Sistemi di comunicazione sicuri per le moderne operazioni militari

Questo libro offre un esame completo dei sistemi di comunicazione sicuri per le moderne operazioni militari, affrontando le sfide tecnologiche e operative dello scambio di informazioni nei campi di battaglia contemporanei e futuri. Traccia l'evoluzione delle comunicazioni militari dai sistemi analogici e digitali alle architetture criptate, definite dal software e potenziate dall'intelligenza artificiale, ponendo l'accento sull'interoperabilità NATO, sulle minacce alla sicurezza informatica e sulla guerra elettronica. Vengono analizzati principi fondamentali come la trasmissione del segnale, la crittografia, l'autenticazione, le tecniche anti-jamming e le reti radio tattiche resilienti. Tra gli argomenti avanzati figurano le comunicazioni sicure tra UAV e centro di comando, il routing e la gestione dello spettro guidati dall'intelligenza artificiale, i sistemi satellitari, le applicazioni militari 5G/6G, le comunicazioni quantistiche e le reti radio cognitive. Il libro propone inoltre un quadro di comunicazione sicura orientato al futuro e integrato con i sistemi C4ISR, supportato da casi di studio pratici, tra cui la ricerca di dottorato dell'autore. È destinato a ricercatori, professionisti militari, ingegneri e responsabili politici alla ricerca di soluzioni di comunicazione resilienti e intelligenti per la difesa.

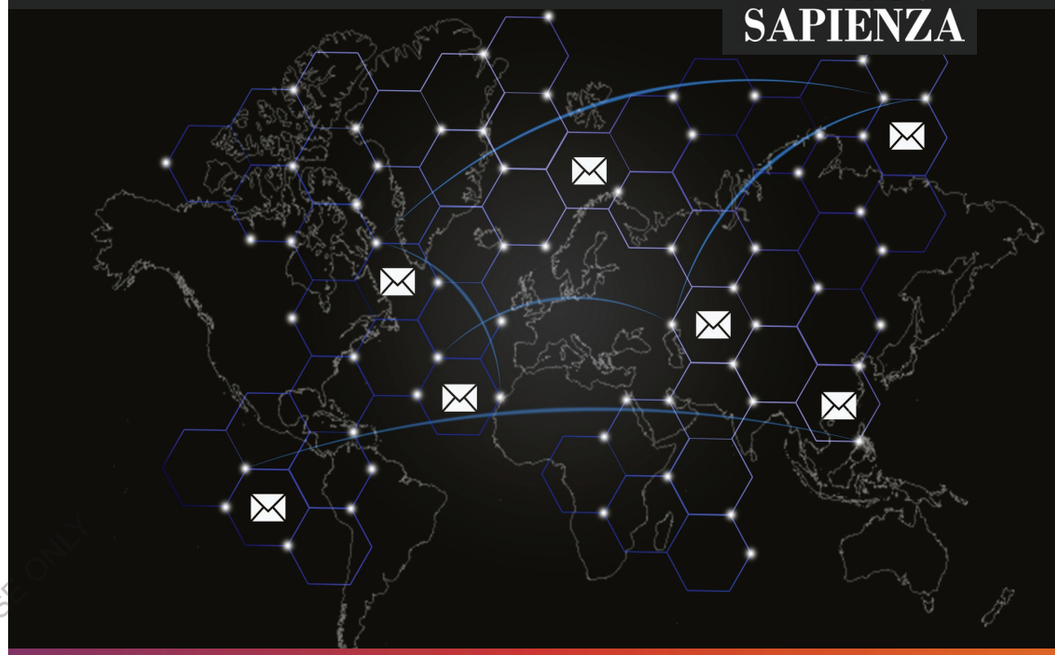
Rexhep Mustafovski, MSc, è un ufficiale di segnale e ricercatore in comunicazioni militari. Ha conseguito una laurea presso l'Accademia militare "General Mihailo Apostolski" di Skopje e un master in Comunicazione e tecnologie dell'informazione presso l'Università "Ss. Cirillo e Metodio".

9 786209 575563

EDIZIONI SAPIENZA

Rexhep Mustafovski

EDIZIONI SAPIENZA



Sistemi di comunicazione sicuri per le moderne operazioni militari

Fondamenti, tecnologie e direzioni future

Rexhep Mustafovski

Rexhep Mustafovski

Sistemi di comunicazione sicuri per le moderne operazioni militari

Rexhep Mustafovski

Sistemi di comunicazione sicuri per le moderne operazioni militari

Fondamenti, tecnologie e direzioni future

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: 978-620-9-57556-3

Sistemi di comunicazione sicuri per le operazioni militari moderne: fondamenti, tecnologie e orientamenti futuri

Indice

Prefazione

Sono Rexhep Mustafovski, MSc, e questo libro è il risultato del mio impegno accademico, professionale e di ricerca nel campo dei moderni sistemi di comunicazione, con particolare attenzione alle applicazioni sicure orientate alla difesa e al settore militare. La motivazione che mi ha spinto a scrivere questo libro nasce dalla crescente importanza delle tecnologie avanzate nel plasmare la società contemporanea e, più specificamente, nel trasformare il modo in cui le forze armate comunicano, coordinano e operano in ambienti complessi e contesi.

Nel mondo moderno, la tecnologia non è più un elemento periferico dell'attività umana, ma un motore centrale del cambiamento in ambito economico, sociale e della sicurezza. Le tecnologie di comunicazione, in particolare, sono diventate fondamentali per il modo in cui le informazioni vengono generate, trasmesse, protette e sfruttate. In contesti militari, la comunicazione sicura non è solo un requisito tecnico, ma una necessità strategica. La capacità di scambiare informazioni in modo sicuro, affidabile e in tempo reale influenza direttamente l'efficacia operativa, il processo decisionale e la protezione delle forze. Questo libro è stato scritto con l'intento di presentare queste realtà a un pubblico accademico e professionale più ampio, collegando le basi teoriche con le applicazioni militari pratiche.

Il mio background accademico nelle tecnologie della comunicazione e dell'informazione, combinato con il mio impegno professionale nell'istruzione e nella ricerca militare, ha plasmato la prospettiva adottata in questo lavoro. Nel corso dei miei studi e delle mie attività di ricerca, ho osservato un divario ricorrente tra le tecnologie di comunicazione in rapida evoluzione e la loro integrazione strutturata a livello di sistema all'interno dei quadri militari. Mentre molti lavori si concentrano su tecnologie isolate o soluzioni tecniche specifiche, pochi tentano di presentare una visione completa e integrata dei sistemi di comunicazione militare sicuri come architetture in evoluzione. Questo libro cerca di colmare tale divario offrendo un esame coerente e strutturato delle tecnologie, dei meccanismi di sicurezza e dei principi architettonici che sono alla base delle comunicazioni militari moderne e future.

Il libro si basa anche sulla mia ricerca di dottorato in corso, che si concentra su quadri di comunicazione sicuri e piattaforme di comunicazione avanzate per applicazioni di difesa. Una parte di questa ricerca è incorporata nel libro sotto forma di un caso di studio dedicato, che presenta un esempio pratico di come i concetti teorici e i principi architettonici possano essere applicati a un sistema reale. Questo caso di studio, derivato dal mio lavoro di dottorato, è stato incluso per dimostrare il passaggio dall'analisi concettuale alla progettazione e all'implementazione del

sistema. Il suo scopo non è quello di fornire una soluzione definitiva, ma piuttosto di illustrare come le piattaforme di comunicazione sicure possano essere strutturate per soddisfare i requisiti operativi quali sicurezza, affidabilità, latenza e interoperabilità.

Nel scrivere questo libro, ho cercato di mantenere un equilibrio tra rigore accademico e rilevanza pratica. Il contenuto si basa su principi consolidati di ingegneria delle comunicazioni, sicurezza informatica e sistemi militari, riflettendo al contempo le attuali tendenze tecnologiche quali l'intelligenza artificiale, le radio definite dal software, i sistemi senza pilota, le comunicazioni satellitari e i meccanismi di sicurezza emergenti. L'intenzione non era quella di produrre un testo puramente teorico, né un manuale strettamente tecnico, ma un lavoro accademico strutturato che potesse servire da riferimento per studenti, ricercatori, ingegneri e professionisti militari interessati alla progettazione e all'evoluzione dei sistemi di comunicazione sicuri.

Il pubblico di questo libro è quindi volutamente ampio e comprende studenti laureati e post-laureati in ingegneria e discipline legate alla difesa, ricercatori che lavorano nei settori della comunicazione e della sicurezza e professionisti coinvolti nella pianificazione delle comunicazioni militari, nello sviluppo di sistemi e nella distribuzione operativa. Allo stesso tempo, il libro è scritto con sufficiente profondità e attenzione analitica per supportare studi accademici avanzati e contribuire alle discussioni in corso all'interno della comunità di ricerca.

Infine, questo libro rappresenta una tappa di un percorso accademico e professionale più lungo. Riflette sia la ricerca completata che quella in corso, riconoscendo che il campo delle comunicazioni militari è dinamico e in continua evoluzione. Le tecnologie, le architetture e i framework discussi in questo lavoro continueranno senza dubbio a svilupparsi in risposta alle nuove esigenze operative e alle minacce emergenti. Mi auguro che questo libro contribuisca a una comprensione più approfondita dei sistemi di comunicazione sicuri e incoraggi ulteriori ricerche, discussioni e innovazioni in questo settore critico.

Introduzione

I sistemi di comunicazione militare hanno sempre svolto un ruolo decisivo nella conduzione delle operazioni belliche, influenzando il modo in cui le forze armate coordinano, decidono e agiscono nei vari contesti operativi. Dalle prime forme di segnalazione sul campo di battaglia alle odierne architetture globali interconnesse e basate sui dati, la comunicazione è rimasta un fattore centrale per il comando, il controllo e l'efficacia operativa. Nelle operazioni militari contemporanee, tuttavia, i sistemi di comunicazione si sono evoluti oltre il loro tradizionale ruolo di supporto e ora costituiscono una capacità strategica a sé stante. Infrastrutture di comunicazione sicure, resilienti e adattabili sono fondamentali per ottenere la superiorità informativa, mantenere il ritmo operativo e garantire la sopravvivenza delle forze in ambienti sempre più complessi e contesi.

La trasformazione della guerra nel XXI secolo ha introdotto nuove sfide che alterano in modo fondamentale i requisiti richiesti ai sistemi di comunicazione militare. Le operazioni moderne sono caratterizzate da elevata mobilità, impegno multidominio e integrazione di attività convenzionali, informatiche e di guerra dell'informazione. Le forze operano nei domini terrestre, aereo, marittimo, spaziale e informatico, spesso simultaneamente e in coordinamento con partner congiunti e della coalizione. In tali condizioni, la capacità di scambiare informazioni accurate, tempestive e protette determina non solo il successo tattico, ma anche i risultati strategici. I sistemi di comunicazione devono quindi funzionare in modo affidabile in condizioni di incertezza, interruzione e interferenza attiva da parte degli avversari.

Una delle caratteristiche distintive delle moderne comunicazioni militari è la centralità della sicurezza. Man mano che le reti di comunicazione diventano più interconnesse e guidate dal software, sono sempre più esposte ad attacchi informatici, guerra elettronica e sfruttamento da parte degli avversari. La riservatezza, l'integrità, la disponibilità e l'autenticità delle informazioni non sono più concetti tecnici astratti, ma necessità operative. I sistemi di comunicazione compromessi possono portare a disinformazione, perdita dell'autorità di comando, fallimento della missione o escalation involontaria. Di conseguenza, le considerazioni di sicurezza devono essere integrate a ogni livello della progettazione dei sistemi di comunicazione, dai meccanismi di trasmissione fisica alle architetture di rete e ai servizi a livello di applicazione.

Allo stesso tempo, l'innovazione tecnologica sta accelerando a un ritmo senza precedenti. I progressi nelle comunicazioni digitali, nella crittografia, nell'intelligenza artificiale, nei sistemi satellitari e nelle tecnologie emergenti come la comunicazione quantistica stanno rapidamente ridisegnando il panorama delle

comunicazioni militari. Questi sviluppi offrono significative opportunità per migliorare le prestazioni, la resilienza e l'adattabilità, ma introducono anche nuove vulnerabilità e complessità. Le istituzioni militari devono quindi bilanciare l'adozione di tecnologie avanzate con una progettazione architettonica rigorosa, una disciplina operativa e una responsabilità etica.

Questo libro nasce dall'esigenza di fornire un'analisi completa e integrata dei sistemi di comunicazione militare sicuri nel contesto delle operazioni di difesa moderne e future. Anziché concentrarsi su tecnologie isolate o problemi tecnici specifici, il libro adotta una prospettiva a livello di sistema che considera la comunicazione come un quadro interconnesso che coinvolge hardware, software, meccanismi di sicurezza, dottrina operativa e processo decisionale umano. L'obiettivo è quello di presentare una visione coerente di come i sistemi di comunicazione sicuri vengono progettati, implementati e sviluppati per soddisfare le esigenze della guerra contemporanea.

I capitoli iniziali stabiliscono il contesto fondamentale per la discussione. Le comunicazioni militari moderne vengono esaminate attraverso la loro evoluzione storica dai sistemi analogici e punto a punto alle architetture digitali, crittografate e in rete. Questa evoluzione riflette cambiamenti più ampi nella dottrina militare, nel ritmo operativo e nei requisiti informativi. L'importanza delle comunicazioni sicure viene sottolineata non solo in termini di protezione delle informazioni, ma anche di coordinamento e legalità delle azioni militari. Il ruolo della standardizzazione, in particolare all'interno dei quadri di alleanza, viene enfatizzato come fattore critico per garantire l'interoperabilità e la coesione operativa tra le forze alleate.

Il libro esplora poi i principi fondamentali alla base dei sistemi di comunicazione sicuri. La trasmissione e la propagazione dei segnali e le sfide associate alla comunicazione in linea di vista e non in linea di vista vengono esaminate per stabilire una base tecnica di riferimento. Questi principi rimangono rilevanti nonostante i progressi tecnologici, poiché i vincoli fisici e i fattori ambientali continuano a influenzare le prestazioni delle comunicazioni. Partendo da queste basi, il libro analizza i meccanismi di sicurezza fondamentali come la crittografia, l'autenticazione, il controllo degli accessi e le tecniche anti-jamming. Questi elementi costituiscono la spina dorsale delle architetture di comunicazione sicure e sono essenziali per mantenere l'affidabilità e la fiducia in ambienti contesi.

La sicurezza informatica emerge come tema centrale nei capitoli successivi. Le reti di comunicazione militari sono sempre più bersaglio di sofisticate minacce informatiche che cercano di interrompere le operazioni, sottrarre informazioni sensibili o manipolare i processi decisionali. Il libro esamina la natura di queste minacce e le strategie utilizzate per mitigarle, tra cui il rafforzamento della rete, la selezione dei protocolli crittografici, le architetture zero trust e i meccanismi di

risposta agli incidenti. Affrontando la sicurezza informatica sia a livello tecnico che architettonico, il libro sottolinea l'importanza della resilienza e dell'adattabilità di fronte a minacce persistenti e in continua evoluzione.

I sistemi di comunicazione radio rimangono una pietra miliare delle operazioni tattiche e il loro ruolo viene esaminato in profondità. I tradizionali sistemi VHF, UHF e HF continuano a fornire capacità essenziali, in particolare in ambienti in cui le infrastrutture sono limitate o degradate. L'integrazione di questi sistemi con radio definite dal software e tecniche di rete mesh illustra come le tecnologie legacy possano essere migliorate attraverso approcci architetturali moderni. L'interoperabilità con le forze alleate è considerata un requisito fondamentale, che riflette la realtà delle operazioni congiunte e di coalizione negli scenari di conflitto contemporanei.

Il crescente utilizzo di sistemi aerei senza pilota introduce nuove dimensioni nelle comunicazioni militari. Gli UAV fungono da raccoglitori di dati, ripetitori di comunicazione e piattaforme operative che estendono la portata e la flessibilità delle reti militari. Il libro analizza le sfide di sicurezza associate alla comunicazione tra gli UAV e il centro di comando, tra cui la crittografia, l'autenticazione, la protezione del livello di collegamento e i vincoli di prestazione come la latenza e l'affidabilità. Un caso di studio dedicato presenta una piattaforma di comunicazione sicura integrata, illustrando come i concetti teorici possano essere applicati nella pratica per soddisfare i requisiti operativi del mondo reale.

L'intelligenza artificiale rappresenta una forza di trasformazione nei sistemi di comunicazione militare. Il libro esplora come le tecniche di IA possano migliorare l'efficienza del routing, il rilevamento delle intrusioni, l'allocazione dello spettro e la gestione della rete in ambienti di battaglia. Consentendo ai sistemi di percepire, apprendere e adattarsi, le architetture di comunicazione basate sull'IA offrono nuovi livelli di resilienza ed efficienza operativa. Allo stesso tempo, l'integrazione dell'IA solleva importanti questioni relative alla trasparenza, alla responsabilità e al controllo, che vengono affrontate attraverso un'analisi equilibrata e critica.

Le tecnologie emergenti costituiscono un altro punto focale del libro. Le reti cellulari di nuova generazione, le comunicazioni satellitari, la distribuzione di chiavi quantistiche e le reti radio cognitive sono esaminate come fattori abilitanti delle future capacità di comunicazione militare. Queste tecnologie ampliano il raggio operativo supportando velocità di trasmissione dati più elevate, connettività globale, maggiore sicurezza e utilizzo intelligente dello spettro. La loro integrazione nei sistemi militari riflette un passaggio verso un'architettura ibrida che combina componenti terrestri, aerei, marittimi e spaziali in un quadro di comunicazione unificato.

I capitoli finali sintetizzano questi sviluppi tecnologici e concettuali in una discussione più ampia su come costruire quadri di comunicazione sicuri per l'esercito del futuro. I requisiti delle forze moderne sono analizzati in termini di resilienza, interoperabilità, scalabilità e sicurezza. Vengono presentati i principi architettonici per illustrare come si possono progettare sistemi di comunicazione tattica sicuri a supporto di operazioni complesse e distribuite. L'integrazione con i sistemi C4ISR è sottolineata come fattore critico per ottenere la consapevolezza situazionale e la superiorità decisionale. Vengono affrontate considerazioni etiche e legali per garantire che l'innovazione tecnologica sia in linea con le norme e le responsabilità stabilite. La discussione sulle tendenze future fornisce una prospettiva lungimirante su come i sistemi di comunicazione militare potrebbero evolversi in risposta alle minacce emergenti e alle opportunità tecnologiche.

Il pubblico a cui è rivolto questo libro comprende professionisti militari, ingegneri della difesa, ricercatori e studenti laureati impegnati nello studio e nello sviluppo di sistemi di comunicazione sicuri. Il libro è rilevante anche per i responsabili politici e i decisori coinvolti nella pianificazione della difesa e nello sviluppo delle capacità. Combinando l'analisi tecnica con prospettive architettoniche e operative, il libro cerca di colmare il divario tra teoria e pratica nelle comunicazioni militari.

Questo libro mira a contribuire alla comprensione e allo sviluppo di sistemi di comunicazione militare sicuri, presentando una prospettiva integrata e orientata al futuro. Poiché la guerra continua ad evolversi in termini di complessità e portata, la capacità di comunicare in modo sicuro, affidabile e intelligente rimarrà un fattore decisivo per l'efficacia militare. Attraverso un esame completo delle tecnologie, dell'architettura e dei principi, questo lavoro cerca di fornire una base per la costruzione di sistemi di comunicazione che supportino il successo operativo, mantenendo al contempo la sicurezza, la resilienza e la responsabilità nelle operazioni militari moderne e future.

Conclusione

Questo libro ha esaminato l'evoluzione, la struttura e la direzione futura dei sistemi di comunicazione militare sicuri nel contesto delle operazioni di difesa moderne ed emergenti. Nei suoi capitoli, l'opera ha dimostrato che le comunicazioni militari non sono più solo tecnologie di supporto, ma costituiscono un pilastro centrale dell'efficacia operativa, del processo decisionale strategico e della superiorità informativa. La crescente complessità del contesto di sicurezza, unita al rapido progresso tecnologico, richiede strutture di comunicazione resilienti, intelligenti, interoperabili ed eticamente fondate.

I primi capitoli hanno stabilito l'importanza fondamentale delle comunicazioni sicure nelle operazioni militari. Le forze armate moderne operano in condizioni di incertezza, mobilità e minaccia persistente, dove la capacità di scambiare informazioni accurate e tempestive determina il successo o il fallimento della missione. Il passaggio da sistemi analogici e isolati ad architetture di comunicazione digitali, crittografate e in rete riflette un più ampio spostamento verso una guerra incentrata sull'informazione. Questa evoluzione ha trasformato i sistemi di comunicazione in facilitatori attivi del comando, del controllo e del coordinamento in tutti i settori operativi.

Un tema centrale in tutto il libro è stato il rapporto indissolubile tra comunicazione e sicurezza. Man mano che le reti militari diventano più interconnesse e guidate dal software, sono sempre più esposte a minacce informatiche, guerra elettronica e sfruttamento da parte di avversari. L'analisi della crittografia, dell'autenticazione, del controllo degli accessi e del rafforzamento della rete ha evidenziato la necessità di integrare meccanismi di sicurezza in tutti i livelli delle architetture di comunicazione. Anziché trattare la sicurezza come un elemento aggiuntivo, i moderni sistemi militari devono adottare un approccio di sicurezza fin dalla progettazione che garantisca la riservatezza, l'integrità, l'autenticità e la disponibilità in condizioni di conflitto.

La discussione sui sistemi di comunicazione radio per le unità tattiche ha dimostrato che le tecnologie legacy rimangono operative quando integrate in un'architettura moderna. I sistemi VHF, UHF e HF continuano a fornire solide capacità di comunicazione, in particolare in ambienti degradati o negati. Se combinate con radio definite dal software e principi di rete mesh, queste tecnologie offrono flessibilità e resilienza essenziali per le operazioni tattiche. La capacità di adattare forme d'onda, frequenze e strategie di routing consente alle forze di mantenere la connettività nonostante la mobilità, i vincoli del terreno e le interferenze ostili.

I sistemi aerei senza pilota e la loro integrazione in strutture di comunicazione sicure sono stati esaminati come una caratteristica distintiva delle operazioni

militari contemporanee. Gli UAV funzionano non solo come piattaforme di rilevamento, ma anche come nodi di comunicazione dinamici dell' , che estendono la portata della rete e migliorano la consapevolezza della situazione. L'analisi della comunicazione tra gli UAV e il centro di comando ha sottolineato l'importanza della crittografia, dell'autenticazione, della sicurezza del livello di collegamento e dell'ottimizzazione delle prestazioni. Il caso di studio presentato ha illustrato come una piattaforma di comunicazione integrata e sicura possa supportare lo scambio di dati in tempo reale, affrontando al contempo i vincoli di latenza, affidabilità e throughput negli ambienti operativi.

L'intelligenza artificiale è emersa come una forza trasformativa nei sistemi di comunicazione militare. L'esplorazione del routing basato sull'IA, del rilevamento delle intrusioni, dell'allocazione dello spettro e del networking sul campo di battaglia ha dimostrato come gli algoritmi intelligenti possano migliorare l'adattabilità e la resilienza. L'IA consente ai sistemi di comunicazione di rispondere in modo dinamico ai cambiamenti ambientali e alle azioni ostili, riducendo il carico cognitivo sugli operatori umani e migliorando il ritmo operativo. Allo stesso tempo, l'integrazione dell'IA solleva importanti questioni relative alla trasparenza, alla responsabilità e al controllo, rafforzando la necessità di un'implementazione responsabile e ben governata.

Le tecnologie emergenti come le reti cellulari di nuova generazione, le comunicazioni satellitari, la distribuzione di chiavi quantistiche e le reti radio cognitive sono state analizzate come fattori abilitanti delle future capacità di comunicazione militare. Queste tecnologie ampliano il raggio d'azione operativo supportando velocità di trasmissione dati più elevate, connettività globale, maggiore sicurezza e utilizzo intelligente dello spettro. La loro integrazione nei sistemi militari riflette un passaggio verso architetture ibride che combinano componenti terrestri, aerei, marittimi e spaziali. Questa convergenza consente operazioni multidominio, introducendo al contempo nuove sfide architetturali e di sicurezza che devono essere affrontate in modo olistico.

I capitoli finali si sono concentrati sulla creazione di un quadro di comunicazione sicuro per l'esercito del futuro. L'analisi ha sottolineato che il progresso tecnologico da solo non è sufficiente senza una progettazione architettonica coerente, l'integrazione con i sistemi C4ISR e la considerazione delle implicazioni etiche e legali. I futuri quadri di comunicazione devono supportare l'interoperabilità, la scalabilità e la resilienza, pur rimanendo conformi al diritto internazionale e ai principi etici. L'inclusione di considerazioni relative alla governance, alla responsabilità e alla sostenibilità garantisce che i sistemi di comunicazione contribuiscano alla sicurezza e alla stabilità a lungo termine, piuttosto che al solo vantaggio tattico a breve termine.

Un'intuizione chiave di questo lavoro è che i futuri sistemi di comunicazione militare devono essere ecosistemi adattivi piuttosto che infrastrutture statiche. La natura dinamica dei conflitti moderni richiede sistemi in grado di riconfigurarsi in risposta alle mutevoli esigenze delle missioni, alle condizioni ambientali e ai vettori di minaccia. Questa adattabilità richiede una stretta integrazione tra tecnologie di comunicazione, meccanismi di sicurezza, sistemi di controllo intelligenti e decisori umani. Il successo dell' e di tali sistemi dipende non solo dall'eccellenza tecnica, ma anche dall'allineamento dottrinale e dalla preparazione organizzativa.

Un'altra conclusione importante è la crescente importanza dell'interoperabilità e delle operazioni di coalizione. Le missioni militari moderne sono sempre più condotte in contesti multinazionali, che richiedono sistemi di comunicazione che consentano la condivisione controllata delle informazioni, preservando al contempo gli interessi di sicurezza nazionale. La standardizzazione, i quadri di sicurezza condivisi e i meccanismi flessibili di controllo degli accessi sono essenziali per una collaborazione efficace. Le architetture di comunicazione che supportano l'interoperabilità fin dalla progettazione forniscono una base per la fiducia e la coerenza operativa tra le forze alleate.

Le dimensioni etiche e legali della tecnologia delle comunicazioni militari rappresentano un'area di responsabilità critica per progettisti, operatori e responsabili politici. Man mano che i sistemi di comunicazione diventano più autonomi e integrati con le funzioni di supporto decisionale, aumentano le potenziali conseguenze di guasti o usi impropri del sistema. L'integrazione di considerazioni etiche e di conformità legale nella progettazione del sistema garantisce che la superiorità tecnologica non comprometta la legittimità o la responsabilità. L'innovazione responsabile nelle comunicazioni militari deve bilanciare l'efficacia operativa con il rispetto delle norme e dei valori stabiliti.

Questo libro contribuisce al settore fornendo una prospettiva completa e integrata sui sistemi di comunicazione militare sicuri. Anziché concentrarsi su tecnologie isolate, enfatizza la coerenza architettonica, l'integrazione della sicurezza e la progettazione orientata al futuro. La combinazione di analisi teorica, considerazioni pratiche ed esame di casi di studio offre un quadro strutturato per la comprensione e lo sviluppo delle moderne infrastrutture di comunicazione militare.

Da un punto di vista accademico, questo lavoro fornisce una base per ulteriori ricerche sulle architetture di comunicazione adattive, la gestione delle reti basata sull'intelligenza artificiale e i sistemi quantistici sicuri. Da un punto di vista operativo, offre approfondimenti sulle sfide e le opportunità associate all'implementazione di tecnologie di comunicazione sicure in ambienti complessi. I concetti presentati possono informare lo sviluppo della dottrina, la progettazione dei sistemi e la formulazione delle politiche in tutte le istituzioni della difesa.

In conclusione, i sistemi di comunicazione militare sicuri sono un fattore decisivo nella guerra moderna e futura. Poiché le forze armate si trovano ad affrontare ambienti operativi sempre più complessi e contesi, la capacità di scambiare informazioni in modo sicuro, affidabile e intelligente rimarrà un imperativo strategico. Adottando quadri di comunicazione integrati, adattivi ed eticamente fondati, gli eserciti del futuro potranno raggiungere la superiorità informativa mantenendo al contempo la resilienza, la legittimità e l'efficacia operativa. Questo libro mira a contribuire a tale obiettivo offrendo un'analisi strutturata e lungimirante delle tecnologie, dell'architettura e dei principi dell' e che plasmeranno il futuro delle comunicazioni militari.

Riferimenti

1. Defence Strategic Communications, *Rivista ufficiale del Centro di eccellenza per le comunicazioni strategiche della NATO,* vol. 10, primavera-autunno 2021, NATO StratCom COE, Riga, Lettonia.
2. Polovic, J., "Challenges of Global Communication: Strategic Competition and Escalation of Tensions in International Relations" (Le *sfide della comunicazione globale*: competizione strategica ed escalation delle tensioni nelle relazioni internazionali)*, Raccolta di articoli della Facoltà di Filosofia*, vol. 48, n. 1, 2024, pagg. 51-57. https://doi.org/10.5671/ca.48.1.7
3. Mustafovski, R., "L'uso delle piattaforme di comunicazione nelle operazioni militari: migliorare l'efficacia strategica e tattica", *Database Systems Journal,* vol. XVI, 2025, Facoltà di Ingegneria Elettrica e Tecnologie dell'Informazione, Università Ss. Cirillo e Metodio, Skopje, Repubblica di Macedonia del Nord.
4. Rienzi, T. M., *Communications-Electronics 1962-1970,* Vietnam Studies Series, Dipartimento dell'Esercito, Washington, DC, USA, 2002.
5. Mazzenga, F., Landry, R. e Young, K., "Comunicazioni militari", *IEEE Communications Magazine,* ottobre 2020, pagg. 50-56.
6. Organizzazione del Trattato del Nord Atlantico (NATO), *Dottrina congiunta alleata per i sistemi di comunicazione e informazione (AJP-6),* Edizione B, Versione 1, Ufficio di standardizzazione della NATO (NSO), aprile 2024.
7. Dipartimento della Difesa degli Stati Uniti, *Strategia di modernizzazione C3: comando, controllo e comunicazioni,* Washington, DC, USA, settembre 2020.
8. Monteiro Marques, M., "STANAG 4586 - Interfacce standard del sistema di controllo UAV (UCS) per l'interoperabilità UAV della NATO", Documento tecnico NATO, Escola Naval - Afeite, Portogallo.
9. Yarnell, A. M., Dullea, C. e Grunberg, N. E., "Comunicazioni militari", in *Comunicazioni militari e mediche,* capitolo 11, Comando di ricerca e sviluppo medico dell'esercito degli Stati Uniti, USA.
10. Timofte, G., "Modernizzazione dei sistemi di comunicazione militare in base ai nuovi requisiti operativi, informativi e tecnici dello spazio di battaglia", *Bollettino scientifico dell'Accademia degli scienziati rumeni,* Bucarest, Romania.
11. Hayes, C., *Accordi di standardizzazione NATO (STANAG) per comandanti e personale,* Notizie dal fronte, Centro per le lezioni apprese dall'esercito (CALL), Esercito degli Stati Uniti, aprile 2019.
12. Sánchez, R., Evans, J. e Minden, G., "Networking on the Battlefield: Challenges in Highly Dynamic Multi-hop Wireless Networks" (Reti sul campo di battaglia: sfide nelle reti wireless multi-hop altamente dinamiche), *Atti del convegno IEEE MILCOM 1999,* Atlantic City, New Jersey, USA, ottobre 1999.

13. Kumar, D., "Challenges of a Digitised Battlefield" (Le sfide di un campo di battaglia digitalizzato), *Journal of the United Service Institution of India,* vol. CXLII, n. 590, ottobre-dicembre 2012.
14. Lipscomb, P., "The Evolution of Communications in the Military as it Relates to Leadership" (L'evoluzione delle comunicazioni nell'esercito in relazione alla leadership), *Studi integrati,* Documento n. 90, Murray State University, 2017. Disponibile all'indirizzo: https://digitalcommons.murraystate.edu/bis437/90
15. Amin, M. G., Lindsey, A. R., Zhao, L. e Zhang, Y., *Anti-Jamming Techniques for GPS Receivers,* Relazione tecnica finale AFRL-IF-RS-TR-2001-186, Air Force Research Laboratory, Rome Research Site, New York, USA, settembre 2001.
16. Bardis, N. G., Doukas, N. e Ntaikos, K., "Progettazione e sviluppo di una comunicazione militare sicura basata sul prototipo di algoritmo crittografico AES e su uno schema avanzato di gestione delle chiavi", *WSEAS Transactions on Information Science and Applications,* Università di Educazione Militare, Accademia dell'Esercito Ellenico, Grecia.
17. Colbeck, M. J. L., "Crittografia quantistica nelle comunicazioni militari", *Atti della conferenza EAAW,* 28-29 novembre 2023.
18. Evans, J., Sánchez, R. e Minden, G., "Networking sul campo di battaglia: sfide nelle reti wireless multi-hop altamente dinamiche", *Atti dell'IEEEMILCOM,* Atlantic City, New Jersey, USA, ottobre 1999.
19. Hayes, C., "Accordi di standardizzazione NATO (STANAG) per comandanti e personale", *Notizie dal fronte,* Centro per le lezioni apprese dall'esercito (CALL), aprile 2019.
20. Kang, J. S., "Independent Authentication Protocol in Tactical Network Environment Using Hash Lock Approach," *International Journal of Machine Learning and Computing,* Vol. 5, No. 5, ottobre 2015.
21. Kovács, L., "Electronic Warfare and the Asymmetric Challenges," *Bolyai Szemle,* n. 3, 2009, pp. 135-151, ISSN 1416-1443.
22. Kumar, D., "Challenges of a Digitised Battlefield" (Le sfide di un campo di battaglia digitalizzato), *Journal of the United Service Institution of India,* vol. CXLII, n. 590, ottobre-dicembre 2012.
23. Lipscomb, P., "The Evolution of Communications in the Military as it Relates to Leadership," *Integrated Studies,* n. 90, Murray State University, 2017.
24. Sayyed, S. Y., Gurap, S. L., Devadhe, J. L. e Gat, K. R., "Una rassegna sulla comunicazione wireless sicura per applicazioni militari", *International Journal of Electrical, Electronics and Data Communication,* vol. 5, n. 11, novembre 2017.
25. Shinde, V., Kulkarni, S. e Malekar, M. R., "Sistema di comunicazione sicuro", *Rivista internazionale delle innovazioni nella ricerca e nella tecnologia ingegneristica (IJIERT),* Atti della conferenza TECHNO-2K17.

26. Timofte, G., "Modernizzazione dei sistemi di comunicazione militari in base ai nuovi requisiti operativi, informativi e tecnici dello spazio di battaglia dell' ", Accademia delle scienze rumena, Bucarest, Romania.
27. Dipartimento dell'Esercito degli Stati Uniti, *Signal Communications Doctrine (FM 100-11),* Dipartimento dell'Esercito, Washington, DC, luglio 1948.
28. Alnifie, G. e Simon, R., "Una difesa multicanale contro gli attacchi di disturbo nelle reti di sensori wireless", in *Atti del 3° Workshop ACM su QoS e sicurezza per reti wireless e mobili,* 2007, pagg. 95-104.
29. Alnifie, G. e Simon, R., "MULEPRO: una risposta multicanale agli attacchi di disturbo nelle reti di sensori wireless", *Wireless Communications and Mobile Computing,* 2010.
30. Bayraktaroglu, E., King, C., Liu, X., Noubir, G., Rajaraman, R. e Thapa, B., "On the Performance of IEEE 802.11 Under Jamming" (Sulle prestazioni dello standard IEEE 802.11 in condizioni di interferenza), in *Atti della 27a conferenza IEEE sulle comunicazioni informatiche,* 2008, pagg. 1265-1273.
31. Bellardo, J. e Savage, S., "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions" (Attacchi Denial-of-Service 802.11: vulnerabilità reali e soluzioni pratiche), in *Atti del 12° Simposio sulla sicurezza USENIX,* 2003, pagg. 15-28.
32. Broustis, I., Pelechrinis, K., Syrivelis, D., Krishnamurthy, S. V., e Tassiulas, L., "FIJI: Fighting Implicit Jamming in 802.11 WLANs" (FIJI: lotta al jamming implicito *nelle reti WLAN 802.11*), *Security and Privacy in Communication Networks,* vol. 19, 2009, pagg. 21-40.
33. Chiang, J. T. e Hu, Y. C., "Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks," *IEEE/ACM Transactions on Networking,* Vol. 19, No. 1, 2011, pp. 286-298.
34. Commander, C. W., Pardalos, P. M., Ryabchenko, V., Shylo, O. V, Uryasev, S. e Zrazhevsky, G., "Jamming Communication Networks Under Complete Uncertainty," *Optimization Letters*, Vol. 2, No. 1, 2008, pp. 53-70.
35. Gencer, C., Aydogan, E. K. e Celik, C., "A Decision Support System for Locating VHF/UHF Radio Jammer Systems on the Terrain" (Un sistema di supporto decisionale per localizzare i sistemi di disturbo radio VHF/UHF sul terreno)*, Information Systems Frontiers,* vol. 10, n. 1, 2008, pagg. 111-124.
36. Gummadi, R., Wetherall, D., Greenstein, B. e Seshan, S., "Comprensione e mitigazione dell'impatto delle interferenze RF sulle reti 802.11", in *Atti della conferenza ACM SIGCOMM su applicazioni, tecnologie, architetture e protocolli per le comunicazioni informatiche,* 2007, pagg. 385-396.
37. Huang, H., Ahmed, N. e Pulluru, S., "On Limited Range Strategic and Random Jamming Attacks in Wireless Ad Hoc Networks" (Attacchi di disturbo strategici e casuali a portata limitata nelle reti wireless ad hoc), in *Atti della 34a*

conferenza IEEE sulle reti informatiche locali, 2010, pagg. 1-8.
38. Jain, S. K. e Garg, K., "A Hybrid Model of Defense Techniques Against Base Station Jamming Attack in Wireless Sensor Networks" (Un modello ibrido *di tecniche di difesa contro gli attacchi di disturbo alle stazioni base nelle reti di sensori wireless*), in *Atti della prima conferenza internazionale sull'intelligenza computazionale, i sistemi di comunicazione e le reti*, 2009, pagg. 102-107.
39. Kerkez, B., Watteyne, T., Magliocco, M., Glaser, S. e Pister, K., " " in *Atti della quarta conferenza internazionale ICST sulle metodologie e gli strumenti di valutazione delle prestazioni*, 2009, pp. 76:1-76:6.
40. Khattab, S., Mosse, D. e Melhem, R., "Jamming Mitigation in Multi-Radio Wireless Networks: Reactive or Proactive?" in *Atti della quarta conferenza internazionale sulla sicurezza e la privacy nelle reti di comunicazione,* 2008, pagg. 27:1-27:10.
41. Khattab, S., Mosse, D. e Melhem, R., "Modellizzazione della difesa anti-interferenza con salto di canale nelle reti wireless multi-radio", in *Atti della 5a Conferenza internazionale annuale sui sistemi mobili e ubiquiti: informatica, reti e servizi,* 2008, pagg. 25:1-25:10.
42. Lazos, L., Liu, S. e Krunz, M., "Mitigating Control Channel Jamming Attacks in MultiChannel Ad Hoc Networks" (Mitigazione degli attacchi di disturbo del canale di controllo nelle reti ad hoc multicanale), in *Atti della 2a Conferenza ACM sulla sicurezza delle reti wireless*, 2009, pagg. 169-180.
43. Li, M., Koutsopoulos, I. e Poovendran, R., "Attacchi di interferenza ottimali e politiche di difesa della rete nelle reti di sensori wireless", in *Atti della 26a Conferenza internazionale IEEE sulla comunicazione informatica,* 2007, pagg. 1307-1315.
44. Liu, H., Liu, Z., Chen, Y. e Xu, W., "Determining the Position of a Jammer Using a Virtual-Force Iterative Approach," *Wireless Networks,* Vol. 17, No. 2, 2011, pp. 531-547.
45. Liu, Z., Liu, H., Xu, W. e Chen, Y., "Sfruttamento dei cambiamenti dei vicini causati dal jamming per la localizzazione del jammer", *IEEE Transactions on Parallel and Distributed Systems,* 2011.
46. Misra, S., Singh, R. e Mohan, S. V. R., "Meccanismo di rilevamento degli attacchi di interferenza degni di una guerra informatica per reti di sensori wireless utilizzando un sistema di inferenza fuzzy"*, Sensors,* vol. 10, 2010, pagg. 3444-3479.
47. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C. e Pantziou, G., "A Survey on Jamming Attacks and Countermeasures in Wireless Sensor Networks" (Indagine sugli attacchi di interferenza e sulle contromisure nelle reti di sensori wireless), *IEEE Communications Surveys and Tutorials*, vol. 11, n. 4, 2009, pagg. 42-56.

48. Muraleedharan, R., e Osadciw, L. A., "Rilevamento degli attacchi di jamming e contromisure nelle reti di sensori wireless utilizzando il sistema Ant", in *Atti della SPIE - The International Society for Optical Engineering,* Vol. 6248, 2006, Articolo 62480G.

49. Navda, V, Bohra, A., Ganguly, S., e Rubenstein, D., "Utilizzo del channel hopping per aumentare la resilienza dello standard 802.11 agli attacchi di jamming", in *Atti della 26a Conferenza internazionale IEEE sulle comunicazioni informatiche*, 2007, pagg. 2526-2530.

50. Panyim, K., Hayajneh, T., Krishnamurthy, P. e Tipper, D., "Jamming Dust: A Low Power Distributed Jammer Network" (Polvere di disturbo: una rete di disturbatori distribuiti a bassa potenza), in *Atti della 27a Conferenza scientifica dell'esercito dell'* , 2009, pagg. 922-929.

51. Pelechrinis, K., Koufogiannakis, C. e Krishnamurthy, S. V., "Gaming the Jammer: Is Frequency Hopping Effective?" in *Atti della 7a Conferenza internazionale sulla modellizzazione e l'ottimizzazione nelle reti mobili, ad hoc e wireless,* 2009, pp. 187-196.

52. Pelechrinis, K., Koutsopoulos, I., Broustis, I. e Krishnamurthy, S. V., "Localizzazione leggera dei disturbatori nelle reti wireless: progettazione e implementazione del sistema", in *Atti della Conferenza globale sulle telecomunicazioni IEEE,* 2009, pagg. 1-6.

53. Pelechrinis, K., Iliofotou, M. e Krishnamurthy, S. V., "Denial of Service Attacks in Wireless Networks: The Case of Jammers" (Attacchi Denial of Service nelle reti wireless: il caso dei disturbatori)*, IEEE Communications Surveys and Tutorials,* vol. 13, n. 2, 2011, pagg. 245-257.

54. Shin, I., Shen, Y., Xuan, Y., Thai, M. T. e Znati, T., "Attacchi di disturbo reattivi nelle reti di sensori wireless multiradio: una misura di mitigazione efficiente attraverso l'identificazione dei nodi trigger", in *Atti del 2° Workshop internazionale ACM sui fondamenti delle reti e del computing wireless ad hoc e dei sensori,* 2009, pagg. 87-96.

55. Strasser, M., Danev, B. e Capkun, S., "Detection of Reactive Jamming in Sensor Networks" (Rilevamento del jamming reattivo nelle reti di sensori), *ACM Transactions on Sensor Networks*, vol. 7, n. 2, 2010, articolo 16.

56. Sun, Y. e Wang, X., "Jammer Localization in Wireless Sensor Networks" (Localizzazione dei disturbatori nelle reti di sensori *wireless*), in *Atti della 5a Conferenza internazionale sulle comunicazioni wireless, le reti e il mobile computing,* 2009, pagg. 1-4.

57. Tague, P., Slater, D., Poovendran, R. e Noubir, G., "Linear Programming Models for Jamming Attacks on Network Traffic Flows" (Modelli di programmazione lineare per attacchi di jamming sui flussi di traffico di rete), in *Atti del 6° Simposio internazionale sulla modellizzazione e l'ottimizzazione nelle reti*

mobili, ad hoc e wireless e workshop, 2008, pagg. 207-216.
58. Thamilarasu, G. e Sridhar, R., "Modellizzazione basata sulla teoria dei giochi degli attacchi di jamming nelle reti ad hoc", in *Atti della 18a Conferenza internazionale sulle comunicazioni e le reti informatiche*, 2009, pagg. 1-6.
59. Wang, H., Zhang, L., Li, T. e Tugnait, J., "Mitigazione dello jamming efficiente dal punto di vista spettrale basata sul salto di frequenza controllato dal codice"*, IEEE Transactions on Wireless Communications,* vol. 10, n. 3, 2011, pagg. 728-732.
60. Wilhelm, M., Martinovic, I., Schmitt, J. B. e Lenders, V., "Reactive Jamming in Wireless Networks: How Realistic Is the Threat?" (Interferenze reattive nelle reti *wireless: quanto è realistica la minaccia*?) in *Atti della quarta conferenza ACM sulla sicurezza delle reti wireless,* 2011, pagg. 47-52.
61. Wood, A., Stankovic, J. e Son, S., "JAM: A Jammed-Area Mapping Service for Sensor Networks," in *Atti del 24° Simposio IEEE sui sistemi in tempo reale,* 2003, pp. 286-297.
62. Wood, A., Stankovic, J. e Zhou, G., "DEEJAM: sconfiggere il jamming efficiente in termini di energia e di larghezza di banda (Energy-) nelle reti wireless basate su IEEE 802.15.4", in *Atti della quarta conferenza annuale della IEEE Communications Society sulle comunicazioni e le reti di sensori, mesh e ad hoc*, 2007, pagg. 60-69.
63. Xu, W., Wood, T., Trappe, W. e Zhang, Y., "Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service" (Navigazione tra i canali e ritirate spaziali: difese contro il denial of service wireless), in *Atti del 3° Workshop ACM sulla sicurezza wireless*, 2004, pagg. 80-89.
64. Xu, W., Trappe, W., Zhang, Y. e Wood, T., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks" (La fattibilità di lanciare e rilevare attacchi di disturbo nelle reti wireless), in *Atti del 6° Simposio internazionale ACM sul Mobile AdHoc Networking and Computing,* 2005, pagg. 46-57.
65. Yoon, S. U., Murawski, R., Ekici, E., Park, S. e Mir, Z., "Adaptive Channel Hopping for Interference-Robust Wireless Sensor Networks" (Salto di canale adattivo per reti di sensori wireless resistenti alle interferenze), in *Atti della Conferenza internazionale IEEE sulle comunicazioni*, 2010, pagg. 1-5.
66. Stato Maggiore dell'Esercito Italiano - Ufficio Sicurezza, *Sistemi Software, Telecomunicazioni e Sicurezza - Documenti non classificati,* Roma, Italia, 2008.
67. Stato Maggiore dell'Esercito Italiano - Ufficio Sicurezza, *Sistemi Software, Telecomunicazioni e Sicurezza - Documenti Classificati,* Roma, Italia, 2008.
68. ISO/IEC 15408-1, *Tecnologia dell'informazione - Tecniche di sicurezza - Criteri di valutazione per la sicurezza IT - Parte 1: Introduzione e modello generale,* Organizzazione internazionale per la normazione, Ginevra, 2009.

69. ISO/IEC 15408-2, *Tecnologia dell'informazione - Tecniche di sicurezza - Criteri di valutazione per la sicurezza IT - Parte 2: Componenti funzionali di sicurezza,* Organizzazione internazionale per la normazione, Ginevra, 2008.
70. ISO/IEC 15408-3, *Tecnologia dell'informazione - Tecniche di sicurezza - Criteri di valutazione per la sicurezza IT - Parte 3: Componenti di garanzia della sicurezza,* Organizzazione internazionale per la normazione, Ginevra, 2008.
71. Dipartimento della Difesa degli Stati Uniti, *Criteri di valutazione dei sistemi informatici affidabili,* DoDD 5200.28-STD, Washington, DC, dicembre 1985.
72. Dipartimento della Difesa degli Stati Uniti, *Direttiva: Garanzia delle informazioni,* DoDD 8500.01E, Washington, DC, ottobre 2002.
73. Bundesamt für Sicherheit in der Informationstechnik, *Note applicative e interpretazione dello schema (AIS): mappatura ITSEC ai criteri comuni con potenziale di attacco specifico,* Bonn, Germania, 2010. Disponibile online: https://www.bsi.bund.de
74. ISO/IEC 27000, *Tecnologia dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Panoramica e vocabolario,* Organizzazione internazionale per la normazione, Ginevra, 2009.
75. Hare, F., "La minaccia informatica alla sicurezza nazionale: perché non riusciamo a trovare un accordo", in *Atti della conferenza sui conflitti informatici,* Tallinn, Estonia, 2010, pagg. 211-225.
76. Liles, S., "Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency" (La guerra informatica: una forma di conflitto a bassa intensità e di insurrezione), in *Atti della conferenza sui conflitti informatici*, Tallinn, Estonia, 2010, pagg. 47-57.
77. Kotenko, I. V., "Multi-Agent Modeling and Simulation of Cyber-Attacks and Cyber Defense for Homeland Security," in *Atti del Workshop internazionale IEEE sull'acquisizione intelligente dei dati e i sistemi informatici avanzati: tecnologia e applicazioni,* Dortmund, Germania, 6-8 settembre 2008.
78. Kotenko, I. V. e Ulanov, A. V., "Simulazione basata su agenti di attacchi DDoS e meccanismi di difesa"*, Journal of Computing,* vol. 4, n. 2, 2005.
79. Gasser, L., "Crittografia post-quantistica", in V. Mulder, A. Mermoud, V. Lenders e B. Tellenbach (a cura di), *Trends in Data Protection and Encryption Technologies,* Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33386-6grafo 10
80. Radanliev, P., "Artificial Intelligence and Quantum Cryptography" (Intelligenza artificiale e crittografia quantistica), *Journal of Analytical Science and Technology,* vol. 15, articolo 4, 2024. https://doi.org/10.1186/s40543-024- 00416-6
81. Atutxa, A., Sanz, A., Sasiain, J., Astorga, J. e Jacob, E., "Verso un 5G quantistico sicuro: distribuzione quantistica delle chiavi nelle reti centrali",

Computer Communications, vol. 224, 2024, pagg. 145-158. https://doi.org/10.1016Zj.comcom.2024.06.005

82. Ricci, S., Dobias, P., Malina, L., Hajny, J. e Jedlicka, P., "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography" (Chiavi ibride nella pratica: combinazione di crittografia classica, quantistica e post-quantistica)*, IEEE Access,* vol. 12, 2024, pagg. 23206-23219. https://doi.org/10.1109/ACCESS.2024.3364520

83. Shim, K.-S., Kim, B. e Lee, W., "Ricerca sui protocolli applicati alle chiavi quantistiche, alle chiavi di distribuzione e alle chiavi di crittografia post-quantistica per la scienza dei dati e la sicurezza web"*, Journal of Web Engineering,* vol. 23, n. 6, settembre 2024, pagg. 813-830. https://doi.org/10.13052/jwe1540-9589.2365

84. Dhar, S., Khare, A., Dwivedi, A. D. e Singh, R., "Protezione dei dispositivi IoT: un approccio innovativo che utilizza la blockchain e la crittografia quantistica", *Internet of Things,* vol. 25, 2024, articolo 101019. https:ZZdoi.org/10.1016Zj.iot.2023.101019

85. Schneier, B., "Lattice-Based Cryptosystems and Quantum Cryptanalysis" (Crittografia basata su reticoli e crittanalisi quantistica)*, Communications of the ACM,* Online First, giugno 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" (Migliorare la crittografia *quantistica con sorgenti di fotoni singoli a punti quantici*)*, npj Quantum Information,* vol. 8, articolo 104, 2022. https://doi.org/10.1038/s41534-022-00626-z

87. Akçay, L., e Yalçın, B. Ö., "Progettazione ASIP leggera per algoritmi di crittografia post-quantistica basati su reticoli ( )", *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., "Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective" (La sicurezza informatica nelle infrastrutture critiche: una prospettiva di crittografia post-quantistica)*, IEEE Internet of Things Journal,* vol. 11, n. 18, 15 settembre 2024, pagg. 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" (Sicurezza del livello di trasporto resistente alla crittografia quantistica), *Computer Communications*, vol. 213, 2024, pagg. 345-358.
https://doi.org/10.1016/j.comcom.2023.11.010

90. Alhakami, H., "Enhancing IoT Security: Quantum-Level Resilience Against Threats" (Migliorare la sicurezza dell'IoT: resilienza a livello quantistico

contro le minacce)*, Computers, Materials and Continua,* vol. 78, n. 1, 2024, pagg. 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" (Indagine sul *quantum computing per la sicurezza dell'Internet delle cose)*, *Procedia Computer Science*, vol. 218, 2023, pagg. 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" (Implementazione della crittografia post-quantistica per sviluppatori), *SN Computer Science*, vol. 4, articolo 365, 2023. https://doi.org/10.1007/s42979-023-01724-1
93. Ji, X., Wang, B., Hu, F., Wang, C. e Zhang, H., "Nuova architettura di calcolo avanzata
per la progettazione e l'analisi della crittografia con D-Wave Quantum Annealer", *Tsinghua Science and Technology,* vol. 27, n. 4, agosto 2022, pagg. 751-759. https://doi.org/10.26599/TST.2021.9010022
94. Hasan, K. F., et al., "Un quadro di riferimento per la migrazione alla crittografia post-quantistica: analisi della dipendenza dalla sicurezza e casi di studio", *IEEE Access,* vol. 12, 2024, pagg. 23427-23450. https://doi.org/10.1109/ACCESS.2024.3360412
95. Kong, I., Janssen, M. e Bharosa, N., "Realizzare una condivisione delle informazioni sicura dal punto di vista quantistico: sfide di implementazione e adozione e raccomandazioni politiche per transizioni sicure dal punto di vista quantistico"*, Government Information Quarterly,* vol. 41, n. 1, 2024, articolo 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" (Esplorazione della crittografia post-quantistica con distribuzione quantistica delle chiavi per la progettazione di architetture di rete mobile sostenibili), in *Atti del 4° Workshop su prestazioni ed efficienza energetica dell' e nei sistemi concorrenti e distribuiti (PECS '24),* ACM, New York, 2024, pagg. 9-16. https://doi.org/10.1145/3659997.3660033
98. Piatkowski, J. e Szymoniak, S., "Trivializing Verification of Cryptographic Protocols" (Semplificazione della verifica dei protocolli crittografici), *Computer Assisted Methods in Engineering and Science*, vol. 30, n. 4, 2023, pagg. 389-406. https://doi.org/10.24423/cames.869
99. Basin, D. A., Cremers, C. e Meadows, C. A., "Model Checking Security Protocols" (Verifica dei modelli dei protocolli di sicurezza), in E. Clarke, T.

Henzinger, H. Veith e R. Bloem (a cura di), *Handbook of Model Checking (Manuale di verifica dei modelli),* Springer, Cham, 2018, pagg. 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, Nos. 12, 2016, pp. 1-135. https://doi.org/10.1561/3300000004

101. Blanchet, B., Cheval, V. e Cortier, V., "ProVerif con lemmi, induzione, sottoscrizione veloce e molto altro", in *Atti del Simposio IEEE sulla sicurezza e la privacy (S&P 2022),* IEEE Computer Society, San Francisco, CA, 2022, pp. 205-222. https://hal.inria.fr/hal-03366962/

102. Bouroulet, R., Devillers, R., Klaudel, H., Pelz, E. e Pommereau, F., "Modellizzazione e analisi dei protocolli di sicurezza utilizzando specifiche basate sui ruoli e reti di Petri", in K. M. van Hee e R. Valk (a cura di), *Applicazioni e teoria delle reti di Petri,* Springer, Berlino e Heidelberg, 2008, pp. 72-91.

103. Burrows, M., Abadi, M. e Needham, R., "Una logica di autenticazione", *ACM*
Transactions on Computer Systems, vol. 8, n. 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," in *Proceedings of the Workshop on Specification and Automated Processing of Security Requirements (SAPS 2004),* Austrian Computer Society, Linz, Austria, 2004, p. 13.

105. Cortier, V., Delaune, S., e Dreier, J., "Generazione automatica di lemmi sorgente in Tamarin: verso prove automatiche dei protocolli di sicurezza", in L. Chen, N. Li, K. Liang e S. Schneider (a cura di), *Computer Security - ESORICS 2020,* Springer, Cham, 2020, pp. 3-22.

106. David, A., Larsen, K. G., Legay, A., Mikucionis, M. e Poulsen, D. B., "UPPAAL SMC Tutorial"*, International Journal on Software Tools for Technology Transfer,* vol. 17, n. 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", in *Atti del 22° Simposio annuale sui fondamenti dell'informatica (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., " " (Concetti: supporto linguistico per la programmazione generica in C++)*, ACM SIGPLAN Notices,* vol. 41, n. 10, 2006, pagg. 291-310. https://doi.org/10.1145/1167515.1167499

109. Grosser, A., Kurkowski, M., Piatkowski, J. e Szymoniak, S., "ProToc: un linguaggio universale per le specifiche dei protocolli di sicurezza", in A. Wilinski, I. E. Fray e J. Pejas (a cura di), *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., "A Typing Result for Stateful Protocols," in *Atti del 31° Simposio IEEE sulle basi della sicurezza informatica (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., "Algorithm 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., "Intrusi pigri multipli indipendenti", in *Atti del 1° Workshop sulle questioni calde in materia di principi di sicurezza e fiducia (HotSpot 2013)*, 2013, 15 pagine.
114. Kordy, B., Mauw, S., Radomirovic, S. e Schweitzer, P., "Foundations of AttackDefense Trees" (Fondamenti degli alberi di difesa dagli attacchi), in P. Degano, S. Etalle e J. Guttman (a cura di), *Formal Aspects in Security and Trust (FAST 2010),* Lecture Notes in Computer Science, Vol. 6561, Springer, Berlino e Heidelberg, 2010, pagg. 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, USA, 1998.
116. Kurkowski, M., *Metodi formali per la verifica delle proprietà dei protocolli di sicurezza nelle reti informatiche* (in polacco), Akademicka Oficyna Wydawnicza Exit, Varsavia, 2013.
117. Liang, J., Nguyen, Q., Simoff, S., Huang, M., "Divide and Conquer Treemaps: Visualizzazione di alberi di grandi dimensioni con forme diverse", *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," *IEEE Transactions on Visualization and Computer Graphics,* Vol. 24, No. 1, 2017, pp. 163-173. https://doi.org/10.1109/TVCG.2017.2744378
119. Mauw, S. e Oostdijk, M., "Fondamenti degli alberi di attacco", in *Conferenza internazionale sulla sicurezza delle informazioni e la crittografia,* Springer, 2005, pp. 186-198. https://doi.org/10.1007/11734727_17
120. Millen, J. K., "CAPSL: Common Authentication Protocol Specification Language" (Linguaggio di specifica del protocollo di autenticazione comune), in *Atti del Workshop sui nuovi paradigmi di sicurezza (NSPW '96),* 1996. https://doi.org/10.1145/304851.304879
121. Morin, P., *Open Data Structures (in C++),* 2013.

https://opendatastructures.org/
122. Modersheim, S., Nielson, F. e Nielson, H. R., "Lazy Mobile Intruders", in D. A. Basin e J. C. Mitchell (a cura di), *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, n. 12, 1978, pp. 993-999. https://doi.org/10.1145/359657.359659
124. Neuman, B. C. e Ts'o, T., "Kerberos: An Authentication Service for Computer Networks" (Kerberos: un servizio di autenticazione per reti informatiche), *IEEE Communications Magazine*, vol. 32, n. 9, 1994, pagg. 33-38. https://doi.org/10.1109/35.312841
125. Piatkowski, J., "The Conditional Multiway Mapped Tree: Modeling and Analysis of Hierarchical Data Dependencies," *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, Londra, 2000.
127. Siedlecka-Lamch, O., Szymoniak, S. e Kurkowski, M., "A Fast Method for Security Protocols Verification," in *Atti della 18a Conferenza internazionale sui sistemi informatici e la gestione industriale (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" (Verso il metodo più efficiente per la verifica dei protocolli di sicurezza non temporizzati), in *Atti della 24a Conferenza dell'Asia Pacifico sui sistemi informativi (PACIS 2020),* Dubai, Emirati Arabi Uniti, 2020, p. 189.
129. Siek, J. G. e Lumsdaine, A., "A Language for Generic Programming in the Large" (Un linguaggio per la programmazione generica su larga scala)*, Science of Computer Programming,* vol. 76, n. 5, 2011, pagg. 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, pagg. 73-81.
https://doi.org/10.1016/j.comcom.2021.07.030
131. Szymoniak, S., Kurkowski, M. e Piatkowski, J., "Modelli temporizzati di protocolli di sicurezza
che includono ritardi nella rete", *Journal of Applied Mathematics and Computational Mechanics,* vol. 14, n. 3, 2015, pagg. 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, 2a ed., McGraw-Hill, Auckland, 1984.
133. Witten, I. H., Frank, E. e Hall, M. A., *Data Mining: Practical Machine Learning Tools and Techniques,* 3a ed., Morgan Kaufmann, Amsterdam, 2011.
134. R. Mustafovski, A. Petrovski e M. Radovanovic, "Integrazione delle tecnologie quantistiche nei sistemi militari mobili e nei framework TOC"*, Land Forces Academy Review,* vol. XXX, n. 3(119), 2025.
135. R. Mustafovski, "Formula-based architectural framework of the SecuDroneComm platform for unmanned aerial vehicle communications" (Struttura architettonica basata su formule della piattaforma SecuDroneComm per le comunicazioni dei veicoli aerei senza pilota), *Management Science Advances*, vol. 2, n. 1, pagg. 288-303, Scientific Oasis, Skopje, Repubblica di Macedonia del Nord, 2025.
136. R. Mustafovski, "Valutazione dell'impatto operativo di SecuDroneComm: valutazione basata su simulazione delle comunicazioni sicure degli UAV in ambienti militari", *Scientific Technical Review,* vol. 75, n. 1, pp. 11-18, 2025, doi: 10.5937/str2500002M.
137. M. Mozaffari, W. Saad, M. Bennis e M. Debbah, "Efficient deployment of multiple unmanned aerial vehicles for optimal wireless coverage" (Implementazione efficiente di più veicoli aerei senza pilota per una copertura wireless ottimale)*, IEEE Communications Letters,* vol. 20, n. 8, pagg. 1647-1650, 2016.
138. L. Ruan et al., "Implementazione efficiente dal punto di vista energetico della copertura multi-UAV nelle reti UAV: un quadro teorico di gioco", *China Communications,* vol. 15, n. 10, pagg. 194209, 2018.
139. M. Mozaffari, W. Saad, M. Bennis e M. Debbah, "Veicoli aerei senza pilota (UAV) mobili per comunicazioni Internet of Things efficienti dal punto di vista energetico", *IEEE Transactions on Wireless Communications*, 2017.
140. S.-Y Lien, K.-C. Chen e Y. Lin, "Verso accessi massicci e ubiquiti nelle comunicazioni machine-to-machine 3GPP", *IEEE Communications Magazine*, vol. 49, n. 4, pagg. 66-74, aprile 2011.
141. M. Malik e S. K. Garg, "Verso il 6G: l'evoluzione della rete oltre il 5G e lo scenario indiano", in *Proc. 2nd Int. Conf. Innovative Practices in Technology and Management (ICIPTM)*, Gautam Buddha Nagar, India, pp. 123-127, 2022.
142. M. A. Khan et al., "Sciame di UAV per la gestione della rete nel 6G: una revisione tecnica", *IEEE Transactions on Network and Service Management,* vol. 20, n. 1, pp. 741761, marzo 2023.
143. S. Dang, O. Amin, B. Shihada e M.-S. Alouini, "What should 6G be?" *Nature Electronics,* vol. 3, n. 1, pp. 20-29, 2020.
144. F. Ronaldo, D. Pramadihanto e A. Sudarsono, "Sistema di comunicazione sicuro per servizi con droni che utilizza crittografia ibrida su rete 4G/LTE", in *Proc.*

Int. Electronics Symposium (IES), Surabaya, Indonesia, pp. 116-122, 2020.
145. T. Li et al., "Comunicazioni sicure tra UAV e veicoli", *IEEE Transactions on Communications*, vol. 69, n. 8, pagg. 5381-5393, agosto 2021.
146. S. A. Ayati e H. R. Naji, "Un meccanismo sicuro per proteggere le comunicazioni UAV", in *Proc. 9° Congresso congiunto iraniano sui sistemi fuzzy e intelligenti (CFIS),* Bam, Iran, pp. 1-6, 2022.
147. D. Pirker, T. Fischer, C. Lesjak e C. Steger, "Sistema di autenticazione UAV globale e sicuro basato sulla sicurezza hardware", in *Proc. 8° IEEE Int. Conf. Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, Oxford, Regno Unito, pp. 84-89, 2020.
148. H. Wang, H. Fang e X. Wang, "Autenticazione decentralizzata soft abilitata dall'intelligenza periferica in uno sciame di UAV", in *Proc. IEEE/CIC Int. Conf. Communications in China (ICCC)*, Xiamen, Cina, pp. 86-91, 2021.
149. M. Markowski, P. Ryba e K. Puchala, "Laboratorio di ricerca sulle reti definite dal software: topologie e scenari sperimentali", in *Proc. 3rd European Network Intelligence Conf. (ENIC),* Breslavia, Polonia, pp. 252-256, 2016.
150. M. A. B. S. Abir, M. Z. Chowdhury e Y. M. Jang, "Reti UAV definite dal software per sistemi 6G: requisiti, opportunità, tecniche emergenti, sfide e direzioni di ricerca", *IEEE Open Journal of the Communications Society,* vol. 4, pp. 2487-2547, 2023.
151. M. Ouadah e F. Merazka, "Un approccio di codifica di rete per reti UAV affidabili basate su SDN", in *Proc. 5th Int. Conf. Electrical Engineering and Control Applications (ICEECA '22),* Khenchela, Algeria, 2022.

Biografia di Rexhep Mustafovski, MSc

Rexhep Mustafovski, MSc, è un ufficiale del Ministero della Difesa della Repubblica di Macedonia del Nord e assistente didattico e di ricerca presso l'Accademia Militare "Generale Mihailo Apostolski" di Skopje, dove presta servizio presso il Dipartimento per la sicurezza informatica e la digital forensics. È specializzato in sistemi di comunicazione sicuri, sicurezza informatica e integrazione delle tecnologie di difesa, con esperienza accademica e professionale che spazia dalle comunicazioni tattiche sicure alla sicurezza delle reti e ai sistemi informativi emergenti.

Ha completato la sua formazione universitaria presso l'Accademia Militare "Generale Mihailo Apostolski" di Skopje, dove si è laureato come ufficiale delle trasmissioni. Durante i suoi studi, ha dimostrato eccezionali risultati accademici e disciplina professionale, raggiungendo il massimo successo formativo della sua generazione. In riconoscimento di questo risultato, è stato ufficialmente premiato come miglior ufficiale della sua generazione, un onore conferitogli dal Presidente del Paese. Questo riconoscimento riflette sia la sua eccellenza accademica che il suo impegno nella professionalità militare.

Dopo la nomina, ha continuato il suo percorso accademico proseguendo gli studi universitari presso la Facoltà di Ingegneria Elettrica e Tecnologie dell'Informazione dell'Università "Ss. Cirillo e Metodio" di Skopje. Ha conseguito il Master of Science in Tecnologie della Comunicazione e dell'Informazione, specializzandosi in sistemi di comunicazione moderni, sicurezza delle informazioni e concetti avanzati di networking. I suoi studi di master hanno ulteriormente rafforzato le sue capacità analitiche e di ricerca, in particolare nei settori delle comunicazioni sicure e dei sistemi di difesa basati sulla tecnologia.

Il suo percorso accademico e professionale combina una formazione militare formale con studi avanzati di ingegneria, fornendo una solida base per la ricerca e il lavoro pratico nel campo delle comunicazioni militari sicure. Questo background

influenza il suo approccio alla progettazione di sistemi di comunicazione, ponendo l'accento su affidabilità, sicurezza, interoperabilità dell' e e rilevanza operativa. Le conoscenze e l'esperienza acquisite sia attraverso l'addestramento militare che la formazione ingegneristica sono alla base delle prospettive presentate in questo libro.