim, S., Nielson, F. y Nielson, H. R., «Lazy Mobile Intruders», en D. A. Basin y J. C. Mitchell (eds.), *Principles of Security and Trust (POST),* Lecture Notes in Computer Science, vol. 7796, Springer, 2013, pp. 147-166.

123. Needham, R. M. y Schroeder, M. D., «Using Encryption for Authentication in Large Networks of Computers», *Communications of the ACM*, vol. 21, n.º 12, 1978, pp. 993-999. https://doi.org/10.1145/359657.359659

124. Neuman, B. C. y Ts'o, T., «Kerberos: An Authentication Service for Computer Networks» (*Kerberos*: un servicio de *autenticación para* redes informáticas), *IEEE Communications Magazine*, vol. 32, n.º 9, 1994, pp. 33-38. https://doi.org/10.1109/35.312841

125. Piatkowski, J., «The Conditional Multiway Mapped Tree: Modeling and Analysis of Hierarchical Data Dependencies» (El árbol mapeado condicional multidireccional: modelado y análisis de dependencias jerárquicas de datos), *IEEE Access*, vol. 8, 2020, pp. 74083-74092. https://doi.org/10.1109/ACCESS.2020.2988358

126. Ryan, P. Y. A., Schneider, S. A., Goldsmith, M. H., Lowe, G. y Roscoe, A. W., *The Modelling and Analysis of Security Protocols: The CSP Approach,* Addison-Wesley Professional, Harlow, Londres, 2000.
127. Siedlecka-Lamch, O., Szymoniak, S. y Kurkowski, M., «A Fast Method for Security Protocols Verification», en *Actas de la 18.ª Conferencia Internacional sobre Sistemas Informáticos y Gestión Industrial (CISIM 2019),* Springer, 2019, pp. 523-534. https://doi.org/10.1007/978-3-030-28957-7_43
128. Siedlecka-Lamch, O., Szymoniak, S., Kurkowski, M. y Fray, I. E., «Towards the Most Efficient Method for Untimed Security Protocols Verification» (Hacia el método más eficiente para la verificación de protocolos de seguridad sin tiempo), en *Actas de la 24.ª Conferencia Asia-Pacífico sobre Sistemas de Información (PACIS 2020),* Dubái, Emiratos Árabes Unidos, 2020, p. 189.
129. Siek, J. G. y Lumsdaine, A., «A Language for Generic Programming in the Large» (Un lenguaje para la programación genérica a gran escala)*, Science of Computer Programming,* vol. 76, n.º 5, 2011, pp. 423-465. https://doi.org/10.1016/j.scico.2008.09.009
130. Szymoniak, S., «Amelia: A New Security Protocol for Protection Against False
Links», *Computer Communications*, vol. 179, 2021, pp. 73-81.
https://doi.org/10.1016/j.comcom.2021.07.030
131. Szymoniak, S., Kurkowski, M. y Piatkowski, J., «Modelos temporizados de protocolos de seguridad
que incluyen retrasos en la red», *Journal of Applied Mathematics and Computational Mechanics,* vol. 14, n.º 3, 2015, pp. 127-139.
https://doi.org/10.17512/jamcm.2015.3.14
132. Tremblay, J.-P. y Sorenson, P. G., *An Introduction to Data Structures with Applications,* 2.ª ed., McGraw-Hill, Auckland, 1984.
133. Witten, I. H., Frank, E. y Hall, M. A., *Data Mining: Practical Machine Learning Tools and Techniques,* 3.ª ed., Morgan Kaufmann, Ámsterdam, 2011.
134. R. Mustafovski, A. Petrovski y M. Radovanovic, «Integrating quantum technologies into mobile military systems and TOC frameworks»*, Land Forces Academy Review,* vol. XXX, n.º 3(119), 2025.
135. R. Mustafovski, «Marco arquitectónico basado en fórmulas de la plataforma SecuDroneComm para las comunicaciones de vehículos aéreos no tripulados», *Management Science Advances*, vol. 2, n.º 1, pp. 288-303, Scientific Oasis, Skopje, República de Macedonia del Norte, 2025.
136. R. Mustafovski, «Evaluación del impacto operativo de SecuDroneComm: evaluación basada en simulación de la comunicación segura de UAV en entornos militares», *Scientific Technical Review,* vol. 75, n.º 1, pp. 11-18, 2025, doi: 10.5937/str2500002M.

137. M. Mozaffari, W. Saad, M. Bennis y M. Debbah, «Despliegue eficiente de múltiples vehículos aéreos no tripulados para una cobertura inalámbrica óptima», *IEEE Communications Letters,* vol. 20, n.º 8, pp. 1647-1650, 2016.
138. L. Ruan et al., «Despliegue de cobertura multi-UAV energéticamente eficiente en redes UAV: un marco teórico de juego», *China Communications,* vol. 15, n.º 10, pp. 194209, 2018.
139. M. Mozaffari, W. Saad, M. Bennis y M. Debbah, «Vehículos aéreos no tripulados (UAV) móviles para comunicaciones de Internet de las cosas energéticamente eficientes», *IEEE Transactions on Wireless Communications*, 2017.
140. S.-Y Lien, K.-C. Chen y Y. Lin, «Hacia accesos masivos ubicuos en las comunicaciones máquina a máquina 3GPP», *IEEE Communications Magazine*, vol. 49, n.º 4, pp. 66-74, abril de 2011.
141. M. Malik y S. K. Garg, «Hacia el 6G: la evolución de las redes más allá del 5G y el escenario indio», en *Proc. 2.ª Conferencia Internacional sobre Prácticas Innovadoras en Tecnología y Gestión (ICIPTM)*, Gautam Buddha Nagar, India, pp. 123-127, 2022.
142. M. A. Khan et al., «Enjambre de UAV para la gestión de redes en 6G: una revisión técnica», *IEEE Transactions on Network and Service Management,* vol. 20, n.º 1, pp. 741-761, marzo de 2023.
143. S. Dang, O. Amin, B. Shihada y M.-S. Alouini, «¿Qué debería ser el 6G?», *Nature Electronics*, vol. 3, n.º 1, pp. 20-29, 2020.
144. F. Ronaldo, D. Pramadihanto y A. Sudarsono, «Sistema de comunicación seguro para servicios con drones mediante criptografía híbrida en redes 4G/LTE», en *Proc. Int. Electronics Symposium (IES),* Surabaya, Indonesia, pp. 116-122, 2020.
145. T. Li et al., «Comunicaciones seguras entre UAV y vehículos», *IEEE Transactions on Communications*, vol. 69, n.º 8, pp. 5381-5393, agosto de 2021.
146. S. A. Ayati y H. R. Naji, «Un mecanismo seguro para proteger las comunicaciones de los UAV», en *Proc. 9.º Congreso Conjunto Iraní sobre Sistemas Difusos e Inteligentes (CFIS),* Bam, Irán, pp. 1-6, 2022.
147. D. Pirker, T. Fischer, C. Lesjak y C. Steger, «Sistema de autenticación global y seguro para UAV basado en la seguridad del hardware», en *Proc. 8.ª Conferencia Internacional IEEE sobre Computación en la Nube Móvil, Servicios e Ingeniería (MobileCloud)*, Oxford, Reino Unido, pp. 84-89, 2020.
148. H. Wang, H. Fang y X. Wang, «Autenticación descentralizada suave habilitada por inteligencia periférica en enjambres de UAV», en *Proc. IEEE/CIC Int. Conf. Communications in China (ICCC)*, Xiamen, China, pp. 86-91, 2021.
149. M. Markowski, P. Ryba y K. Puchala, «Laboratorio de investigación de redes definidas por software: topologías y escenarios experimentales», en *Proc. 3.ª Conferencia Europea sobre Inteligencia de Redes (ENIC),* Breslavia, Polonia, pp.

252-256, 2016.
150. M. A. B. S. Abir, M. Z. Chowdhury y Y. M. Jang, «Redes de UAV definidas por software para sistemas 6G: requisitos, oportunidades, técnicas emergentes, retos y direcciones de investigación», *IEEE Open Journal of the Communications Society,* vol. 4, pp. 2487-2547, 2023.
151. M. Ouadah y F. Merazka, «Un enfoque de codificación de red para redes UAV fiables basadas en SDN», en *Proc. 5.ª Conferencia Internacional de Ingeniería Eléctrica y Aplicaciones de Control (ICEECA '22),* Khenchela, Argelia, 2022.

Biografía de Rexhep Mustafovski, MSc

Rexhep Mustafovski, MSc, es funcionario del Ministerio de Defensa de la República de Macedonia del Norte y asistente de docencia e investigación en la Academia Militar «General Mihailo Apostolski» de Skopje, donde trabaja en el Departamento de Ciberseguridad y Análisis Forense Digital. Es especialista en sistemas de comunicación seguros, ciberseguridad e integración de tecnología de defensa, con experiencia académica y profesional en comunicaciones tácticas seguras, seguridad de redes y sistemas de información emergentes.

Completó su educación universitaria en la Academia Militar «General Mihailo Apostolski» de Skopje, donde se graduó como oficial de transmisiones. Durante sus estudios, demostró un rendimiento académico y una disciplina profesional excepcionales, logrando el mayor éxito educativo de su generación. En reconocimiento a este logro, fue galardonado oficialmente como el mejor oficial de su generación, un honor que le fue conferido por el presidente del país. Esta distinción refleja tanto su excelencia académica como su compromiso con la profesionalidad militar.

Tras su nombramiento, continuó su desarrollo académico cursando estudios de posgrado en la Facultad de Ingeniería Eléctrica y Tecnologías de la Información de la Universidad «Ss. Cyril and Methodius» de Skopje. Obtuvo el título de Máster en Ciencias de la Comunicación y las Tecnologías de la Información, especializándose en sistemas de comunicación modernos, seguridad de la información y conceptos avanzados de redes. Sus estudios de máster reforzaron aún más sus capacidades analíticas y de investigación, especialmente en las áreas de comunicaciones seguras y sistemas de defensa basados en la tecnología.

Su trayectoria académica y profesional combina la educación militar formal con estudios avanzados de ingeniería, lo que le proporciona una base sólida para la investigación y el trabajo práctico en el ámbito de las comunicaciones militares seguras. Esta formación influye en su enfoque del diseño de sistemas de

comunicación, en el que destaca la fiabilidad, la seguridad, la interoperabilidad e e y la relevancia operativa. Los conocimientos y la experiencia adquiridos a través de la formación militar y la educación en ingeniería sustentan las perspectivas presentadas a lo largo de este libro.