Sistemas de comunicação seguros para operações militares modernas

Este livro oferece uma análise abrangente de sistemas de comunicação seguros para operações militares modernas, abordando os desafios tecnológicos e operacionais da troca de informações em campos de batalha contemporâneos e futuros. Traça a evolução das comunicações militares desde os sistemas analógicos e digitais até às arquitecturas encriptadas, definidas por software e melhoradas por IA, com ênfase na interoperabilidade da NATO, nas ameaças à cibersegurança e na guerra eletrónica. São analisados princípios fundamentais como a transmissão de sinais, a encriptação, a autenticação, as técnicas anti-bloqueio e as redes de rádio tácticas resilientes. Os tópicos avançados incluem comunicações seguras entre UAV e centro de comando, encaminhamento orientado por IA e gestão de espetro, sistemas de satélite, aplicações militares 5G/6G, comunicação quântica e redes de rádio cognitivas. O livro também propõe uma estrutura de comunicação segura orientada para o futuro integrada com sistemas C4ISR, apoiada por estudos de casos práticos, incluindo a investigação de doutoramento do autor. Destina-se a investigadores, profissionais militares, engenheiros e decisores políticos que procuram soluções de comunicação de defesa resilientes e inteligentes.

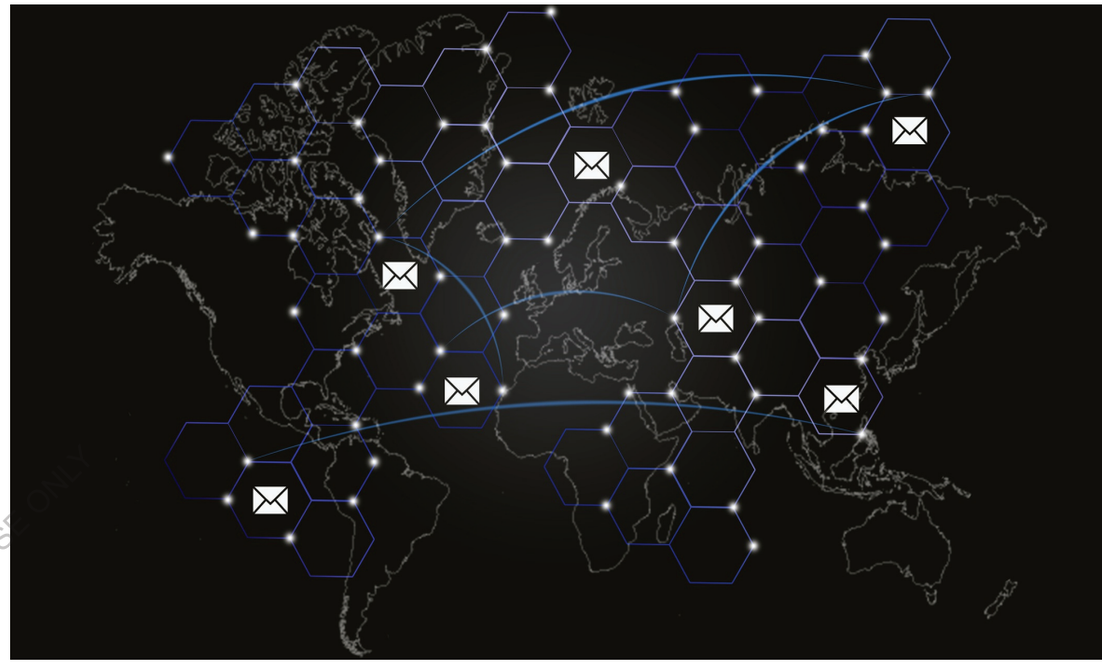
Rexhep Mustafovski, MSc, é um oficial de sinalização e investigador em comunicações militares. Tem um bacharelato da Academia Militar "General Mihailo Apostolski" em Skopje e um mestrado em Tecnologias da Comunicação e da Informação da Universidade "Ss. Cyril and Methodius".

9 786209 588365

EDIÇÕES
NOSSO CONHECIMENTO

Rexhep Mustafovski

EDIÇÕES
NOSSO CONHECIMENTO



Sistemas de comunicação seguros para operações militares modernas

Fundamentos, tecnologias e direcções futuras

Rexhep Mustafovski

Rexhep Mustafovski

Sistemas de comunicação seguros para operações militares modernas

Rexhep Mustafovski

Sistemas de comunicação seguros para operações militares modernas

Fundamentos, tecnologias e direcções futuras

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: 978-620-9-58836-5

Sistemas de comunicação seguros para operações militares modernas: fundamentos, tecnologias e direções futuras

Índice

Prefácio

Sou Rexhep Mustafovski, Mestre em Ciências, e este livro é o resultado do meu envolvimento académico, profissional e de investigação na área dos sistemas de comunicação modernos, com especial enfoque em aplicações seguras para fins militares e de defesa. A motivação para escrever este livro surge da crescente importância das tecnologias avançadas na formação da sociedade contemporânea e, mais especificamente, na transformação da forma como as forças militares comunicam, coordenam e operam em ambientes complexos e disputados.

No mundo moderno, a tecnologia já não é um elemento periférico da atividade humana, mas um motor central de mudança nos domínios económico, social e de segurança. As tecnologias de comunicação, em particular, tornaram-se fundamentais para a forma como a informação é gerada, transmitida, protegida e explorada. Em contextos militares, a comunicação segura não é apenas um requisito técnico, mas uma necessidade estratégica. A capacidade de trocar informações de forma segura, fiável e em tempo real influencia diretamente a eficácia operacional, a tomada de decisões e a proteção das forças. Este livro foi escrito com a intenção de apresentar estas realidades a um público académico e profissional mais vasto, fazendo a ponte entre os fundamentos teóricos e as aplicações militares práticas.

A minha formação académica em tecnologias de comunicação e informação, combinada com o meu envolvimento profissional na educação e investigação militar, moldou a perspetiva adotada neste trabalho. Ao longo dos meus estudos e atividades de investigação, observei uma lacuna recorrente entre as tecnologias de comunicação em rápido avanço e a sua integração estruturada ao nível do sistema dentro das estruturas militares. Embora muitos trabalhos se concentrem em tecnologias isoladas ou soluções técnicas específicas, poucos tentam apresentar uma visão abrangente e integrada dos sistemas de comunicação militar segura como arquiteturas em evolução. Este livro procura colmatar essa lacuna, oferecendo uma análise coerente e estruturada das tecnologias, mecanismos de segurança e princípios arquitetónicos que sustentam as comunicações militares modernas e futuras.

O livro também é baseado na minha pesquisa de doutorado em andamento, que se concentra em estruturas de comunicação seguras e plataformas de comunicação avançadas para aplicações de defesa. Uma parte dessa pesquisa foi incorporada ao livro na forma de um estudo de caso dedicado, que apresenta um exemplo prático de como conceitos teóricos e princípios arquitetónicos podem ser aplicados a um sistema real. Este estudo de caso, derivado do meu trabalho de doutoramento, foi incluído para demonstrar a transição da análise conceitual para o design e a implementação do sistema. O seu objetivo não é fornecer uma solução finalizada,

mas sim ilustrar como as plataformas de comunicação seguras podem ser estruturadas para atender aos requisitos operacionais , tais como segurança, confiabilidade, latência e interoperabilidade.

Ao escrever este livro, procurei manter um equilíbrio entre o rigor académico e a relevância prática. O conteúdo baseia-se em princípios estabelecidos de engenharia de comunicação, cibersegurança e sistemas militares, ao mesmo tempo que reflete as tendências tecnológicas atuais, tais como inteligência artificial, rádios definidos por software, sistemas não tripulados, comunicação por satélite e mecanismos de segurança emergentes. A intenção não era produzir um texto puramente teórico, nem um manual estritamente técnico, mas sim um trabalho académico estruturado que pudesse servir de referência para estudantes, investigadores, engenheiros e profissionais militares interessados na conceção e evolução de sistemas de comunicação seguros.

O público-alvo deste livro é, portanto, intencionalmente amplo, abrangendo estudantes de graduação e pós-graduação em engenharia e disciplinas relacionadas à defesa, pesquisadores que trabalham nas áreas de comunicação e segurança e profissionais envolvidos no planejamento de comunicações militares, desenvolvimento de sistemas e implantação operacional. Ao mesmo tempo, o livro foi escrito com profundidade e foco analítico suficientes para apoiar estudos acadêmicos avançados e contribuir para as discussões em andamento na comunidade de pesquisa.

Por fim, este livro representa um passo numa longa jornada académica e profissional. Reflete tanto pesquisas concluídas quanto investigações em andamento, reconhecendo que o campo das comunicações militares é dinâmico e está em constante evolução. As tecnologias, arquiteturas e estruturas discutidas neste trabalho, sem dúvida, continuarão a se desenvolver em resposta a novos requisitos operacionais e ameaças emergentes. Espero que este livro contribua para uma compreensão mais profunda dos sistemas de comunicação seguros e incentive mais pesquisas, discussões e inovações neste domínio crítico.

Introdução

Os sistemas de comunicação militar sempre desempenharam um papel decisivo na condução da guerra, moldando a forma como as forças coordenam, decidem e agem em ambientes operacionais. Desde as primeiras formas de sinalização no campo de batalha até às arquiteturas globais em rede e orientadas por dados da atualidade, a comunicação continua a ser um facilitador central do comando, controlo e eficácia operacional. Nas operações militares contemporâneas, no entanto, os sistemas de comunicação evoluíram para além do seu papel tradicional de apoio e constituem agora uma capacidade estratégica por direito próprio. Infraestruturas de comunicação seguras, resilientes e adaptáveis são fundamentais para alcançar a superioridade da informação, manter o ritmo operacional e garantir a sobrevivência das forças em ambientes cada vez mais complexos e disputados.

A transformação da guerra no século XXI introduziu novos desafios que alteram fundamentalmente os requisitos impostos aos sistemas de comunicação militar. As operações modernas são caracterizadas por alta mobilidade, envolvimento em vários domínios e integração de atividades convencionais, cibernéticas e de guerra de informação. As forças operam nos domínios terrestre, aéreo, marítimo, espacial e cibernético, muitas vezes simultaneamente e em coordenação com parceiros conjuntos e de coalizão. Em tais condições, a capacidade de trocar informações precisas, oportunas e protegidas determina não apenas o sucesso tático, mas também os resultados estratégicos. Os sistemas de comunicação devem, portanto, funcionar de forma confiável em condições de incerteza, interrupção e interferência adversária ativa.

Uma das características definidoras das comunicações militares modernas é a centralidade da segurança. À medida que as redes de comunicação se tornam mais interligadas e orientadas por software, ficam cada vez mais expostas a ciberataques, guerra eletrónica e exploração por parte de adversários. A confidencialidade, integridade, disponibilidade e autenticidade das informações não são mais conceitos técnicos abstratos, mas necessidades operacionais. Sistemas de comunicação comprometidos podem levar à desinformação, perda de autoridade de comando, falha na missão ou escalada indesejada. Consequentemente, as considerações de segurança devem ser incorporadas em todos os níveis do projeto do sistema de comunicação, desde mecanismos de transmissão física até arquiteturas de rede e serviços no nível do aplicativo.

Ao mesmo tempo, a inovação tecnológica está a acelerar a um ritmo sem precedentes. Os avanços nas comunicações digitais, criptografia, inteligência artificial, sistemas de satélite e tecnologias emergentes, como a comunicação quântica, estão a remodelar rapidamente o panorama das comunicações militares.

Esses desenvolvimentos oferecem oportunidades significativas para melhorar o desempenho, a resiliência e a adaptabilidade, mas também introduzem novas vulnerabilidades e complexidades. As instituições militares devem, portanto, equilibrar a adoção de tecnologias avançadas com um projeto arquitetónico rigoroso, disciplina operacional e responsabilidade ética.

Este livro é motivado pela necessidade de fornecer uma análise abrangente e integrada dos sistemas de comunicação militar seguros no contexto das operações de defesa modernas e futuras. Em vez de se concentrar em tecnologias isoladas ou problemas técnicos específicos, o livro adota uma perspetiva ao nível do sistema que considera a comunicação como uma estrutura interligada envolvendo hardware, software, mecanismos de segurança, doutrina operacional e tomada de decisões humanas. O objetivo é apresentar uma compreensão coerente de como os sistemas de comunicação seguros são projetados, implementados e desenvolvidos para atender às exigências da guerra contemporânea.

Os capítulos iniciais estabelecem o contexto fundamental para a discussão. As comunicações militares modernas são examinadas através da sua evolução histórica, desde sistemas analógicos e ponto a ponto até arquiteturas digitais, criptografadas e em rede. Esta evolução reflete mudanças mais amplas na doutrina militar, no ritmo operacional e nos requisitos de informação. A importância das comunicações seguras é destacada não só em termos de proteção da informação, mas também na viabilização de ações militares coordenadas e legais. O papel da normalização, particularmente no âmbito das alianças, é enfatizado como um fator crítico para garantir a interoperabilidade e a coesão operacional entre as forças aliadas.

O livro explora então os princípios fundamentais subjacentes aos sistemas de comunicação segura. A transmissão de sinais, a propagação e os desafios associados à comunicação com e sem linha de visão são examinados para estabelecer uma base técnica. Estes princípios continuam a ser relevantes, apesar dos avanços tecnológicos, uma vez que as restrições físicas e os fatores ambientais continuam a moldar o desempenho das comunicações. Com base nesta fundação, o livro analisa mecanismos de segurança essenciais, tais como encriptação, autenticação, controlo de acesso e técnicas anti-interferência. Estes elementos formam a espinha dorsal das arquiteturas de comunicação seguras e são essenciais para manter a fiabilidade e a confiança em ambientes contestados.

A cibersegurança surge como um tema central nos capítulos seguintes. As redes de comunicação militar são cada vez mais alvo de ameaças cibernéticas sofisticadas que procuram interromper operações, extrair informações confidenciais ou manipular processos de tomada de decisão. O livro examina a natureza dessas ameaças e as estratégias utilizadas para mitigá-las, incluindo o reforço da rede, a

seleção de protocolos criptográficos, arquiteturas de confiança zero e mecanismos de resposta a incidentes. Ao abordar a cibersegurança tanto a nível técnico como arquitetónico, o livro enfatiza a importância da resiliência e da adaptabilidade face a ameaças persistentes e em evolução.

Os sistemas de comunicação por rádio continuam a ser uma pedra angular das operações táticas, e o seu papel é examinado em profundidade. Os sistemas tradicionais de VHF, UHF e HF continuam a fornecer capacidades essenciais, particularmente em ambientes onde a infraestrutura é limitada ou degradada. A integração desses sistemas com rádios definidos por software e técnicas de rede em malha ilustra como as tecnologias legadas podem ser aprimoradas por meio de abordagens arquitetónicas modernas. A interoperabilidade com as forças aliadas é tratada como um requisito fundamental, refletindo as realidades das operações conjuntas e de coalizão em cenários de conflito contemporâneos.

O uso crescente de sistemas aéreos não tripulados introduz novas dimensões nas comunicações militares. Os UAVs servem como coletores de dados, retransmissores de comunicação e plataformas operacionais que ampliam o alcance e a flexibilidade das redes militares. O livro analisa os desafios de segurança associados à comunicação entre UAVs e centros de comando, incluindo criptografia, autenticação, proteção da camada de enlace e restrições de desempenho, como latência e confiabilidade. Um estudo de caso dedicado apresenta uma plataforma de comunicação segura integrada, ilustrando como os conceitos teóricos podem ser aplicados na prática para atender aos requisitos operacionais do mundo real.

A inteligência artificial representa uma força transformadora nos sistemas de comunicação militar. O livro explora como as técnicas de IA podem melhorar a eficiência do roteamento, a deteção de intrusões, a alocação de espectro e o gerenciamento de rede em ambientes de campo de batalha. Ao permitir que os sistemas detectem, aprendam e se adaptem, as arquiteturas de comunicação impulsionadas por IA oferecem novos níveis de resiliência e eficiência operacional. Ao mesmo tempo, a integração da IA levanta questões importantes relacionadas à transparência, responsabilidade e controle, que são abordadas por meio de uma análise equilibrada e crítica.

As tecnologias emergentes constituem outro ponto central do livro. As redes celulares de próxima geração, a comunicação por satélite, a distribuição de chaves quânticas e as redes de rádio cognitivas são examinadas como facilitadoras das futuras capacidades de comunicação militar. Estas tecnologias expandem o envelope operacional, suportando taxas de dados mais elevadas, conectividade global, segurança reforçada e utilização inteligente do espectro. A sua integração nos sistemas militares reflete uma mudança para uma arquitetura híbrida que

combina componentes terrestres, aéreos, marítimos e espaciais numa estrutura de comunicação unificada.

Os capítulos finais sintetizam estes desenvolvimentos tecnológicos e conceptuais numa discussão mais ampla sobre como estruturas de comunicação seguras podem ser construídas para o exército do futuro. Os requisitos para as forças modernas são analisados em termos de resiliência, interoperabilidade, escalabilidade e segurança. Princípios arquitetónicos são apresentados para ilustrar como sistemas de comunicação tática seguros podem ser projetados para suportar operações complexas e distribuídas. A integração com sistemas C4ISR é enfatizada como um fator crítico para alcançar consciência situacional e superioridade de decisão. Considerações éticas e legais são abordadas para garantir que a inovação tecnológica esteja alinhada com as normas e responsabilidades estabelecidas. A discussão sobre as tendências futuras oferece uma perspectiva voltada para o futuro sobre como os sistemas de comunicação militar provavelmente evoluirão em resposta às ameaças emergentes e às oportunidades tecnológicas.

O público-alvo deste livro inclui profissionais militares, engenheiros de defesa, investigadores e estudantes de pós-graduação envolvidos no estudo e desenvolvimento de sistemas de comunicação seguros. O livro também é relevante para formuladores de políticas e tomadores de decisão envolvidos no planejamento de defesa e desenvolvimento de capacidades. Ao combinar análise técnica com perspectivas arquitetónicas e operacionais, o livro busca preencher a lacuna entre a teoria e a prática nas comunicações militares.

Este livro visa contribuir para a compreensão e o desenvolvimento de sistemas de comunicação militar seguros, apresentando uma perspetiva integrada e orientada para o futuro. À medida que a guerra continua a evoluir em complexidade e alcance, a capacidade de comunicar de forma segura, fiável e inteligente continuará a ser um fator decisivo na eficácia militar. Através da sua análise abrangente de tecnologias, arquitetura e princípios, este trabalho procura fornecer uma base para a construção de sistemas de comunicação que apoiem o sucesso operacional, mantendo a segurança, a resiliência e a responsabilidade nas operações militares modernas e futuras.

Conclusão

Este livro examinou a evolução, a estrutura e a direção futura dos sistemas de comunicação militar segura no contexto das operações de defesa modernas e emergentes. Ao longo dos seus capítulos, o trabalho demonstrou que as comunicações militares já não são meramente tecnologias de apoio, mas constituem um pilar central da eficácia operacional, da tomada de decisões estratégicas e da superioridade da informação. A crescente complexidade do ambiente de segurança, combinada com o rápido avanço tecnológico, requer estruturas de comunicação resilientes, inteligentes, interoperáveis e com base ética.

Os primeiros capítulos estabeleceram a importância fundamental das comunicações seguras nas operações militares. As forças armadas modernas operam em condições de incerteza, mobilidade e ameaça persistente, onde a capacidade de trocar informações precisas e oportunas determina o sucesso ou o fracasso da missão. A transição de sistemas analógicos e isolados para arquiteturas de comunicação digitais, criptografadas e em rede reflete uma mudança mais ampla em direção à guerra centrada na informação. Essa evolução transformou os sistemas de comunicação em facilitadores ativos do comando, controle e coordenação em todos os domínios de operação.

Um tema central ao longo do livro tem sido a relação inseparável entre comunicação e segurança. À medida que as redes militares se tornam mais interligadas e orientadas por software, ficam cada vez mais expostas a ameaças cibernéticas, guerra eletrónica e exploração adversária. A análise da encriptação, autenticação, controlo de acesso e reforço da rede destacou a necessidade de incorporar mecanismos de segurança em todas as camadas das arquiteturas de comunicação. Em vez de tratar a segurança como um complemento, os sistemas militares modernos devem adotar uma abordagem de segurança desde a conceção que garanta a confidencialidade, integridade, autenticidade e disponibilidade em condições contestadas.

A discussão sobre sistemas de comunicação por rádio para unidades táticas demonstrou que as tecnologias legadas continuam a ser operacionalmente relevantes quando integradas na arquitetura moderna. Os sistemas VHF, UHF e HF continuam a fornecer capacidades de comunicação robustas, particularmente em ambientes degradados ou negados. Quando combinadas com rádios definidos por software e princípios de redes em malha, estas tecnologias oferecem flexibilidade e resiliência essenciais para operações táticas. A capacidade de adaptar formas de onda, frequências e estratégias de encaminhamento permite que as forças mantenham a conectividade apesar da mobilidade, das restrições do terreno e da interferência hostil.

Os sistemas aéreos não tripulados e a sua integração em estruturas de comunicação seguras foram examinados como uma característica definidora das operações militares contemporâneas. Os UAVs funcionam não só como plataformas de deteção, mas também como nós de comunicação dinâmicos e e es que ampliam o alcance da rede e melhoram a consciência situacional. A análise da comunicação entre o UAV e o centro de comando enfatizou a importância da criptografia, autenticação, segurança da camada de enlace e otimização do desempenho. O estudo de caso apresentado ilustrou como uma plataforma de comunicação integrada e segura pode dar suporte à troca de dados em tempo real, ao mesmo tempo em que lida com as restrições de latência, confiabilidade e rendimento em ambientes operacionais.

A inteligência artificial surgiu como uma força transformadora nos sistemas de comunicação militar. A exploração do roteamento orientado por IA, deteção de intrusão, alocação de espectro e redes de campo de batalha demonstrou como algoritmos inteligentes podem aumentar a adaptabilidade e a resiliência. A IA permite que os sistemas de comunicação respondam dinamicamente a mudanças ambientais e ações adversas, reduzindo a carga cognitiva sobre os operadores humanos e melhorando o ritmo operacional. Ao mesmo tempo, a integração da IA levanta questões importantes relacionadas à transparência, responsabilidade e controle, reforçando a necessidade de uma implementação responsável e bem governada.

Tecnologias emergentes, como redes celulares de última geração, comunicação por satélite, distribuição de chaves quânticas e redes de rádio cognitivas, foram analisadas como facilitadoras das futuras capacidades de comunicação militar. Estas tecnologias expandem o envelope operacional, suportando taxas de dados mais elevadas, conectividade global, segurança reforçada e utilização inteligente do espectro. A sua integração nos sistemas militares reflete uma mudança para arquiteturas híbridas que combinam componentes terrestres, aéreos, marítimos e espaciais. Esta convergência permite operações multidomínio, ao mesmo tempo que introduz novos desafios arquitetónicos e de segurança que devem ser abordados de forma holística.

Os capítulos finais centraram-se na construção de uma estrutura de comunicação segura para o exército do futuro. A análise enfatizou que o avanço tecnológico por si só é insuficiente sem um projeto arquitetónico coerente, integração com sistemas C4ISR e consideração das implicações éticas e legais. As futuras estruturas de comunicação devem apoiar a interoperabilidade, a escalabilidade e a resiliência, mantendo a conformidade com o direito internacional e os princípios éticos. A inclusão de considerações de governança, responsabilidade e sustentabilidade garante que os sistemas de comunicação contribuam para a segurança e a

estabilidade a longo prazo, em vez de apenas para vantagens táticas a curto prazo.

Uma conclusão importante deste trabalho é que os futuros sistemas de comunicação militar devem ser ecossistemas adaptáveis, em vez de infraestruturas estáticas. A natureza dinâmica dos conflitos modernos exige sistemas que possam ser reconfigurados em resposta às mudanças nos requisitos da missão, nas condições ambientais e nos vetores de ameaça. Essa adaptabilidade requer uma integração estreita entre tecnologias de comunicação, mecanismos de segurança, sistemas de controlo inteligentes e tomadores de decisão humanos. O sucesso e e de tais sistemas depende não apenas da excelência técnica, mas também do alinhamento doutrinário e da prontidão organizacional.

Outra conclusão importante é a crescente importância da interoperabilidade e das operações de coalizão. As missões militares modernas são cada vez mais conduzidas em contextos multinacionais, exigindo sistemas de comunicação que permitam o compartilhamento controlado de informações, preservando os interesses de segurança nacional. Padronização, estruturas de segurança compartilhadas e mecanismos flexíveis de controle de acesso são essenciais para uma colaboração eficaz. Arquiteturas de comunicação que suportam a interoperabilidade por design fornecem uma base para a confiança e a coerência operacional entre as forças aliadas.

As dimensões éticas e jurídicas da tecnologia de comunicação militar representam uma área crítica de responsabilidade para designers, operadores e decisores políticos. À medida que os sistemas de comunicação se tornam mais autónomos e integrados com funções de apoio à decisão, as consequências potenciais de falhas ou uso indevido do sistema aumentam. Incorporar considerações éticas e conformidade jurídica no design do sistema garante que a superioridade tecnológica não comprometa a legitimidade ou a responsabilidade. A inovação responsável nas comunicações militares deve equilibrar a eficácia operacional com a adesão às normas e valores estabelecidos.

Este livro contribui para o campo ao fornecer uma perspetiva abrangente e integrada sobre sistemas de comunicação militar seguros. Em vez de se concentrar em tecnologias isoladas, ele enfatiza a coerência arquitetónica, a integração da segurança e o design orientado para o futuro. A combinação de análise teórica, considerações práticas e exame de estudos de caso oferece uma estrutura para compreender e desenvolver infraestruturas modernas de comunicação militar.

Do ponto de vista académico, este trabalho fornece uma base para pesquisas adicionais sobre arquiteturas de comunicação adaptativas, gestão de redes impulsionada por IA e sistemas quânticos seguros. Do ponto de vista operacional, oferece insights sobre os desafios e oportunidades associados à implantação de

tecnologias de comunicação seguras em ambientes complexos. Os conceitos apresentados podem informar o desenvolvimento de doutrinas, o design de sistemas e a formulação de políticas em instituições de defesa.

Em conclusão, os sistemas de comunicação militar seguros são um fator decisivo na guerra moderna e futura. À medida que as forças armadas enfrentam ambientes operacionais cada vez mais complexos e disputados, a capacidade de trocar informações de forma segura, fiável e inteligente continuará a ser um imperativo estratégico. Ao adotar estruturas de comunicação integradas, adaptativas e baseadas na ética, os exércitos do futuro poderão alcançar a superioridade da informação, mantendo a resiliência, a legitimidade e a eficácia operacional. Este livro visa contribuir para esse objetivo, oferecendo uma análise estruturada e voltada para o futuro das tecnologias, arquiteturas e princípios es que moldarão o futuro das comunicações militares.

Referências

1. Defence Strategic Communications, *Jornal Oficial do Centro de Excelência em Comunicações Estratégicas da OTAN,* Vol. 10, Primavera-Outono 2021, NATO StratCom COE, Riga, Letónia.
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., "O uso de plataformas de comunicação em operações militares: aumentando a eficácia estratégica e tática", *Database Systems Journal,* vol. XVI, 2025, Faculdade de Engenharia Elétrica e Tecnologias da Informação, Universidade Ss. Cyril e Methodius, Skopje, República da Macedónia do Norte.
4. Rienzi, T. M., *Comunicações-Eletrónica 1962-1970,* Série de Estudos sobre o Vietname, Departamento do Exército, Washington, DC, EUA, 2002.
5. Mazzenga, F., Landry, R. e Young, K., «Comunicações Militares», *IEEE Communications Magazine,* outubro de 2020, pp. 50-56.
6. Organização do Tratado do Atlântico Norte (OTAN), *Doutrina Conjunta Aliada para Sistemas de Comunicação e Informação (AJP-6),* Edição B, Versão 1, Gabinete de Normalização da OTAN (NSO), abril de 2024.
7. Departamento de Defesa dos Estados Unidos, *Estratégia de Modernização C3: Comando, Controlo e Comunicações,* Washington, DC, EUA, setembro de 2020.
8. Monteiro Marques, M., «STANAG 4586 - Interfaces Padrão do Sistema de Controlo de UAV (UCS) para Interoperabilidade de UAV da OTAN», Documento Técnico da OTAN, Escola Naval - Afeite, Portugal.
9. Yarnell, A. M., Dullea, C. e Grunberg, N. E., «Comunicação Militar», em *Comunicação Militar e Médica,* Capítulo 11, Comando de Investigação e Desenvolvimento Médico do Exército dos EUA, EUA.
10. Timofte, G., «Modernização dos Sistemas de Comunicações Militares de acordo com os Novos Requisitos Operacionais, Informativos e Técnicos do Espaço de Batalha», *Boletim Científico da Academia de Cientistas Romenos,* Bucareste, Roménia.
11. Hayes, C., *Acordos de Normalização da OTAN (STANAG) para Comandantes e Estado-Maior,* Notícias da Frente, Centro de Lições Aprendidas do Exército (CALL), Exército dos EUA, abril de 2019.
12. Sánchez, R., Evans, J. e Minden, G., "Networking on the Battlefield: Challenges in Highly Dynamic Multi-hop Wireless Networks" (Redes no campo de batalha: desafios em redes sem fios multissaltos altamente dinâmicas)*, Anais da IEEE MILCOM 1999,* Atlantic City, Nova Jérsia, EUA, outubro de 1999.

13. Kumar, D., “Challenges of a Digitised Battlefield” (Desafios de um campo de batalha digitalizado)*, Journal of the United Service Institution of India,* vol. CXLII, n.º 590, outubro-dezembro de 2012.
14. Lipscomb, P., “The Evolution of Communications in the Military as it Relates to Leadership” (A evolução das comunicações nas forças armadas no que se refere à liderança)*, Estudos Integrados*, Artigo n.º 90, Murray State University, 2017. Disponível em: https://digitalcommons.murraystate.edu/bis437/90
15. Amin, M. G., Lindsey, A. R., Zhao, L., e Zhang, Y., *Anti-Jamming Techniques for GPS Receivers,* Relatório Técnico Final AFRL-IF-RS-TR-2001-186, Laboratório de Investigação da Força Aérea, Centro de Investigação de Roma, Nova Iorque, EUA, setembro de 2001.
16. Bardis, N. G., Doukas, N., e Ntaikos, K., “Design and Development of a Secure Military Communication Based on AES Prototype Crypto Algorithm and Advanced Key Management Scheme,” *WSEAS Transactions on Information Science and Applications,* Universidade de Educação Militar, Academia do Exército Helénico, Grécia.
17. Colbeck, M. J. L., “Criptografia quântica em comunicações militares”, *Anais da Conferência da EAAW,* 28-29 de novembro de 2023.
18. Evans, J., Sánchez, R. e Minden, G., “Redes no campo de batalha: desafios em redes sem fios multissaltos altamente dinâmicas”, *Anais da IEEEMILCOM,* Atlantic City, Nova Jérsia, EUA, outubro de 1999.
19. Hayes, C., “Acordos de Normalização da OTAN (STANAG) para Comandantes e Estado-Maior”, *Notícias da Frente,* Centro de Lições Aprendidas do Exército (CALL), abril de 2019.
20. Kang, J. S., “Protocolo de autenticação independente em ambiente de rede tática usando abordagem de bloqueio de hash”, *International Journal of Machine Learning and Computing,* vol. 5, n.º 5, outubro de 2015.
21. Kovács, L., “Guerra Eletrónica e os Desafios Assimétricos”, *Bolyai Szemle,* n.º 3, 2009, pp. 135-151, ISSN 1416-1443.
22. Kumar, D., “Challenges of a Digitised Battlefield” (Desafios de um campo de batalha digitalizado)*, Journal of the United Service Institution of India,* vol. CXLII, n.º 590, outubro-dezembro de 2012.
23. Lipscomb, P., “The Evolution of Communications in the Military as it Relates to Leadership” (A evolução das comunicações nas forças armadas no que se refere à liderança)*, Integrated Studies*, n.º 90, Murray State University, 2017.
24. Sayyed, S. Y., Gurap, S. L., Devadhe, J. L., e Gat, K. R., “Uma revisão sobre comunicações sem fios seguras para aplicações militares”, *Revista Internacional de Eletricidade, Eletrónica e Comunicação de Dados,* vol. 5, n.º 11, novembro de 2017.
25. Shinde, V., Kulkarni, S., e Malekar, M. R., “Sistema de Comunicação

Segura", *Revista Internacional de Inovações em Pesquisa e Tecnologia de Engenharia (IJIERT),* Anais da Conferência TECHNO-2K17.
26. Timofte, G., "Modernização dos sistemas de comunicações militares de acordo com os novos requisitos operacionais, informativos e técnicos do espaço de batalha da Força Aérea dos Estados Unidos ( )", Academia de Cientistas Romenos, Bucareste, Roménia.
27. Departamento do Exército dos Estados Unidos, *Doutrina de Comunicações de Sinais (FM 100-11),* Departamento do Exército, Washington, DC, julho de 1948.
28. Alnifie, G., e Simon, R., "Uma defesa multicanal contra ataques de interferência em redes de sensores sem fios", em *Anais do 3.º Workshop ACM sobre QoS e Segurança para Redes Sem Fios e Móveis,* 2007, pp. 95-104.
29. Alnifie, G., e Simon, R., "MULEPRO: Uma resposta multicanal a ataques de interferência em redes de sensores sem fios", *Wireless Communications and Mobile Computing,* 2010.
30. Bayraktaroglu, E., King, C., Liu, X., Noubir, G., Rajaraman, R., e Thapa, B., "Sobre o desempenho do IEEE 802.11 sob interferência", em *Anais da 27ª Conferência IEEE sobre Comunicações Informáticas,* 2008, pp. 1265-1273.
31. Bellardo, J., e Savage, S., "Ataques de negação de serviço 802.11: vulnerabilidades reais e soluções práticas", em *Anais do 12º Simpósio de Segurança USENIX,* 2003, pp. 15-28.
32. Broustis, I., Pelechrinis, K., Syrivelis, D., Krishnamurthy, S. V., e Tassiulas, L., "FIJI: Combate ao Jamming Implícito em WLANs 802.11", *Segurança e Privacidade em Redes de Comunicação,* Vol. 19, 2009, pp. 21-40.
33. Chiang, J. T., e Hu, Y. C., "Detecção e mitigação de interferência entre camadas em redes de transmissão sem fios", *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., e Zrazhevsky, G., "Interferência em redes de comunicação sob incerteza total", *Optimization Letters*, vol. 2, n.º 1, 2008, pp. 53-70.
35. Gencer, C., Aydogan, E. K., e Celik, C., "Um sistema de apoio à decisão para localizar sistemas de interferência de rádio VHF/UHF no terreno", *Information Systems Frontiers,* vol. 10, n.º 1, 2008, pp. 111-124.
36. Gummadi, R., Wetherall, D., Greenstein, B., e Seshan, S., "Compreendendo e Mitigando o Impacto da Interferência de RF em Redes 802.11", em *Anais da Conferência ACM SIGCOMM sobre Aplicações, Tecnologias, Arquiteturas e Protocolos para Comunicações Informáticas,* 2007, pp. 385-396.
37. Huang, H., Ahmed, N., e Pulluru, S., "Sobre ataques de interferência estratégicos e aleatórios de alcance limitado em redes ad hoc sem fios", em *Anais da 34ª Conferência IEEE sobre Redes Locais de Computadores*, 2010, pp. 1-8.
38. Jain, S. K., e Garg, K., "Um modelo híbrido de técnicas de defesa contra

ataques de interferência em estações base em redes de sensores sem fios", em *Anais da Primeira Conferência Internacional sobre Inteligência Computacional, Sistemas de Comunicação e Redes*, 2009, pp. 102-107.

39. Kerkez, B., Watteyne, T., Magliocco, M., Glaser, S., e Pister, K., "Análise de viabilidade do projeto de controlador para salto de canal adaptativo", em *Anais da Quarta Conferência Internacional ICST sobre Metodologias e Ferramentas de Avaliação de Desempenho*, 2009, pp. 76:1-76:6.

40. Khattab, S., Mosse, D., e Melhem, R., "Mitigação de interferência em redes sem fios multirádio: reativa ou proativa?", em *Anais da 4ª Conferência Internacional sobre Segurança e Privacidade em Redes de Comunicação,* 2008, pp. 27:1-27:10.

41. Khattab, S., Mosse, D., e Melhem, R., "Modelagem da defesa anti-interferência com salto de canal em redes sem fio multirádio", em *Anais da 5ª Conferência Internacional Anual sobre Sistemas Móveis e Ubíquos: Computação, Redes e Serviços,* 2008, pp. 25:1-25:10.

42. Lazos, L., Liu, S., e Krunz, M., "Mitigação de ataques de interferência no canal de controlo em redes ad hoc multicanais", em *Anais da 2ª Conferência ACM sobre Segurança de Redes Sem Fios,* 2009, pp. 169-180.

43. Li, M., Koutsopoulos, I., e Poovendran, R., "Ataques de interferência ótimos e políticas de defesa de rede em redes de sensores sem fios", em *Anais da 26ª Conferência Internacional IEEE sobre Comunicações Informáticas,* 2007, pp. 1307-1315.

44. Liu, H., Liu, Z., Chen, Y., e Xu, W., "Determining the Position of a Jammer Using a Virtual-Force Iterative Approach" (Determinação da posição de um interferidor usando uma abordagem iterativa de força virtual)*, Wireless Networks,* vol. 17, n.º 2, 2011, pp. 531-547.

45. Liu, Z., Liu, H., Xu, W. e Chen, Y., "Explorando alterações nas proximidades causadas por interferência para localização de interferentes", *IEEE Transactions on Parallel and Distributed Systems,* 2011.

46. Misra, S., Singh, R. e Mohan, S. V. R., "Mecanismo de deteção de ataques de interferência dignos de guerra de informação para redes de sensores sem fios utilizando um sistema de inferência difusa"*, Sensors,* vol. 10, 2010, pp. 3444-3479.

47. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., e Pantziou, G., "Um estudo sobre ataques de interferência e contramedidas em redes de sensores sem fios", *IEEE Communications Surveys and Tutorials*, vol. 11, n.º 4, 2009, pp. 42-56.

48. Muraleedharan, R., e Osadciw, L. A., "Detecção e contramedidas contra ataques de interferência em redes de sensores sem fios utilizando o sistema Ant", em *Proceedings of SPIE - The International Society for Optical Engineering,* Vol. 6248, 2006, Artigo 62480G.

49. Navda, V, Bohra, A., Ganguly, S., e Rubenstein, D., "Utilização de salto de

canal para aumentar a resiliência 802.11 a ataques de interferência", em *Anais da 26ª Conferência Internacional IEEE sobre Comunicações Informáticas*, 2007, pp. 2526-2530.

50. Panyim, K., Hayajneh, T., Krishnamurthy, P., e Tipper, D., "Jamming Dust: A Low Power Distributed Jammer Network" (Interferência de poeira: uma rede de interferência distribuída de baixa potência), em *Anais da 27ª Conferência Científica do Exército dos EUA (*), 2009, pp. 922-929.

51. Pelechrinis, K., Koufogiannakis, C., e Krishnamurthy, S. V., "Gaming the Jammer: Is Frequency Hopping Effective?" em *Anais da 7ª Conferência Internacional sobre Modelagem e Otimização em Redes Móveis, AdHoc e Sem Fio,* 2009, pp. 187-196.

52. Pelechrinis, K., Koutsopoulos, I., Broustis, I., e Krishnamurthy, S. V., "Localização leve de interferentes em redes sem fios: projeto e implementação do sistema", em *Anais da Conferência Global de Telecomunicações do IEEE,* 2009, pp. 1-6.

53. Pelechrinis, K., Iliofotou, M., e Krishnamurthy, S. V., "Ataques de negação de serviço em redes sem fios: o caso dos interferentes", *IEEE Communications Surveys and Tutorials,* vol. 13, n.º 2, 2011, pp. 245-257.

54. Shin, I., Shen, Y., Xuan, Y., Thai, M. T., e Znati, T., «Ataques de interferência reativa em redes de sensores sem fios multirádio: uma medida de mitigação eficiente através da identificação de nós desencadeadores», em *Proceedings of the 2nd ACM International Workshop on Foundations of Wireless Ad Hoc and Sensor Networking and Computing,* 2009, pp. 87-96.

55. Strasser, M., Danev, B., e Capkun, S., "Detecção de interferência reativa em redes de sensores", *ACM Transactions on Sensor Networks*, vol. 7, n.º 2, 2010, artigo 16.

56. Sun, Y., e Wang, X., "Localização de Interferência em Redes de Sensores Sem Fios", em *Anais da 5ª Conferência Internacional sobre Comunicações Sem Fios, Redes e Computação Móvel,* 2009, pp. 1-4.

57. Tague, P., Slater, D., Poovendran, R., e Noubir, G., "Linear Programming Models for Jamming Attacks on Network Traffic Flows" (Modelos de programação linear para ataques de interferência em fluxos de tráfego de rede), *em Proceedings of the 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops (Anais do 6º Simpósio Internacional sobre Modelagem e Otimização em Redes Móveis, Ad Hoc e Sem Fio e Workshops)*, 2008, pp. 207-216.

58. Thamilarasu, G., e Sridhar, R., "Modelagem Teórica de Jogos de Ataques de Interferência em Redes Ad Hoc", em *Anais da 18ª Conferência Internacional sobre Comunicações e Redes de Computadores*, 2009, pp. 1-6.

59. Wang, H., Zhang, L., Li, T., e Tugnait, J., "Mitigação de interferência

espectralmente eficiente com base em salto de frequência 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., e Lenders, V., "Interferência reativa em redes sem fios: quão realista é a ameaça?", em *Anais da Quarta Conferência ACM sobre Segurança de Redes Sem Fios,* 2011, pp. 47-52.
61. Wood, A., Stankovic, J., e Son, S., "JAM: A Jammed-Area Mapping Service for Sensor Networks," em *Proceedings of the 24th IEEE Real-Time Systems Symposium,* 2003, pp. 286-297.
62. Wood, A., Stankovic, J. e Zhou, G., "DEEJAM: Derrotando a interferência eficiente em termos de energia e eficiência (Energy-) em redes sem fios baseadas em IEEE 802.15.4", em *Anais da 4ª Conferência Anual da Sociedade de Comunicações IEEE sobre Sensores, Malhas e Comunicações e Redes Ad Hoc*, 2007, pp. 60-69.
63. Xu, W., Wood, T., Trappe, W., e Zhang, Y., "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service" (Navegação por canais e retiradas espaciais: defesas contra negação de serviço sem fios), em *Proceedings of the 3rd ACM Workshop on Wireless Security* (Anais do 3.º Workshop ACM *sobre Segurança Sem Fios*), 2004, pp. 80-89.
64. Xu, W., Trappe, W., Zhang, Y., e Wood, T., "A viabilidade de lançar e detetar ataques de interferência em redes sem fios", em *Atas do 6.º Simpósio Internacional ACM sobre Redes e Computação Ad Hoc Móveis,* 2005, pp. 46-57.
65. Yoon, S. U., Murawski, R., Ekici, E., Park, S., e Mir, Z., "Salto de canal adaptativo para redes de sensores sem fios resistentes a interferências", em *Anais da Conferência Internacional IEEE sobre Comunicações*, 2010, pp. 1-5.
66. Estado-Maior do Exército Italiano - Gabinete de Segurança, *Sistemas de Software, Telecomunicações e Segurança - Documentos Não Classificados,* Roma, Itália, 2008.
67. Estado-Maior do Exército Italiano - Gabinete de Segurança, *Sistemas de Software, Telecomunicações e Segurança - Documentos Classificados,* Roma, Itália, 2008.
68. ISO/IEC 15408-1, *Tecnologia da informação - Técnicas de segurança - Critérios de avaliação para segurança de TI - Parte 1: Introdução e modelo geral,* Organização Internacional de Normalização, Genebra, 2009.
69. ISO/IEC 15408-2, *Tecnologia da Informação - Técnicas de Segurança - Critérios de Avaliação para Segurança de TI - Parte 2: Componentes Funcionais de Segurança,* Organização Internacional de Normalização, Genebra, 2008.
70. ISO/IEC 15408-3, *Tecnologia da Informação - Técnicas de Segurança - Critérios de Avaliação para Segurança de TI - Parte 3: Componentes de Garantia de Segurança,* Organização Internacional de Normalização, Genebra, 2008.
71. Departamento de Defesa dos EUA, *Critérios de Avaliação de Sistemas*

Informáticos Confiáveis, DoDD 5200.28-STD, Washington, DC, dezembro de 1985.
72. Departamento de Defesa dos EUA, *Diretiva: Garantia da Informação,* DoDD 8500.01E, Washington, DC, outubro de 2002.
73. Bundesamt für Sicherheit in der Informationstechnik, *Notas de aplicação e interpretação do esquema (AIS): ITSEC para mapeamento de critérios comuns com potencial de ataque específico,* Bona, Alemanha, 2010. Disponível online: https://www.bsi.bund.de
74. ISO/IEC 27000, *Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão da Segurança da Informação - Visão Geral e Vocabulário,* Organização Internacional de Normalização, Genebra, 2009.
75. Hare, F., "A ameaça cibernética à segurança nacional: por que não conseguimos chegar a um acordo", em *Anais da Conferência sobre Conflitos Cibernéticos,* Tallinn, Estónia, 2010, pp. 211-225.
76. Liles, S., «Guerra cibernética: como uma forma de conflito de baixa intensidade e insurgência», em *Anais da Conferência sobre Conflitos Cibernéticos*, Tallinn, Estónia, 2010, pp. 47-57.
77. Kotenko, I. V., "Multi-Agent Modeling and Simulation of Cyber-Attacks and Cyber Defense for Homeland Security" (Modelagem e simulação multiagente de ataques cibernéticos e defesa cibernética para a segurança interna), em *Anais do Workshop Internacional do IEEE sobre Aquisição Inteligente de Dados e Sistemas Avançados de Computação: Tecnologia e Aplicações,* Dortmund, Alemanha, 6-8 de setembro de 2008.
78. Kotenko, I. V., e Ulanov, A. V., "Simulação baseada em agentes de ataques DDoS e mecanismos de defesa"*, Journal of Computing,* vol. 4, n.º 2, 2005.
79. Gasser, L., "Criptografia pós-quântica", em V. Mulder, A. Mermoud, V. Lenders e B. Tellenbach (eds.), *Tendências em tecnologias de proteção de dados e criptografia,* Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33386-6.10
80. Radanliev, P., "Artificial Intelligence and Quantum Cryptography" (Inteligência artificial e criptografia quântica)*, Journal of Analytical Science and Technology,* vol. 15, artigo 4, 2024. https://doi.org/10.1186/s40543-024- 00416-6
81. Atutxa, A., Sanz, A., Sasiain, J., Astorga, J. e Jacob, E., "Rumo a um 5G quântico seguro: distribuição de chaves quânticas em redes centrais", *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., e Jedlicka, P., "Chaves híbridas na prática: combinando criptografia clássica, quântica e pós-quântica", *IEEE Access,* vol. 12, 2024, pp. 23206-23219. https://doi.org/10.1109/ACCESS.2024.3364520

83. Shim, K.-S., Kim, B., e Lee, W., “Pesquisa sobre protocolos aplicados de chaves quânticas, chaves de distribuição e chaves de criptografia pós-quântica para ciência de dados e segurança na web”, *Journal of Web Engineering,* vol. 23, n.º 6, setembro de 2024, pp. 813-830. https://doi.org/10.13052/jwe1540-9589.2365
84. Dhar, S., Khare, A., Dwivedi, A. D., e Singh, R., “Protegendo dispositivos IoT: uma nova abordagem usando blockchain e criptografia quântica”, *Internet of Things,* vol. 25, 2024, artigo 101019. https:ZZdoi.org/10.1016Zj.iot.2023.101019
85. Schneier, B., “Sistemas criptográficos baseados em redes e criptoanálise quântica”, *Communications of the ACM,* Online First, junho 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” (Aprimorando a criptografia quântica com fontes de fótons únicos de pontos quânticos)*, npj Quantum Information,* vol. 8, artigo 104, 2022. https://doi.org/10.1038/s41534-022-00626-z
87. Akçay, L., e Yalçın, B. Ö., “Lightweight ASIP Design for Lattice-Based Post-Quantum Cryptography Algorithms” (Projeto ASIP leve para algoritmos de criptografia pós-quântica baseados em rede), *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., e Etxezarreta Martinez, J., “Cibersegurança em infraestruturas críticas: uma perspetiva da criptografia pós-quântica”, *IEEE Internet of Things Journal,* vol. 11, n.º 18, 15 de setembro 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.,
e 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” (Aumentando a segurança da IoT: resiliência em nível quântico contra ameaças), *Computers, Materials and Continua*, vol. 78, n.º 1, 2024, pp. 329-356. https://doi.org/10.32604/cmc.2023.043439
91. Chawla, D., e Mehra, P. S., “A Survey on Quantum Computing for Internet of Things Security” (*Um estudo sobre computação quântica* para a segurança da Internet das Coisas), *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” (Implementação da criptografia pós-quântica para desenvolvedores), *SN Computer Science*, vol. 4, artigo 365, 2023.

https://doi.org/10.1007/s42979-023-01724-1
93. Ji, X., Wang, B., Hu, F., Wang, C., e Zhang, H., "Nova arquitetura de computação avançada
para o design e análise de criptografia pelo D-Wave Quantum Annealer", *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., "Uma estrutura para migração para criptografia pós-quântica: análise de dependência de segurança e estudos de caso", *IEEE Access,* vol. 12, 2024, pp. 23427-23450. https://doi.org/10.1109/ACCESS.2024.3360412
95. Kong, I., Janssen, M., e Bharosa, N., "Realizando o compartilhamento de informações com segurança quântica: desafios de implementação e adoção e recomendações de políticas para transições com segurança quântica"*, Government Information Quarterly,* vol. 41, n.º 1, 2024, artigo 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," *IEEE Communications Surveys and Tutorials,* Vol. 26, No. 3, 2024, pp. 1898-1949. https://doi.org/10.1109/COMST.2024.3367535
97. Hoque, S., Aydeger, A., e Zeydan, E., "Exploring Post-Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design" (Explorando a criptografia pós-quântica com distribuição de chaves quânticas para o projeto de arquitetura de rede móvel sustentável), *em Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems (PECS '24) (Anais do 4º Workshop sobre Desempenho e Eficiência Energética em Sistemas Concorrentes e Distribuídos*), ACM, Nova Iorque, 2024, pp. 9-16. https://doi.org/10.1145/3659997.3660033
98. Piatkowski, J., e Szymoniak, S., "Trivializando a verificação de protocolos criptográficos", *Métodos Assistidos por Computador em Engenharia e Ciência*, vol. 30, n.º 4, 2023, pp. 389-406. https://doi.org/10.24423/cames.869
99. Basin, D. A., Cremers, C., e Meadows, C. A., "Model Checking Security Protocols" (Verificação de Modelos de Protocolos de Segurança), em E. Clarke, T. Henzinger, H. Veith e R. Bloem (eds.), *Handbook of Model Checking (Manual de Verificação 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" (Modelagem *e verificação de protocolos de segurança com o cálculo Pi* aplicado e o 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., e Cortier, V., "ProVerif com Lemas, Indução, Subsumção Rápida e Muito Mais", em *Anais do Simpósio IEEE sobre Segurança e Privacidade (S&P 2022),* IEEE Computer Society, São Francisco, Califórnia,

2022, pp. 205-222. https://hal.inria.fr/hal-03366962/
102. Bouroulet, R., Devillers, R., Klaudel, H., Pelz, E., e Pommereau, F., "Modelagem e análise de protocolos de segurança usando especificações baseadas em funções e redes de Petri", em K. M. van Hee e R. Valk (eds.), *Aplicações e teoria das redes de Petri,* Springer, Berlim e Heidelberg, 2008, pp. 72-91.
103. Burrows, M., Abadi, M., e Needham, R., "A Logic of Authentication" (Uma lógica de autenticação), *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," em *Proceedings of the Workshop on Specification and Automated Processing of Security Requirements (SAPS 2004),* Austrian Computer Society, Linz, Áustria, 2004, p. 13.
105. Cortier, V., Delaune, S., e Dreier, J., "Geração automática de lemas de origem em Tamarin: rumo a provas automáticas de protocolos de segurança", em L. Chen, N. Li, K. Liang e S. Schneider (eds.), *Segurança informática - ESORICS 2020,* Springer, Cham, 2020, pp. 3-22.
106. David, A., Larsen, K. G., Legay, A., Mikucionis, M., e Poulsen, D. B., "Tutorial UPPAAL SMC", *Revista Internacional sobre Ferramentas de Software para Transferência de Tecnologia,* vol. 17, n.º 4, 2015, pp. 397-415. https://doi.org/10.1007/s10009-014-0361-y
107. Dolev, D., e Yao, A. C., "On the Security of Public Key Protocols," em *Proceedings of the 22nd Annual Symposium on Foundations of Computer Science (SFCS '81),* IEEE Computer Society, Washington, DC, 1981, pp. 350-357.
108. Gregor, D., Järvi, J., Siek, J., Reis, G., Stroustrup, B., e Lumsdaine, A., « » (Conceitos: suporte linguístico para programação genérica em 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., e Szymoniak, S., "ProToc: uma linguagem universal para especificações de protocolos de segurança", em A. Wilinski, I. E. Fray e 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., e Modersheim, S., "Um Resultado de Tipagem para Protocolos com Estado", em *Anais do 31º Simpósio de Fundamentos de Segurança Informática do IEEE (CSF 2018),* IEEE, 2018, pp. 374-388. https://doi.org/10.1109/CSF.2018.00034
112. Järvi, J., Gregor, D., Willcock, J., Lumsdaine, A., e Siek, J., "Algoritmo

Specialization in Generic Programming: Challenges of Constrained Generics in C++," *ACM SIGPLAN Notices*, Vol. 41, No. 6, 2006, pp. 272-282. https://doi.org/10.1145/1133255.1134014

113. Kassem, A., Lafourcade, P., Lakhnech, Y., e Modersheim, S., "Intrusos preguiçosos múltiplos independentes", em *Anais do 1º Workshop sobre Questões Quentes em Princípios de Segurança e Confiança (HotSpot 2013)*, 2013, 15 páginas.

114. Kordy, B., Mauw, S., Radomirovic, S., e Schweitzer, P., «Fundamentos das árvores de ataque-defesa», em P. Degano, S. Etalle e J. Guttman (eds.), *Aspectos formais em segurança e confiança (FAST 2010),* Notas de aula em ciência da computação, vol. 6561, Springer, Berlim e Heidelberg, 2010, pp. 80-95. https://doi.org/10.1007/978-3-642-19751-2_6

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

116. Kurkowski, M., *Métodos formais para verificação das propriedades do protocolo de segurança em redes de computadores* (em polaco), Akademicka Oficyna Wydawnicza Exit, Varsóvia, 2013.

117. Liang, J., Nguyen, Q., Simoff, S., Huang, M., "Divide and Conquer Treemaps: Visualização de árvores grandes com várias formas", *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. e Zhu, J., "Visual Diagnosis of Tree Boosting Methods" (Diagnóstico visual de métodos de reforço de árvores), *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., e Oostdijk, M., "Fundamentos das árvores de ataque", em *Conferência Internacional sobre Segurança da Informação e Criptologia,* Springer, 2005, pp. 186-198. https://doi.org/10.1007/11734727_17

120. Millen, J. K., "CAPSL: Common Authentication Protocol Specification Language" (CAPSL: Linguagem de Especificação de Protocolo de Autenticação Comum), em *Proceedings of the Workshop on New Security Paradigms (NSPW '96) (Anais do Workshop sobre Novos Paradigmas de Segurança),* 1996. https://doi.org/10.1145/304851.304879

121. Morin, P., *Estruturas de dados abertas (em C++),* 2013. https://opendatastructures.org/

122. Modersheim, S., Nielson, F., e Nielson, H. R., "Lazy Mobile Intruders," em D. A. Basin e 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., e Schroeder, M. D., "Using Encryption for Authentication in Large Networks of Computers," *Communications of the ACM*, Vol. 21, No. 12,

1978, pp. 993-999. https://doi.org/10.1145/359657.359659
124. Neuman, B. C., e Ts'o, T., "Kerberos: Um Serviço de Autenticação para Redes de Computadores", *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" (A árvore mapeada multivias condicional: modelagem e análise de dependências hierárquicas de dados), *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., e 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., e Kurkowski, M., «Um método rápido para verificação de protocolos de segurança», em *Anais da 18ª Conferência Internacional sobre Sistemas de Informação Computacional e Gestão 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., e Fray, I. E., "Towards the Most Efficient Method for Untimed Security Protocols Verification" (Rumo ao método mais eficiente para verificação de protocolos de segurança sem tempo), em *Anais da 24ª Conferência Ásia-Pacífico sobre Sistemas de Informação (PACIS 2020),* Dubai, Emirados Árabes Unidos, 2020, p. 189.
129. Siek, J. G., e Lumsdaine, A., "A Language for Generic Programming in the Large" (Uma linguagem para programação genérica em grande 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. e Piatkowski, J., "Modelos temporizados de protocolos de segurança
incluindo atrasos na rede", *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., e Sorenson, P. G., *An Introduction to Data Structures with Applications,* 2.ª ed., McGraw-Hill, Auckland, 1984.
133. Witten, I. H., Frank, E., e Hall, M. A., *Mineração de dados: ferramentas e técnicas práticas de aprendizagem automática,* 3.ª ed., Morgan Kaufmann, Amesterdão, 2011.

134. R. Mustafovski, A. Petrovski e M. Radovanovic, "Integrando tecnologias quânticas em sistemas militares móveis e estruturas TOC", *Land Forces Academy Review,* vol. XXX, n.º 3(119), 2025.
135. R. Mustafovski, "Estrutura arquitetónica baseada em fórmulas da plataforma SecuDroneComm para comunicações de veículos aéreos não tripulados", *Management Science Advances*, vol. 2, n.º 1, pp. 288-303, Scientific Oasis, Skopje, República da Macedónia do Norte, 2025.
136. R. Mustafovski, "Avaliação do impacto operacional do SecuDroneComm: Avaliação baseada em simulação da comunicação segura de UAV em ambientes militares", *Scientific Technical Review,* vol. 75, n.º 1, pp. 11-18, 2025, doi: 10.5937/str2500002M.
137. M. Mozaffari, W. Saad, M. Bennis e M. Debbah, "Implantação eficiente de múltiplos veículos aéreos não tripulados para cobertura sem fios ideal", *IEEE Communications Letters,* vol. 20, n.º 8, pp. 1647-1650, 2016.
138. L. Ruan et al., "Implantação de cobertura multi-UAV com eficiência energética em redes UAV: uma estrutura de teoria de jogos", *China Communications,* vol. 15, n.º 10, pp. 194209, 2018.
139. M. Mozaffari, W. Saad, M. Bennis e M. Debbah, "Veículos aéreos não tripulados móveis (UAVs) para comunicações de Internet das Coisas energeticamente eficientes", *IEEE Transactions on Wireless Communications*, 2017.
140. S.-Y Lien, K.-C. Chen e Y. Lin, "Rumo a acessos massivos ubíquos em comunicações máquina a máquina 3GPP", *IEEE Communications Magazine*, vol. 49, n.º 4, pp. 66-74, abril de 2011.
141. M. Malik e S. K. Garg, "Rumo ao 6G: evolução da rede além do 5G e o cenário indiano", em *Proc. 2ª Conferência Internacional sobre Práticas Inovadoras em Tecnologia e Gestão (ICIPTM)*, Gautam Buddha Nagar, Índia, pp. 123-127, 2022.
142. M. A. Khan et al., "Enxame de UAVs para gestão de rede em 6G: uma revisão técnica", *IEEE Transactions on Network and Service Management,* vol. 20, n.º 1, pp. 741761, março de 2023.
143. S. Dang, O. Amin, B. Shihada e M.-S. Alouini, "O que deve ser o 6G?", *Nature Electronics*, vol. 3, n.º 1, pp. 20-29, 2020.
144. F. Ronaldo, D. Pramadihanto e A. Sudarsono, "Sistema de comunicação seguro para serviços de drones usando criptografia híbrida em rede 4G/LTE", em *Proc. Int. Electronics Symposium (IES),* Surabaya, Indonésia, pp. 116-122, 2020.
145. T. Li et al., "Comunicações seguras entre UAV e veículos", *IEEE Transactions on Communications*, vol. 69, n.º 8, pp. 5381-5393, agosto de 2021.
146. S. A. Ayati e H. R. Naji, "Um mecanismo seguro para proteger as comunicações de UAV", em *Proc. 9º Congresso Conjunto Iraniano sobre Sistemas*

Fuzzy e Inteligentes (CFIS), Bam, Irão, pp. 1-6, 2022.
147. D. Pirker, T. Fischer, C. Lesjak e C. Steger, "Sistema de autenticação global e seguro para UAVs baseado em segurança de hardware", em *Proc. 8.ª Conferência Internacional IEEE sobre Computação em Nuvem Móvel, Serviços e Engenharia (MobileCloud)*, Oxford, Reino Unido, pp. 84-89, 2020.
148. H. Wang, H. Fang e X. Wang, "Autenticação descentralizada suave habilitada por inteligência de ponta em enxame de UAV", em *Proc. IEEE/CIC Int. Conf. Communications in China (ICCC)*, Xiamen, China, pp. 86-91, 2021.
149. M. Markowski, P. Ryba e K. Puchala, "Laboratório de pesquisa em redes definidas por software: topologias e cenários experimentais", em *Proc. 3rd European Network Intelligence Conf. (ENIC),* Wroclaw, Polónia, pp. 252-256, 2016.
150. M. A. B. S. Abir, M. Z. Chowdhury e Y. M. Jang, "Redes UAV definidas por software para sistemas 6G: Requisitos, oportunidades, técnicas emergentes, desafios e direções de pesquisa", *IEEE Open Journal of the Communications Society,* vol. 4, pp. 2487-2547, 2023.
151. M. Ouadah e F. Merazka, "Uma abordagem de codificação de rede para redes UAV confiáveis baseadas em SDN", em *Proc. 5ª Conferência Internacional de Engenharia Elétrica e Aplicações de Controlo (ICEECA '22),* Khenchela, Argélia, 2022.

Biografia de Rexhep Mustafovski, MSc

Rexhep Mustafovski, MSc, é oficial do Ministério da Defesa da República da Macedónia do Norte e assistente de ensino e investigação na Academia Militar "General Mihailo Apostolski" em Skopje, onde trabalha no Departamento de Cibersegurança e Perícia Digital. É especialista em sistemas de comunicação seguros, cibersegurança e integração de tecnologia de defesa, com experiência académica e profissional que abrange comunicações táticas seguras, segurança de redes e sistemas de informação emergentes.

Concluiu a sua formação de licenciatura na Academia Militar «General Mihailo Apostolski» em Skopje, onde se formou como Oficial de Comunicações. Durante os seus estudos, demonstrou um desempenho académico e uma disciplina profissional excecionais, alcançando o maior sucesso educativo da sua geração. Em reconhecimento a esta conquista, foi oficialmente premiado como o melhor oficial da sua geração, uma honra conferida pelo Presidente do país. Esta distinção reflete tanto a sua excelência académica como o seu compromisso com o profissionalismo militar.

Após a sua nomeação, continuou o seu desenvolvimento académico, prosseguindo estudos de pós-graduação na Faculdade de Engenharia Elétrica e Tecnologias da Informação da Universidade «Ss. Cyril and Methodius» em Skopje. Obteve o grau de Mestre em Ciências da Comunicação e Tecnologias da Informação, com especialização em sistemas de comunicação modernos, segurança da informação e conceitos avançados de redes. Os seus estudos de mestrado reforçaram ainda mais as suas capacidades analíticas e de investigação, particularmente nas áreas das comunicações seguras e dos sistemas de defesa baseados na tecnologia.

A sua trajetória académica e profissional combina educação militar formal com estudos avançados de engenharia, proporcionando uma base sólida para a investigação e o trabalho prático em comunicações militares seguras. Esta formação influencia a sua abordagem ao design de sistemas de comunicação, enfatizando a

fiabilidade, a segurança, a interoperabilidade e e e a relevância operacional. O conhecimento e a experiência adquiridos através da formação militar e da educação em engenharia sustentam as perspetivas apresentadas ao longo deste livro.