Bezpieczne systemy komunikacji dla nowoczesnych operacji wojskowych

Książka ta oferuje kompleksową analizę bezpiecznych systemów łączności dla współczesnych operacji wojskowych, odnosząc się do technologicznych i operacyjnych wyzwań związanych z wymianą informacji na współczesnych i przyszłych polach bitew. Śledzi ewolucję komunikacji wojskowej od systemów analogowych i cyfrowych po szyfrowane, definiowane programowo i wspomagane sztuczną inteligencją architektury, z naciskiem na interoperacyjność NATO, zagrożenia cyberbezpieczeństwa i wojnę elektroniczną. Analizowane są podstawowe zasady, takie jak transmisja sygnału, szyfrowanie, uwierzytelnianie, techniki przeciwzakłóceniowe i odporne taktyczne sieci radiowe. Zaawansowane tematy obejmują bezpieczną komunikację UAV z centrum dowodzenia, routing oparty na sztucznej inteligencji i zarządzanie widmem, systemy satelitarne, zastosowania wojskowe 5G/6G, komunikację kwantową i kognitywne sieci radiowe. Książka proponuje również przyszłościowe ramy bezpiecznej komunikacji zintegrowane z systemami C4ISR, poparte praktycznymi studiami przypadków, w tym badaniami doktoranckimi autora. Przeznaczona jest dla naukowców, specjalistów wojskowych, inżynierów i decydentów poszukujących odpornych i inteligentnych rozwiązań komunikacyjnych w dziedzinie obronności.

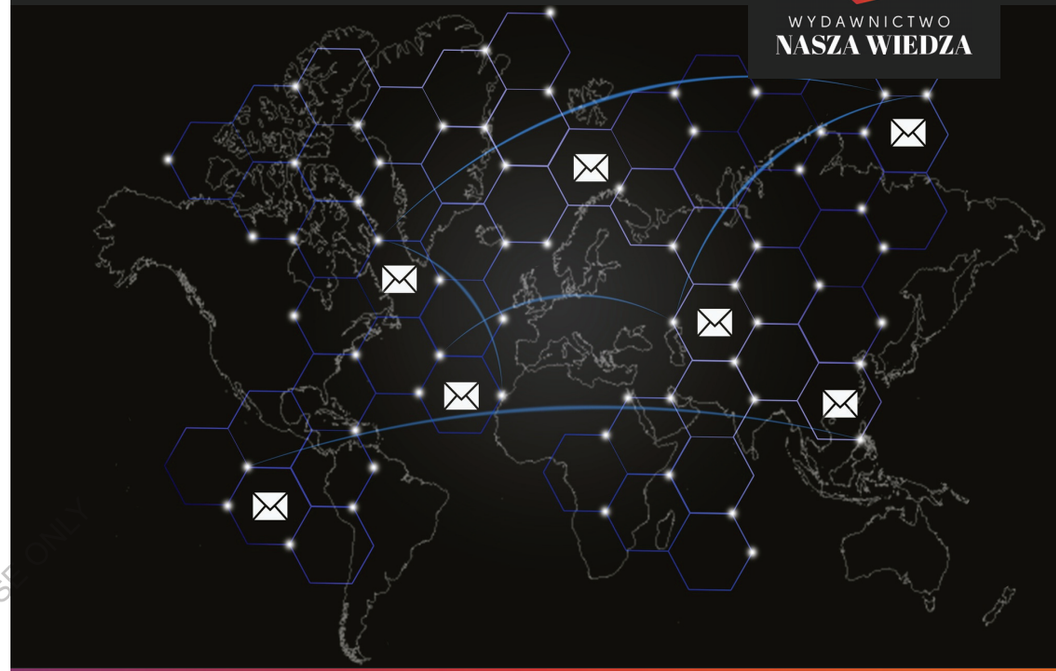
Rexhep Mustafovski, MSc, jest oficerem sygnałowym i badaczem komunikacji wojskowej. Posiada tytuł licencjata Akademii Wojskowej "Generał Mihailo Apostolski" w Skopje oraz tytuł magistra technologii komunikacyjnych i informacyjnych Uniwersytetu "Ss. Cyryla i Metodego".

9 786209 578120

WYDAWNICTWO
NASZA WIEDZA

Rexhep Mustafovski

WYDAWNICTWO
NASZA WIEDZA



Bezpieczne systemy komunikacji dla nowoczesnych operacji wojskowych

Podstawy, technologie i przyszłe kierunki

Rexhep Mustafovski

Rexhep Mustafovski

Bezpieczne systemy komunikacji dla nowoczesnych operacji wojskowych

Rexhep Mustafovski

Bezpieczne systemy komunikacji dla nowoczesnych operacji wojskowych

Podstawy, technologie i przyszłe kierunki

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: 978-620-9-57812-0

Bezpieczne systemy komunikacyjne dla współczesnych operacji wojskowych: podstawy, technologie i kierunki rozwoju w przyszłości

Spis treści

Przedmowa

Nazywam się Rexhep Mustafovski, jestem magistrem nauk ścisłych, a niniejsza książka jest wynikiem mojego zaangażowania akademickiego, zawodowego i badawczego w dziedzinie nowoczesnych systemów komunikacyjnych, ze szczególnym uwzględnieniem bezpiecznych zastosowań wojskowych i obronnych. Motywacją do napisania tej książki jest rosnące znaczenie zaawansowanych technologii w kształtowaniu współczesnego społeczeństwa, a dokładniej w transformacji sposobu komunikacji, koordynacji i działania sił zbrojnych w złożonych i spornych środowiskach.

W dzisiejszym świecie technologia nie jest już elementem peryferyjnym działalności ludzkiej, ale głównym motorem zmian w dziedzinie gospodarki, społeczeństwa i bezpieczeństwa. W szczególności technologie komunikacyjne stały się fundamentalnym elementem generowania, przekazywania, ochrony i wykorzystywania informacji. W kontekście wojskowym bezpieczna komunikacja jest nie tylko wymogiem technicznym, ale także strategiczną koniecznością. Możliwość bezpiecznej, niezawodnej i bieżącej wymiany informacji ma bezpośredni wpływ na skuteczność operacyjną, podejmowanie decyzji i ochronę sił zbrojnych. Niniejsza książka została napisana z zamiarem przedstawienia tych realiów szerszemu gronu odbiorców akademickich i profesjonalnych, łącząc podstawy teoretyczne z praktycznymi zastosowaniami wojskowymi.

Moje wykształcenie akademickie w zakresie technologii komunikacyjnych i informacyjnych w połączeniu z moim zawodowym zaangażowaniem w edukację i badania wojskowe ukształtowały perspektywę przyjętą w niniejszej pracy. W trakcie moich studiów i badań zauważyłem powtarzającą się lukę między szybko rozwijającymi się technologiami komunikacyjnymi a ich ustrukturyzowaną integracją na poziomie systemowym w ramach struktur wojskowych. Podczas gdy wiele prac koncentruje się na izolowanych technologiach lub konkretnych rozwiązaniach technicznych, niewiele z nich próbuje przedstawić kompleksowy i zintegrowany obraz bezpiecznych wojskowych systemów komunikacyjnych jako ewoluujących architektur. Niniejsza książka ma na celu wypełnienie tej luki poprzez spójną i ustrukturyzowaną analizę technologii, mechanizmów bezpieczeństwa i zasad architektury, które stanowią podstawę współczesnej i przyszłej komunikacji wojskowej.

Książka opiera się również na moich bieżących badaniach doktoranckich, które koncentrują się na bezpiecznych ramach komunikacyjnych i zaawansowanych platformach komunikacyjnych do zastosowań obronnych. Część tych badań została włączona do książki w formie dedykowanego studium przypadku, które przedstawia praktyczny przykład zastosowania koncepcji teoretycznych i zasad

architektury w rzeczywistym systemie. Studium przypadku, zaczerpnięte z mojej pracy doktorskiej, zostało zamieszczone w celu zilustrowania przejścia od analizy koncepcyjnej do projektowania i wdrażania systemu. Jego celem nie jest przedstawienie ostatecznego rozwiązania, ale raczej zilustrowanie, w jaki sposób można skonstruować bezpieczne platformy komunikacyjne, aby spełniały one wymagania operacyjne , takie jak bezpieczeństwo, niezawodność, opóźnienia i interoperacyjność.

Pisząc tę książkę, starałem się zachować równowagę między rygorem akademickim a praktyczną przydatnością. Treść opiera się na ustalonych zasadach inżynierii komunikacyjnej, cyberbezpieczeństwa i systemów wojskowych, odzwierciedlając jednocześnie aktualne trendy technologiczne, takie jak sztuczna inteligencja, radia definiowane programowo, systemy bezzałogowe, komunikacja satelitarna i nowe mechanizmy bezpieczeństwa. Nie zamierzałem stworzyć tekstu czysto teoretycznego ani wąsko technicznego podręcznika, ale uporządkowaną pracę naukową, która może służyć jako punkt odniesienia dla studentów, badaczy, inżynierów i wojskowych zainteresowanych projektowaniem i rozwojem bezpiecznych systemów komunikacyjnych.

Dlatego też książka ta jest skierowana do szerokiego grona odbiorców, obejmującego studentów studiów magisterskich i doktoranckich kierunków inżynieryjnych i związanych z obronnością, naukowców zajmujących się komunikacją i bezpieczeństwem oraz praktyków zaangażowanych w planowanie komunikacji wojskowej, rozwój systemów i wdrażanie operacyjne. Jednocześnie książka została napisana z wystarczającą głębią i analitycznym podejściem, aby wspierać zaawansowane badania naukowe i przyczyniać się do bieżących dyskusji w środowisku naukowym.

Wreszcie, książka ta stanowi krok w dłuższej podróży akademickiej i zawodowej. Odzwierciedla zarówno zakończone badania, jak i trwające poszukiwania, uznając, że dziedzina komunikacji wojskowej jest dynamiczna i stale ewoluuje. Technologie, architektury i struktury omówione w niniejszej pracy będą niewątpliwie nadal rozwijać się w odpowiedzi na nowe wymagania operacyjne i pojawiające się zagrożenia. Mam nadzieję, że książka ta przyczyni się do głębszego zrozumienia bezpiecznych systemów komunikacyjnych i zachęci do dalszych badań, dyskusji i innowacji w tej kluczowej dziedzinie.

Wprowadzenie

Wojskowe systemy łączności zawsze odgrywały decydującą rolę w prowadzeniu działań wojennych, kształtując sposób koordynacji, podejmowania decyzji i działania sił zbrojnych w różnych środowiskach operacyjnych. Od najwcześniejszych form sygnalizacji na polu bitwy po dzisiejsze globalnie połączone i oparte na danych architektury, komunikacja pozostaje kluczowym czynnikiem umożliwiającym dowodzenie, kontrolę i skuteczność operacyjną. Jednak we współczesnych operacjach wojskowych systemy łączności ewoluowały poza swoją tradycyjną rolę wspierającą i obecnie stanowią samodzielny element zdolności strategicznych. Bezpieczna, odporna i elastyczna infrastruktura łączności ma fundamentalne znaczenie dla osiągnięcia przewagi informacyjnej, utrzymania tempa operacyjnego i zapewnienia przetrwania sił zbrojnych w coraz bardziej złożonym i spornym środowisku.

Transformacja działań wojennych w XXI wieku wprowadziła nowe wyzwania, które zasadniczo zmieniają wymagania stawiane wojskowym systemom łączności. Współczesne operacje charakteryzują się dużą mobilnością, zaangażowaniem w wielu obszarach oraz integracją działań konwencjonalnych, cybernetycznych i informacyjnych. Siły zbrojne działają na lądzie, w powietrzu, na morzu, w przestrzeni kosmicznej i w cyberprzestrzeni, często jednocześnie i w koordynacji z partnerami sojuszniczymi i koalicyjnymi. W takich warunkach zdolność do wymiany dokładnych, aktualnych i chronionych informacji decyduje nie tylko o sukcesie taktycznym, ale także o wynikach strategicznych. Systemy łączności muszą zatem działać niezawodnie w warunkach niepewności, zakłóceń i aktywnej ingerencji przeciwnika.

Jedną z charakterystycznych cech współczesnej komunikacji wojskowej jest centralne znaczenie bezpieczeństwa. W miarę jak sieci komunikacyjne stają się coraz bardziej połączone i oparte na oprogramowaniu, są one coraz bardziej narażone na cyberataki, wojnę elektroniczną i wykorzystanie przez przeciwników. Poufność, integralność, dostępność i autentyczność informacji nie są już abstrakcyjnymi pojęciami technicznymi, ale koniecznością operacyjną. Naruszenie bezpieczeństwa systemów łączności może prowadzić do dezinformacji, utraty dowództwa, niepowodzenia misji lub niezamierzonej eskalacji konfliktu. W związku z tym kwestie bezpieczeństwa muszą być uwzględnione na każdym poziomie projektowania systemów łączności, od fizycznych mechanizmów transmisji po architekturę sieci i usługi na poziomie aplikacji.

Jednocześnie innowacje technologiczne przyspieszają w niespotykanym dotąd tempie. Postępy w dziedzinie komunikacji cyfrowej, kryptografii, sztucznej inteligencji, systemów satelitarnych i nowych technologii, takich jak komunikacja

kwantowa, szybko zmieniają krajobraz komunikacji wojskowej. Rozwój ten stwarza znaczące możliwości poprawy wydajności, odporności i zdolności adaptacyjnych, ale wprowadza również nowe słabe punkty i złożoność. Instytucje wojskowe muszą zatem znaleźć równowagę między wdrażaniem zaawansowanych technologii a rygorystycznym projektowaniem architektury, dyscypliną operacyjną i odpowiedzialnością etyczną.

Książka ta powstała z potrzeby przedstawienia kompleksowej i zintegrowanej analizy bezpiecznych systemów komunikacji wojskowej w kontekście współczesnych i przyszłych operacji obronnych. Zamiast skupiać się na pojedynczych technologiach lub wąskich problemach technicznych, książka przyjmuje perspektywę systemową, traktując komunikację jako połączoną strukturę obejmującą sprzęt, oprogramowanie, mechanizmy bezpieczeństwa, doktrynę operacyjną i podejmowanie decyzji przez ludzi. Celem jest przedstawienie spójnego zrozumienia tego, w jaki sposób projektowane, wdrażane i rozwijane są bezpieczne systemy komunikacyjne, aby sprostać wymaganiom współczesnej wojny.

W pierwszych rozdziałach przedstawiono podstawowy kontekst dyskusji. Współczesną komunikację wojskową analizuje się poprzez jej historyczną ewolucję od systemów analogowych i punkt-punkt do architektur cyfrowych, szyfrowanych i sieciowych. Ewolucja ta odzwierciedla szersze zmiany w doktrynie wojskowej, tempie operacyjnym i wymaganiach informacyjnych. Znaczenie bezpiecznej komunikacji podkreśla się nie tylko w kontekście ochrony informacji, ale także umożliwiania skoordynowanych i zgodnych z prawem działań wojskowych. Podkreśla się rolę standaryzacji, szczególnie w ramach sojuszy, jako kluczowego czynnika zapewniającego interoperacyjność i spójność operacyjną sił sojuszniczych.

Następnie w książce omówiono podstawowe zasady leżące u podstaw bezpiecznych systemów łączności. Przesyłanie sygnałów, propagacja oraz wyzwania związane z łącznością w linii wzroku i poza linią wzroku są analizowane w celu ustalenia podstawowych założeń technicznych. Zasady te pozostają aktualne pomimo postępu technologicznego, ponieważ ograniczenia fizyczne i czynniki środowiskowe nadal wpływają na wydajność łączności. Opierając się na tych podstawach, w książce przeanalizowano podstawowe mechanizmy bezpieczeństwa, takie jak szyfrowanie, uwierzytelnianie, kontrola dostępu i techniki przeciwzakłóceniowe. Elementy te stanowią podstawę bezpiecznych architektur komunikacyjnych i są niezbędne do utrzymania niezawodności i zaufania w środowiskach spornych.

W kolejnych rozdziałach głównym tematem staje się cyberbezpieczeństwo. Wojskowe sieci komunikacyjne są coraz częściej celem wyrafinowanych

cyberzagrożeń, których celem jest zakłócenie operacji, wykradzenie poufnych informacji lub manipulowanie procesami decyzyjnymi. W książce przeanalizowano charakter tych zagrożeń oraz strategie stosowane w celu ich ograniczenia, w tym wzmocnienie sieci, wybór protokołów kryptograficznych, architektury typu zero trust oraz mechanizmy reagowania na incydenty. Poruszając kwestię cyberbezpieczeństwa zarówno na poziomie technicznym, jak i architektonicznym, książka podkreśla znaczenie odporności i zdolności adaptacyjnych w obliczu ciągłych i ewoluujących zagrożeń.

Systemy łączności radiowej pozostają podstawą operacji taktycznych, a ich rola jest dogłębnie analizowana. Tradycyjne systemy VHF, UHF i HF nadal zapewniają niezbędne możliwości, szczególnie w środowiskach, w których infrastruktura jest ograniczona lub zdegradowana. Integracja tych systemów z radiami definiowanymi programowo i technikami sieci kratowych ilustruje, w jaki sposób stare technologie można ulepszyć dzięki nowoczesnym podejściom architektonicznym. Interoperacyjność z siłami sojuszniczymi jest traktowana jako kluczowy wymóg, odzwierciedlający realia operacji wspólnych i koalicyjnych we współczesnych scenariuszach konfliktów.

Coraz częstsze wykorzystanie bezzałogowych systemów powietrznych wprowadza nowy wymiar do komunikacji wojskowej. Bezzałogowe statki powietrzne (UAV) służą jako urządzenia do gromadzenia danych, przekaźniki komunikacyjne i platformy operacyjne, które zwiększają zasięg i elastyczność sieci wojskowych. W książce przeanalizowano wyzwania związane z bezpieczeństwem komunikacji między UAV a centrum dowodzenia, w tym szyfrowanie, uwierzytelnianie, ochronę warstwy łącza oraz ograniczenia wydajności, takie jak opóźnienia i niezawodność. W dedykowanym studium przypadku przedstawiono zintegrowaną platformę bezpiecznej komunikacji, ilustrującą, w jaki sposób koncepcje teoretyczne można zastosować w praktyce, aby sprostać rzeczywistym wymaganiom operacyjnym.

Sztuczna inteligencja stanowi siłę transformacyjną w wojskowych systemach łączności. Książka bada, w jaki sposób techniki sztucznej inteligencji mogą poprawić wydajność routingu, wykrywanie włamań, alokację widma i zarządzanie siecią w środowiskach bojowych. Umożliwiając systemom wykrywanie, uczenie się i adaptację, architektury łączności oparte na sztucznej inteligencji oferują nowy poziom odporności i wydajności operacyjnej. Jednocześnie integracja sztucznej inteligencji rodzi ważne pytania związane z przejrzystością, odpowiedzialnością i kontrolą, które są poruszane w zrównoważonej i krytycznej analizie.

Kolejnym ważnym tematem książki są nowe technologie. Sieci komórkowe nowej generacji, komunikacja satelitarna, kwantowa dystrybucja kluczy i kognitywne sieci radiowe są analizowane jako czynniki umożliwiające rozwój przyszłych

zdolności komunikacyjnych wojska. Technologie te rozszerzają zakres operacyjny, umożliwiając większą przepustowość danych, globalną łączność, zwiększone bezpieczeństwo i inteligentne wykorzystanie widma. Ich integracja z systemami wojskowymi odzwierciedla przejście w kierunku architektury hybrydowej, która łączy elementy naziemne, powietrzne, morskie i kosmiczne w jednolitej strukturze komunikacyjnej.

W ostatnich rozdziałach te zmiany technologiczne i koncepcyjne zostały podsumowane w szerszej dyskusji na temat tego, jak można zbudować bezpieczne ramy komunikacyjne dla przyszłej armii. Wymagania wobec nowoczesnych sił zbrojnych zostały przeanalizowane pod kątem odporności, interoperacyjności, skalowalności i bezpieczeństwa. Przedstawiono zasady architektury, aby zilustrować, w jaki sposób można zaprojektować bezpieczne taktyczne systemy komunikacyjne wspierające złożone i rozproszone operacje. Podkreślono znaczenie integracji z systemami C4ISR jako kluczowego czynnika w osiągnięciu świadomości sytuacyjnej i przewagi decyzyjnej. Omówiono kwestie etyczne i prawne, aby zapewnić zgodność innowacji technologicznych z ustalonymi normami i obowiązkami. Dyskusja na temat przyszłych trendów zapewnia perspektywę na przyszłość dotyczącą prawdopodobnego rozwoju wojskowych systemów komunikacyjnych w odpowiedzi na pojawiające się zagrożenia i możliwości technologiczne.

Książka jest skierowana do profesjonalistów wojskowych, inżynierów obronnych, badaczy i studentów studiów magisterskich zajmujących się badaniem i rozwojem bezpiecznych systemów łączności. Książka jest również przydatna dla decydentów politycznych i osób odpowiedzialnych za planowanie obronne i rozwój zdolności obronnych. Łącząc analizę techniczną z perspektywą architektoniczną i operacyjną, książka ma na celu wypełnienie luki między teorią a praktyką w zakresie łączności wojskowej.

Książka ma na celu przyczynienie się do zrozumienia i rozwoju bezpiecznych wojskowych systemów łączności poprzez przedstawienie zintegrowanej i zorientowanej na przyszłość perspektywy. W miarę jak działania wojenne stają się coraz bardziej złożone i rozległe, zdolność do bezpiecznej, niezawodnej i inteligentnej komunikacji pozostanie decydującym czynnikiem skuteczności wojskowej. Poprzez kompleksową analizę technologii, architektury i zasad, niniejsza praca ma na celu zapewnienie podstaw do budowy systemów łączności, które wspierają sukces operacyjny, jednocześnie zapewniając bezpieczeństwo, odporność i odpowiedzialność w nowoczesnych i przyszłych operacjach wojskowych.

Wnioski

W niniejszej książce przeanalizowano ewolucję, strukturę i przyszły kierunek rozwoju bezpiecznych systemów łączności wojskowej w kontekście współczesnych i pojawiających się operacji obronnych. W poszczególnych rozdziałach wykazano, że łączność wojskowa nie jest już jedynie technologią wspomagającą, ale stanowi centralny filar skuteczności operacyjnej, strategicznego podejmowania decyzji i przewagi informacyjnej. Rosnąca złożoność środowiska bezpieczeństwa w połączeniu z szybkim postępem technologicznym wymaga struktur komunikacyjnych, które są odporne, inteligentne, interoperacyjne i oparte na zasadach etycznych.

W pierwszych rozdziałach ustalono fundamentalne znaczenie bezpiecznej komunikacji w operacjach wojskowych. Współczesne siły zbrojne działają w warunkach niepewności, mobilności i ciągłego zagrożenia, gdzie zdolność do wymiany dokładnych i aktualnych informacji decyduje o sukcesie lub porażce misji. Przejście od systemów analogowych i izolowanych do cyfrowych, szyfrowanych i sieciowych architektur komunikacyjnych odzwierciedla szersze przesunięcie w kierunku wojny opartej na informacjach. Ewolucja ta przekształciła systemy komunikacyjne w aktywne narzędzia dowodzenia, kontroli i koordynacji we wszystkich obszarach operacyjnych.

Centralnym tematem całej książki jest nierozerwalny związek między komunikacją a bezpieczeństwem. W miarę jak sieci wojskowe stają się coraz bardziej połączone i oparte na oprogramowaniu, są one coraz bardziej narażone na cyberzagrożenia, wojnę elektroniczną i wykorzystanie przez przeciwników. Analiza szyfrowania, uwierzytelniania, kontroli dostępu i wzmacniania sieci podkreśliła konieczność wbudowania mechanizmów bezpieczeństwa we wszystkie warstwy architektur komunikacyjnych. Zamiast traktować bezpieczeństwo jako dodatek, nowoczesne systemy wojskowe muszą przyjąć podejście oparte na bezpieczeństwie projektowym, które zapewnia poufność, integralność, autentyczność i dostępność w warunkach konfliktu.

Dyskusja na temat systemów łączności radiowej dla jednostek taktycznych wykazała, że starsze technologie pozostają istotne z operacyjnego punktu widzenia, gdy są zintegrowane z nowoczesną architekturą. Systemy VHF, UHF i HF nadal zapewniają solidne możliwości komunikacyjne, szczególnie w środowiskach o ograniczonej lub braku łączności. W połączeniu z radiami definiowanymi programowo i zasadami sieci kratowych technologie te zapewniają elastyczność i odporność, które są niezbędne w operacjach taktycznych. Możliwość dostosowania przebiegów, częstotliwości i strategii routingu pozwala siłom zbrojnym utrzymać łączność pomimo mobilności, ograniczeń terenowych i wrogich zakłóceń.

Bezzałogowe systemy powietrzne i ich integracja z bezpiecznymi strukturami komunikacyjnymi zostały zbadane jako cecha charakterystyczna współczesnych operacji wojskowych. Bezzałogowe statki powietrzne (UAV) funkcjonują nie tylko jako platformy sensoryczne, ale także jako dynamiczne węzły komunikacyjne typu „ ", które rozszerzają zasięg sieci i zwiększają świadomość sytuacyjną. Analiza komunikacji między bezzałogowymi statkami powietrznymi a centrum dowodzenia podkreśliła znaczenie szyfrowania, uwierzytelniania, bezpieczeństwa warstwy łącza i optymalizacji wydajności. Przedstawione studium przypadku ilustruje, w jaki sposób zintegrowana i bezpieczna platforma komunikacyjna może wspierać wymianę danych w czasie rzeczywistym, jednocześnie rozwiązując problemy związane z opóźnieniami, niezawodnością i przepustowością w środowiskach operacyjnych.

Sztuczna inteligencja stała się siłą transformacyjną w wojskowych systemach łączności. Badania nad routingiem opartym na sztucznej inteligencji, wykrywaniem włamań, alokacją widma i sieciami bojowymi wykazały, w jaki sposób inteligentne algorytmy mogą zwiększyć zdolność adaptacyjną i odporność. Sztuczna inteligencja umożliwia systemom łączności dynamiczne reagowanie na zmiany środowiskowe i działania przeciwnika, zmniejszając obciążenie poznawcze operatorów ludzkich i poprawiając tempo operacyjne. Jednocześnie integracja sztucznej inteligencji rodzi ważne pytania związane z przejrzystością, odpowiedzialnością i kontrolą, wzmacniając potrzebę odpowiedzialnego i dobrze zarządzanego wdrażania.

Nowe technologie, takie jak sieci komórkowe nowej generacji, komunikacja satelitarna, kwantowa dystrybucja kluczy i kognitywne sieci radiowe, zostały przeanalizowane jako czynniki umożliwiające rozwój przyszłych zdolności komunikacyjnych wojska. Technologie te rozszerzają zakres operacyjny, obsługując wyższe prędkości transmisji danych, globalną łączność, zwiększone bezpieczeństwo i inteligentne wykorzystanie widma. Ich integracja z systemami wojskowymi odzwierciedla przejście w kierunku architektur hybrydowych, łączących elementy naziemne, powietrzne, morskie i kosmiczne. Ta konwergencja umożliwia operacje wielodomenowe, wprowadzając jednocześnie nowe wyzwania architektoniczne i bezpieczeństwa, które należy rozwiązać w sposób holistyczny.

Ostatnie rozdziały skupiały się na stworzeniu bezpiecznej struktury komunikacyjnej dla przyszłej armii. Analiza podkreślała, że sam postęp technologiczny nie wystarczy bez spójnego projektu architektonicznego, integracji z systemami C4ISR oraz uwzględnienia implikacji etycznych i prawnych. Przyszłe ramy komunikacyjne muszą wspierać interoperacyjność, skalowalność i odporność, pozostając jednocześnie zgodnymi z prawem międzynarodowym i zasadami etycznymi. Uwzględnienie kwestii zarządzania, odpowiedzialności i

zrównoważonego rozwoju gwarantuje, że systemy komunikacyjne przyczyniają się do długoterminowego bezpieczeństwa i stabilności, a nie tylko do krótkoterminowej przewagi taktycznej.

Kluczowym wnioskiem płynącym z niniejszej pracy jest to, że przyszłe wojskowe systemy komunikacyjne muszą być adaptacyjnymi ekosystemami, a nie statyczną infrastrukturą. Dynamiczny charakter współczesnych konfliktów wymaga systemów, które mogą się rekonfigurować w odpowiedzi na zmieniające się wymagania misji, warunki środowiskowe i wektory zagrożeń. Ta zdolność adaptacyjna wymaga ścisłej integracji między technologiami komunikacyjnymi, mechanizmami bezpieczeństwa, inteligentnymi systemami kontroli i ludźmi podejmującymi decyzje. Sukces takich systemów w zakresie zdolności operacyjnych ( ) zależy nie tylko od doskonałości technicznej, ale także od zgodności doktrynalnej i gotowości organizacyjnej.

Kolejnym ważnym wnioskiem jest rosnące znaczenie interoperacyjności i operacji koalicyjnych. Współczesne misje wojskowe są coraz częściej prowadzone w kontekście wielonarodowym, co wymaga systemów komunikacyjnych umożliwiających kontrolowaną wymianę informacji przy jednoczesnym zachowaniu interesów bezpieczeństwa narodowego. Standaryzacja, wspólne ramy bezpieczeństwa i elastyczne mechanizmy kontroli dostępu są niezbędne do skutecznej współpracy. Architektury komunikacyjne, które z założenia wspierają interoperacyjność, stanowią podstawę zaufania i spójności operacyjnej między siłami sojuszniczymi.

Etyczne i prawne aspekty technologii komunikacji wojskowej stanowią kluczowy obszar odpowiedzialności projektantów, operatorów i decydentów. W miarę jak systemy komunikacyjne stają się coraz bardziej autonomiczne i zintegrowane z funkcjami wspomagania decyzji, potencjalne konsekwencje awarii lub niewłaściwego wykorzystania systemów rosną. Uwzględnienie kwestii etycznych i zgodności z prawem w projektowaniu systemów gwarantuje, że przewaga technologiczna nie podważa legitymizacji ani odpowiedzialności. Odpowiedzialne innowacje w komunikacji wojskowej muszą równoważyć skuteczność operacyjną z przestrzeganiem ustalonych norm i wartości.

Książka ta wnosi wkład w tę dziedzinę, przedstawiając kompleksową i zintegrowaną perspektywę bezpiecznych systemów komunikacji wojskowej. Zamiast skupiać się na pojedynczych technologiach, kładzie nacisk na spójność architektury, integrację bezpieczeństwa i projektowanie zorientowane na przyszłość. Połączenie analizy teoretycznej, praktycznych rozważań i analizy studiów przypadków stanowi uporządkowane ramy dla zrozumienia i rozwoju nowoczesnej infrastruktury komunikacyjnej wojska.

Z akademickiego punktu widzenia praca ta stanowi podstawę do dalszych badań nad adaptacyjnymi architekturami komunikacyjnymi, zarządzaniem sieciami opartym na sztucznej inteligencji oraz systemami kwantowymi zapewniającymi bezpieczeństwo. Z operacyjnego punktu widzenia oferuje wgląd w wyzwania i możliwości związane z wdrażaniem bezpiecznych technologii komunikacyjnych w złożonych środowiskach. Przedstawione koncepcje mogą stanowić podstawę do opracowania doktryny, projektowania systemów i formułowania polityki w instytucjach obronnych.

Podsumowując, bezpieczne systemy komunikacji wojskowej są decydującym czynnikiem we współczesnej i przyszłej wojnie. W obliczu coraz bardziej złożonych i kontrowersyjnych środowisk operacyjnych siły zbrojne będą nadal musiały zapewnić sobie strategiczną przewagę w zakresie bezpiecznej, niezawodnej i inteligentnej wymiany informacji. Dzięki przyjęciu zintegrowanych, adaptacyjnych i opartych na zasadach etycznych ram komunikacyjnych przyszłe armie będą mogły osiągnąć przewagę informacyjną, zachowując jednocześnie odporność, legitymizację i skuteczność operacyjną. Niniejsza książka ma na celu przyczynienie się do realizacji tego celu poprzez uporządkowane i przyszłościowe omówienie technologii, architektury i zasad komunikacji wojskowej, które będą kształtować przyszłość komunikacji wojskowej ( ).

Referencje

1. Defence Strategic Communications, *oficjalny dziennik Centrum Doskonałości Komunikacji Strategicznej NATO,* tom 10, wiosna-jesień 2021 r., NATO StratCom COE, Ryga, Łotwa.
2. Polovic, J., „Wyzwania globalnej komunikacji: strategiczna rywalizacja i eskalacja napięć w stosunkach międzynarodowych", *Zbiór prac Wydziału Filozofii,* tom 48, nr 1, 2024, s. 51-57. https://doi.org/10.5671/ca.48.1.7
3. Mustafovski, R., „Wykorzystanie platform komunikacyjnych w operacjach wojskowych: zwiększenie skuteczności strategicznej i taktycznej", *Database Systems Journal,* tom XVI, 2025, Wydział Elektrotechniki i Technologii Informacyjnych, Uniwersytet św. Cyryla i Metodego, Skopje, Republika Macedonii Północnej.
4. Rienzi, T. M., *Communications-Electronics 1962-1970,* seria Vietnam Studies, Departament Armii, Waszyngton, DC, USA, 2002.
5. Mazzenga, F., Landry, R. i Young, K., „Komunikacja wojskowa", *IEEE Communications Magazine,* październik 2020 r., s. 50-56.
6. Organizacja Traktatu Północnoatlantyckiego (NATO), *Allied Joint Doctrine for Communication and Information Systems (AJP-6),* wydanie B, wersja 1, Biuro Normalizacji NATO (NSO), kwiecień 2024 r.
7. Departament Obrony Stanów Zjednoczonych, *Strategia modernizacji C3: dowodzenie, kontrola i łączność,* Waszyngton, DC, USA, wrzesień 2020 r.
8. Monteiro Marques, M., „STANAG 4586 – Standardowe interfejsy systemu sterowania bezzałogowymi statkami powietrznymi (UCS) dla interoperacyjności bezzałogowych statków powietrznych NATO", dokument techniczny NATO, Escola Naval – Afeite, Portugalia.
9. Yarnell, A. M., Dullea, C. i Grunberg, N. E., „Komunikacja wojskowa", w: *Komunikacja wojskowa i medyczna,* rozdział 11, Dowództwo Badań i Rozwoju Medycznego Armii Stanów Zjednoczonych, USA.
10. Timofte, G., „Modernizacja wojskowych systemów łączności zgodnie z nowymi wymaganiami operacyjnymi, informacyjnymi i technicznymi pola walki", *Biuletyn naukowy Akademii Nauk Rumunii,* Bukareszt, Rumunia.
11. Hayes, C., *Umowy normalizacyjne NATO (STANAG) dla dowódców i sztabów,* Wiadomości z frontu, Centrum Doświadczeń Wojskowych (CALL), Armia Stanów Zjednoczonych, kwiecień 2019 r.
12. Sánchez, R., Evans, J. i Minden, G., „Networking on the Battlefield: Challenges in Highly Dynamic Multi-hop Wireless Networks" [Sieci *na polu walki*: wyzwania związane z wysoce dynamicznymi sieciami bezprzewodowymi typu multi-hop], *materiały konferencyjne IEEE MILCOM 1999,* Atlantic City, New Jersey, USA, październik 1999 r.

13. Kumar, D., „Challenges of a Digitised Battlefield" [Wyzwania związane z cyfryzacją pola walki], *Journal of the United Service Institution of India,* tom CXLII, nr 590, październik–grudzień 2012 r.
14. Lipscomb, P., „The Evolution of Communications in the Military as it Relates to Leadership" (Ewolucja komunikacji w wojsku w kontekście przywództwa), *Integrated Studies*, artykuł nr 90, Murray State University, 2017 r. Dostępny pod adresem: https://digitalcommons.murraystate.edu/bis437/90
15. Amin, M. G., Lindsey, A. R., Zhao, L. i Zhang, Y., *„Techniki przeciwzakłóceniowe dla odbiorników GPS",* końcowy raport techniczny AFRL-IF-RS-TR-2001-186, Laboratorium Badawcze Sił Powietrznych, ośrodek badawczy w Rzymie, Nowy Jork, USA, wrzesień 2001 r.
16. Bardis, N. G., Doukas, N. i Ntaikos, K., „Projektowanie i rozwój bezpiecznej komunikacji wojskowej w oparciu o prototypowy algorytm kryptograficzny AES i zaawansowany system zarządzania kluczami", *WSEAS Transactions on Information Science and Applications,* Uniwersytet Edukacji Wojskowej, Akademia Wojskowa Grecji, Grecja.
17. Colbeck, M. J. L., „Szyfrowanie kwantowe w komunikacji wojskowej", *materiały konferencyjne EAAW,* 28–29 listopada 2023 r.
18. Evans, J., Sánchez, R. i Minden, G., „Networking on the Battlefield: Challenges in Highly Dynamic Multi-hop Wireless Networks" (Sieci *na polu* bitwy: wyzwania *związane z wysoce dynamicznymi* sieciami bezprzewodowymi *typu multi-hop*), *materiały konferencyjne IEEEMILCOM,* Atlantic City, New Jersey, USA, październik 1999 r.
19. Hayes, C., „Porozumienia NATO w sprawie standaryzacji (STANAG) dla dowódców i personelu", *News from the Front,* Center for Army Lessons Learned (CALL), kwiecień 2019 r.
20. Kang, J. S., „Independent Authentication Protocol in Tactical Network Environment Using Hash Lock Approach" [Niezależny protokół uwierzytelniania w środowisku sieci taktycznej z wykorzystaniem podejścia Hash Lock], *International Journal of Machine Learning and Computing*, tom 5, nr 5, październik 2015 r.
21. Kovács, L., „Wojna elektroniczna i wyzwania asymetryczne", *Bolyai Szemle,* nr 3, 2009, s. 135–151, ISSN 1416-1443.
22. Kumar, D., „Wyzwania związane z cyfrowym polem walki", *Journal of the United Service Institution of India,* tom CXLII, nr 590, październik–grudzień 2012 r.
23. Lipscomb, P., „Ewolucja komunikacji w wojsku w kontekście przywództwa", *Integrated Studies,* nr 90, Murray State University, 2017.
24. Sayyed, S. Y., Gurap, S. L., Devadhe, J. L. i Gat, K. R., „Przegląd bezpiecznej komunikacji bezprzewodowej do zastosowań wojskowych",

International Journal of Electrical, Electronics and Data Communication, tom 5, nr 11, listopad 2017 r.
25. Shinde, V., Kulkarni, S. i Malekar, M. R., „Bezpieczny system komunikacyjny", *International Journal of Innovations in Engineering Research and Technology (IJIERT),* materiały konferencyjne TECHNO-2K17.
26. Timofte, G., „Modernizacja wojskowych systemów łączności zgodnie z nowymi wymaganiami operacyjnymi, informacyjnymi i technicznymi pola walki nowej generacji ( )", Akademia Nauk Rumunii, Bukareszt, Rumunia.
27. Departament Armii Stanów Zjednoczonych, *Doktryna łączności sygnałowej (FM 100-11),* Departament Armii, Waszyngton, lipiec 1948 r.
28. Alnifie, G. i Simon, R., „Wielokanałowa ochrona przed atakami zakłócającymi w bezprzewodowych sieciach czujników", w: *Materiały z 3. warsztatów ACM dotyczących jakości usług i bezpieczeństwa sieci bezprzewodowych i mobilnych,* 2007, s. 95-104.
29. Alnifie, G. i Simon, R., „MULEPRO: wielokanałowa odpowiedź na ataki zakłócające w bezprzewodowych sieciach czujników", *Wireless Communications and Mobile Computing,* 2010.
30. Bayraktaroglu, E., King, C., Liu, X., Noubir, G., Rajaraman, R. i Thapa, B., „O wydajności IEEE 802.11 w warunkach zakłóceń", w: *Materiały z 27. konferencji IEEE poświęconej komunikacji komputerowej,* 2008, str. 1265-1273.
31. Bellardo, J. i Savage, S., „Ataki typu denial-of-service w standardzie 802.11: rzeczywiste luki w zabezpieczeniach i praktyczne rozwiązania", w: *Materiały z 12. sympozjum USENIX Security Symposium,* 2003, s. 15–28.
32. Broustis, I., Pelechrinis, K., Syrivelis, D., Krishnamurthy, S. V. i Tassiulas, L., „FIJI: Fighting Implicit Jamming in 802.11 WLANs" [FI*JI*: Walka z niejawnym zakłócaniem w *sieciach WLAN 802*.11]*, Security and Privacy in Communication Networks*, tom 19, 2009, str. 21-40.
33. Chiang, J. T. i Hu, Y. C., „Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks" [Wykrywanie i ograniczanie zakłóceń międzywarstwowych w bezprzewodowych sieciach nadawczych]*, IEEE/ACM Transactions on Networking*, tom 19, nr 1, 2011, str. 286-298.
34. Commander, C. W., Pardalos, P. M., Ryabchenko, V., Shylo, O. V, Uryasev, S. i Zrazhevsky, G., „Zakłócanie sieci komunikacyjnych w warunkach całkowitej niepewności", *Optimization Letters*, tom 2, nr 1, 2008, str. 53-70.
35. Gencer, C., Aydogan, E. K. i Celik, C., „System wspomagania decyzji w zakresie lokalizacji systemów zakłócających radiowych VHF/UHF w terenie", *Information Systems Frontiers,* tom 10, nr 1, 2008, str. 111-124.
36. Gummadi, R., Wetherall, D., Greenstein, B. i Seshan, S., „Zrozumienie i łagodzenie wpływu zakłóceń radiowych na sieci 802.11", w*: Materiały konferencji ACM SIGCOMM poświęconej zastosowaniom, technologiom, architekturom i*

protokołom komunikacji komputerowej, 2007, str. 385-396.
37. Huang, H., Ahmed, N. i Pulluru, S., „On Limited Range Strategic and Random Jamming Attacks in Wireless Ad Hoc Networks" [O strategicznych i losowych atakach zakłócających o ograniczonym zasięgu w bezprzewodowych sieciach ad hoc], w: *Proceedings of the IEEE 34th Conference on Local Computer Networks* [Materiały z *34. konferencji IEEE poświęconej lokalnym sieciom komputer*owym], 2010, str. 1-8.
38. Jain, S. K. i Garg, K., „Hybrydowy model technik obrony przed atakami zakłócającymi stacje bazowe w bezprzewodowych sieciach czujników", w: *Materiały z pierwszej międzynarodowej konferencji poświęconej inteligencji obliczeniowej, systemom komunikacyjnym i sieciom*, 2009, str. 102-107.
39. Kerkez, B., Watteyne, T., Magliocco, M., Glaser, S. i Pister, K., „ " [Analiza wykonalności projektu kontrolera do adaptacyjnego przeskakiwania kanałów], w: *Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools*, 2009, s. 76:1-76:6.
40. Khattab, S., Mosse, D. i Melhem, R., „Jamming Mitigation in Multi-Radio Wireless Networks: Reactive or Proactive?" [Ograniczanie zakłóceń w sieciach bezprzewodowych z wieloma radiami*: reaktywne czy proaktywne?*], *w: Proceedings of the 4th International Conference on Security and Privacy in Communication Networks [Materiały z czwartej międzynarodowej konferencji poświęconej bezpieczeństwu i prywatności w sieciach komunikacyjnych]*, 2008, str. 27:1-27:10.
41. Khattab, S., Mosse, D. i Melhem, R., „Modelowanie obrony przed zakłóceniami poprzez przeskakiwanie kanałów w sieciach bezprzewodowych z wieloma radiami", w: *Materiały z 5. dorocznej międzynarodowej konferencji poświęconej systemom mobilnym i wszechobecnym: informatyka, sieci i usługi,* 2008, str. 25:1-25:10.
42. Lazos, L., Liu, S. i Krunz, M., „Mitigating Control Channel Jamming Attacks in MultiChannel Ad Hoc Networks" [Łagodzenie ataków zakłócających kanał sterowania w wielokanałowych sieciach ad hoc], w: *Proceedings of the 2nd ACM Conference on Wireless Network Security [Materiały z 2. konferencji ACM poświęconej bezpieczeństwu sieci bezprzewodowych]*, 2009, str. 169-180.
43. Li, M., Koutsopoulos, I. i Poovendran, R., „Optymalne ataki zakłócające i zasady ochrony sieci w bezprzewodowych sieciach czujników", w: *Materiały z 26. międzynarodowej konferencji IEEE poświęconej komunikacji komputerowej,* 2007, str. 1307-1315.
44. Liu, H., Liu, Z., Chen, Y. i Xu, W., „Określanie pozycji urządzenia zakłócającego przy użyciu iteracyjnego podejścia opartego na sile wirtualnej"*, Wireless Networks*, tom 17, nr 2, 2011, str. 531-547.
45. Liu, Z., Liu, H., Xu, W. i Chen, Y., „Wykorzystanie zmian sąsiedztwa

spowodowanych zakłóceniami do lokalizacji zakłócacza", *IEEE Transactions on Parallel and Distributed Systems,* 2011.
46. Misra, S., Singh, R. i Mohan, S. V. R., „Mechanizm wykrywania ataków zakłócających w sieciach bezprzewodowych czujników z wykorzystaniem systemu wnioskowania rozmytego, przydatny w wojnie informacyjnej", *Sensors*, tom 10, 2010, str. 3444-3479.
47. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C. i Pantziou, G., „Badanie dotyczące ataków zakłócających i środków zaradczych w bezprzewodowych sieciach czujników", *IEEE Communications Surveys and Tutorials*, tom 11, nr 4, 2009, str. 42-56.
48. Muraleedharan, R. i Osadciw, L. A., „Wykrywanie ataków zakłócających i środki zaradcze w bezprzewodowej sieci czujników z wykorzystaniem systemu mrówek", w: *Proceedings of SPIE – The International Society for Optical Engineering,* tom 6248, 2006, artykuł 62480G.
49. Navda, V, Bohra, A., Ganguly, S. i Rubenstein, D., „Wykorzystanie przeskakiwania kanałów w celu zwiększenia odporności standardu 802.11 na ataki zakłócające", w: *Proceedings of the IEEE 26th International Conference on Computer Communications*, 2007, str. 2526-2530.
50. Panyim, K., Hayajneh, T., Krishnamurthy, P. i Tipper, D., „Jamming Dust: A Low Power Distributed Jammer Network" [Zakłócanie pyłem: rozproszona sieć zakłócaczy o niskiej mocy], w: *Proceedings of the 27th Army Science Conference (*), 2009, str. 922-929.
51. Pelechrinis, K., Koufogiannakis, C. i Krishnamurthy, S. V., „Gaming the Jammer: Is Frequency Hopping Effective?" [Oszukiwanie zakłócacza: czy przeskakiwanie częstotliwości jest skuteczne?], w: *Materiały z 7. międzynarodowej konferencji poświęconej modelowaniu i optymalizacji sieci komórkowych, ad hoc i bezprzewodowych,* 2009, str. 187-196.
52. Pelechrinis, K., Koutsopoulos, I., Broustis, I. i Krishnamurthy, S. V., „Lightweight Jammer Localization in Wireless Networks: System Design and Implementation" [Lokalizacja zakłócaczy w sieciach *bezprzewodowych:* projekt systemu i wdrożenie], w: *Proceedings of the IEEE Global Telecommunications Conference,* 2009, str. 1-6.
53. Pelechrinis, K., Iliofotou, M. i Krishnamurthy, S. V., „Ataki typu denial of service w sieciach bezprzewodowych: przypadek zakłócaczy", *IEEE Communications Surveys and Tutorials,* tom 13, nr 2, 2011, str. 245-257.
54. Shin, I., Shen, Y., Xuan, Y., Thai, M. T. i Znati, T., „Reaktywne ataki zakłócające w sieciach bezprzewodowych czujników MultiRadio: skuteczny środek zaradczy poprzez identyfikację węzłów wyzwalających", w*: Proceedings of the 2nd ACM International Workshop on Foundations of Wireless Ad Hoc and Sensor Networking and Computing,* 2009, str. 87-96.

55. Strasser, M., Danev, B. i Capkun, S., „Wykrywanie reaktywnego zakłócania w sieciach czujników", *ACM Transactions on Sensor Networks*, tom 7, nr 2, 2010, artykuł 16.
56. Sun, Y. i Wang, X., „Lokalizacja zakłócaczy w bezprzewodowych sieciach czujników", w: *Materiały z 5. międzynarodowej konferencji poświęconej komunikacji bezprzewodowej, sieciom i komputerom mobilnym,* 2009, str. 1-4.
57. Tague, P., Slater, D., Poovendran, R. i Noubir, G., „Linear Programming Models for Jamming Attacks on Network Traffic Flows" [Modele programowania liniowego dla ataków zakłócających przepływ ruchu sieciowego], w: *Proceedings of the 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops [Materiały z 6. międzynarodowego sympozjum poświęconego modelowaniu i optymalizacji w sieciach mobilnych, ad hoc i bezprzewodowych oraz warsztatach]*, 2008, str. 207-216.
58. Thamilarasu, G. i Sridhar, R., „Modelowanie teoretyczne ataków zakłócających w sieciach ad hoc", w: *Materiały z 18. międzynarodowej konferencji poświęconej komunikacji komputerowej i sieciom*, 2009, str. 1-6.
59. Wang, H., Zhang, L., Li, T. i Tugnait, J., „Spectrally Efficient Jamming Mitigation Based on Code-Controlled Frequency Hopping" [Efektywne spektralnie ograniczanie zakłóceń oparte na sterowanym kodem przeskakiwaniu częstotliwości]*, IEEE Transactions on Wireless Communications*, tom 10, nr 3, 2011, str. 728-732.
60. Wilhelm, M., Martinovic, I., Schmitt, J. B. i Lenders, V., „Reactive Jamming in Wireless Networks: How Realistic Is the Threat?" [Reaktywne zakłócanie *w sieciach bezprzewodowych: jak realne* jest zagrożenie?], w: *Materiały z czwartej konferencji ACM poświęconej bezpieczeństwu sieci bezprzewodowych,* 2011, str. 47-52.
61. Wood, A., Stankovic, J. i Son, S., „JAM: A Jammed-Area Mapping Service for Sensor Networks" [JAM: usługa mapowania obszarów zakłóconych dla sieci czujników]*,* w: *Proceedings of the 24th IEEE Real-Time Systems Symposium [Materiały z 24. sympozjum IEEE poświęconego systemom czasu rzeczywistego],* 2003, str. 286-297.
62. Wood, A., Stankovic, J. i Zhou, G., „DEEJAM: pokonanie zakłóceń typu Energy- Efficient w sieciach bezprzewodowych opartych na standardzie IEEE 802.15.4", w*: Materiały z 4. dorocznej konferencji IEEE Communications Society poświęconej komunikacji i sieciom czujników, sieciom typu mesh i sieciom ad hoc*, 2007, s. 60-69.
63. Xu, W., Wood, T., Trappe, W. i Zhang, Y., „Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service" [Przeglądanie kanałów i wycofywanie się przestrzenne: obrona przed bezprzewodowym odmawianiem usługi], w: *Proceedings of the 3rd ACM Workshop on Wireless Security* [Materiały

z *trzeciego warsztatu ACM poświęconego bezpieczeństwu bezprzewodowemu*], 2004, str. 80-89.
64. Xu, W., Trappe, W., Zhang, Y. i Wood, T., „The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks" [Możliwość przeprowadzania i wykrywania ataków zakłócających w sieciach bezprzewodowych], w: *Proceedings of the 6th ACM International Symposium on Mobile AdHoc Networking and Computing [Materiały z 6. międzynarodowego sympozjum ACM poświęconego mobilnym sieciom ad hoc i przetwarzaniu danych],* 2005, s. 46–57.
65. Yoon, S. U., Murawski, R., Ekici, E., Park, S. i Mir, Z., „Adaptacyjne przeskakiwanie kanałów dla odpornych na zakłócenia bezprzewodowych sieci czujników", w: *Materiały z międzynarodowej konferencji IEEE poświęconej komunikacji*, 2010, str. 1-5.
66. Sztab Generalny Armii Włoskiej – Biuro Bezpieczeństwa, *Systemy Oprogramowania, Telekomunikacja i Bezpieczeństwo – Dokumenty nieobjęte klauzulą tajności,* Rzym, Włochy, 2008 r.
67. Sztab Generalny Armii Włoskiej – Biuro Bezpieczeństwa, *Systemy Oprogramowania, Telekomunikacja i Bezpieczeństwo – Dokumenty niejawne,* Rzym, Włochy, 2008.
68. ISO/IEC 15408-1, *Technologia informacyjna – Techniki bezpieczeństwa – Kryteria oceny bezpieczeństwa IT – Część 1: Wprowadzenie i model ogólny,* Międzynarodowa Organizacja Normalizacyjna, Genewa, 2009.
69. ISO/IEC 15408-2, *Technologia informacyjna – Techniki bezpieczeństwa – Kryteria oceny bezpieczeństwa IT – Część 2: Funkcjonalne elementy bezpieczeństwa,* Międzynarodowa Organizacja Normalizacyjna, Genewa, 2008 r.
70. ISO/IEC 15408-3, *Technologia informacyjna – Techniki bezpieczeństwa – Kryteria oceny bezpieczeństwa IT – Część 3: Elementy zapewniające bezpieczeństwo,* Międzynarodowa Organizacja Normalizacyjna, Genewa, 2008 r.
71. Departament Obrony Stanów Zjednoczonych, *Kryteria oceny zaufanych systemów komputerowych,* DoDD 5200.28-STD, Waszyngton, grudzień 1985 r.
72. Departament Obrony Stanów Zjednoczonych, *Dyrektywa: Zapewnienie bezpieczeństwa informacji,* DoDD 8500.01E, Waszyngton, październik 2002 r.
73. Federalny Urząd ds. Bezpieczeństwa Technologii Informacyjnych, *Uwagi dotyczące stosowania i interpretacja schematu (AIS): ITSEC do mapowania wspólnych kryteriów z potencjałem konkretnych ataków,* Bonn, Niemcy, 2010 r. Dostępne online: https://www.bsi.bund.de
74. ISO/IEC 27000, *Technologia informacyjna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i słownictwo,* Międzynarodowa Organizacja Normalizacyjna, Genewa, 2009 r.
75. Hare, F., „Cyberzagrożenie dla bezpieczeństwa narodowego: dlaczego nie

możemy się zgodzić", w: *Materiały z konferencji poświęconej konfliktom cybernetycznym,* Tallinn, Estonia, 2010 r., s. 211-225.
76. Liles, S., „Wojna cybernetyczna: jako forma konfliktu o niskiej intensywności i rebelii", w: *Materiały z konferencji poświęconej konfliktom cybernetycznym*, Tallinn, Estonia, 2010, s. 47-57.
77. Kotenko, I. V., „Multi-Agent Modeling and Simulation of Cyber-Attacks and Cyber Defense for Homeland Security" [Modelowanie wieloagentowe i symulacja cyberataków oraz cyberobrony dla bezpieczeństwa wewnętrznego], w: *Proceedings of the IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications [Materiały z międzynarodowych warsztatów IEEE dotyczących inteligentnego gromadzenia danych i zaawansowanych systemów obliczeniowych: technologia i zastosowania],* Dortmund, Niemcy, 6-8 września 2008 r.
78. Kotenko, I. V. i Ulanov, A. V., „Agent-Based Simulation of DDoS Attacks and Defense Mechanisms" [Symulacja ataków DDoS i mechanizmów obronnych oparta na agentach]*, Journal of Computing*, tom 4, nr 2, 2005.
79. Gasser, L., „Kryptografia postkwantowa", w: V. Mulder, A. Mermoud, V. Lenders i B. Tellenbach (red.), *Trendy w technologiach ochrony danych i szyfrowania,* Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33386-6.10
80. Radanliev, P., „Sztuczna inteligencja i kryptografia kwantowa", *Journal of Analytical Science and Technology,* tom 15, artykuł 4, 2024. https://doi.org/10.1186/s40543-024- 00416-6
81. Atutxa, A., Sanz, A., Sasiain, J., Astorga, J. i Jacob, E., „W kierunku bezpiecznej kwantowo sieci 5G: kwantowa dystrybucja kluczy w sieciach rdzeniowych", *Computer Communications*, tom 224, 2024, str. 145-158. https://doi.org/10.1016Zj.comcom.2024.06.005
82. Ricci, S., Dobias, P., Malina, L., Hajny, J. i Jedlicka, P., „Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography" [Klucze hybrydowe w praktyce: połączenie kryptografii klasycznej, kwantowej i postkwantowej]*, IEEE Access*, tom 12, 2024, str. 23206–23219. https://doi.org/10.1109/ACCESS.2024.3364520
83. Shim, K.-S., Kim, B. i Lee, W., „Badania nad protokołami stosowanymi w kryptografii kwantowej, dystrybucji kluczy i kryptografii postkwantowej w naukach o danych i bezpieczeństwie sieci"*, Journal of Web Engineering*, tom 23, nr 6, wrzesień 2024, str. 813-830. https://doi.org/10.13052/jwe1540-9589.2365
84. Dhar, S., Khare, A., Dwivedi, A. D. i Singh, R., „Zabezpieczanie urządzeń IoT: nowatorskie podejście z wykorzystaniem technologii blockchain i kryptografii kwantowej"*, Internet of Things,* tom 25, 2024, artykuł 101019. https:ZZdoi.org/10.1016Zj.iot.2023.101019

85. Schneier, B., „Systemy kryptograficzne oparte na sieciach i kwantowa kryptoanaliza", *Communications of the ACM,* Online First, czerwiec 2024 r. https://doi.org/10.1145/3665224
86. Bozzio, M., Vyvlecka, M., Cosacchi, M. i in., „Enhancing Quantum Cryptography with Quantum Dot Single-Photon Sources" [Ulepszanie kryptografii kwantowej za pomocą źródeł fotonów pojedynczych kwantów], *npj Quantum Information*, tom 8, artykuł 104, 2022. https://doi.org/10.1038/s41534-022-00626-z
87. Akçay, L. i Yalçın, B. Ö., „Lightweight ASIP Design for Lattice-Based Post-Quantum Cryptography Algorithms" [Lekka konstrukcja ASIP *dla* algorytmów kryptografii postkwantowej opartych na sieciach krystalicznych], *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. i Etxezarreta Martinez, J., „Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective" [Cyberbezpieczeństwo w infrastrukturze krytycznej: perspektywa kryptografii postkwantowej], *IEEE Internet of Things Journal*, tom 11, nr 18, 15 września 2024 r., str. 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.
i Tafur Monroy, I., „Quantum-Resistant Transport Layer Security" [Bezpieczeństwo warstwy transportowej odporne na kwantowe ataki], *Computer Communications*, tom 213, 2024, str. 345-358.
https://doi.org/10.1016/j.comcom.2023.11.010
90. Alhakami, H., „Enhancing IoT Security: Quantum-Level Resilience Against Threats" [Zwiększanie bezpieczeństwa IoT: odporność na zagrożenia na poziomie kwantowym], *Computers, Materials and Continua*, tom 78, nr 1, 2024, str. 329-356. https://doi.org/10.32604/cmc.2023.043439
91. Chawla, D. i Mehra, P. S., „Badanie dotyczące obliczeń kwantowych w zakresie bezpieczeństwa Internetu rzeczy", *Procedia Computer Science*, tom 218, 2023, str. 2191-2200. https://doi.org/10.1016Zj.procs.2023.01.195
92. Hekkala, J., Muurman, M., Halunen, K. i in., „Wdrażanie kryptografii postkwantowej dla programistów", *SN Computer Science*, tom 4, artykuł 365, 2023. https://doi.org/10.1007/s42979-023-01724-1
93. Ji, X., Wang, B., Hu, F., Wang, C. i Zhang, H., „Nowa zaawansowana architektura obliczeniowa
do projektowania i analizy kryptografii za pomocą kwantowego urządzenia annealingowego D-Wave", *Tsinghua Science and Technology,* tom 27, nr 4, sierpień 2022 r., str. 751-759.

https://doi.org/10.26599/TST.2021.9010022
94. Hasan, K. F. i in., „A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies" [Struktura migracji do kryptografii postkwantowej: analiza zależności bezpieczeństwa i studia przypadków], *IEEE Access*, tom 12, 2024, str. 23427–23450. https://doi.org/10.1109/ACCESS.2024.3360412
95. Kong, I., Janssen, M. i Bharosa, N., „Realizacja bezpiecznej wymiany informacji w erze kwantowej: wyzwania związane z wdrożeniem i przyjęciem oraz zalecenia dotyczące polityki w zakresie przejścia na technologie bezpieczne w erze kwantowej", *Government Information Quarterly*, tom 41, nr 1, 2024, artykuł 101884. https://doi.Org/10.1016/j.giq.2023.101884
96. Pan, D. i in., „The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet" [Ewolucja bezpiecznej *komunikacji kwantowej: w* drodze do Qinternetu], *IEEE Communications Surveys and Tutorials*, tom 26, nr 3, 2024, str. 1898–1949. https://doi.org/10.1109/COMST.2024.3367535
97. Hoque, S., Aydeger, A. i Zeydan, E., „Exploring Post-Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design" [Badanie kryptografii postkwantowej z wykorzystaniem kwantowej dystrybucji kluczy w celu zaprojektowania zrównoważonej architektury sieci komórkowej], w: *Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems (PECS '24) [Materiały z 4. warsztatów dotyczących wydajności i efektywności energetycznej w systemach współbieżnych i rozproszonych (PECS '24)*], ACM, Nowy Jork, 2024, s. 9–16. https://doi.org/10.1145/3659997.3660033
98. Piatkowski, J. i Szymoniak, S., „Trivializing Verification of Cryptographic Protocols" [Trywializacja weryfikacji protokołów kryptograficznych], *Computer Assisted Methods in Engineering and Science*, tom 30, nr 4, 2023, str. 389406. https://doi.org/10.24423/cames.869
99. Basin, D. A., Cremers, C. i Meadows, C. A., „Model Checking Security Protocols" [Sprawdzanie modeli protokołów bezpieczeństwa], w: E. Clarke, T. Henzinger, H. Veith i R. Bloem (red.), *Handbook of Model Checking [Podręcznik sprawdzania modeli],* Springer, Cham, 2018, s. 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" [Modelowanie *i weryfikacja protokołów bezpieczeństwa* za pomocą stosowanego rachunku Pi i ProVerif], *Foundations and Trends in Privacy and Security*, tom 1, nr 12, 2016, str. 1-135. https://doi.org/10.1561/3300000004
101. Blanchet, B., Cheval, V. i Cortier, V., „ProVerif z lemmatami, indukcją, szybką subsumacją i wieloma innymi funkcjami", w: *Proceedings of the IEEE*

Symposium on Security and Privacy (S&P 2022), IEEE Computer Society, San Francisco, Kalifornia, 2022, s. 205–222. https://hal.inria.fr/hal-03366962/

102. Bouroulet, R., Devillers, R., Klaudel, H., Pelz, E. i Pommereau, F., „Modelowanie i analiza protokołów bezpieczeństwa przy użyciu specyfikacji opartych na rolach i sieciach Petriego", w: K. M. van Hee i R. Valk (red.), *Applications and Theory of Petri Nets,* Springer, Berlin i Heidelberg, 2008, s. 72-91.

103. Burrows, M., Abadi, M. i Needham, R., „A Logic of Authentication" [Logika uwierzytelniania], *ACM Transactions on Computer Systems,* tom 8, nr 1, 1990, str. 18-36. https://doi.org/10.1145/77648.77649

104. Chevalier, Y. i in., „A High Level Protocol Specification Language for Industrial Security Sensitive Protocols" [Język specyfikacji protokołów wysokiego poziomu dla protokołów wrażliwych pod względem bezpieczeństwa przemysłowego], w: *Proceedings of the Workshop on Specification and Automated Processing of Security Requirements (SAPS 2004) [*Materiały z warsztatów dotyczących *specyfikacji i automatycznego przetwarzania wymagań bezpieczeństwa* (SAPS 2004*)]*, Austriackie Towarzystwo Informatyczne, Linz, Austria, 2004, s. 13.

105. Cortier, V., Delaune, S. i Dreier, J., „Automatic Generation of Source Lemmas in Tamarin: Towards Automatic Proofs of Security Protocols" [Automatyczne generowanie lemmatów źródłowych w Tamarin: w kierunku automatycznego dowodzenia protokołów bezpieczeństwa], w: L. Chen, N. Li, K. Liang i S. Schneider (red.), *Computer Security - ESORICS 2020,* Springer, Cham, 2020, s. 3-22.

106. David, A., Larsen, K. G., Legay, A., Mikucionis, M. i Poulsen, D. B., „UPPAAL SMC Tutorial", *International Journal on Software Tools for Technology Transfer,* tom 17, nr 4, 2015, str. 397-415. https://doi.org/10.1007/s10009-014-0361-y

107. Dolev, D. i Yao, A. C., „On the Security of Public Key Protocols" [O bezpieczeństwie protokołów klucza publicznego], w: *Proceedings of the 22nd Annual Symposium on Foundations of Computer Science (SFCS '81) [Materiały z 22. dorocznego sympozjum poświęconego podstawom informatyki]*, IEEE Computer Society, Waszyngton, 1981, s. 350–357.

108. Gregor, D., Järvi, J., Siek, J., Reis, G., Stroustrup, B. i Lumsdaine, A., „ " („Koncepcje: wsparcie językowe dla programowania generycznego w języku C++"), *ACM SIGPLAN Notices*, tom 41, nr 10, 2006, str. 291-310. https://doi.org/10.1145/1167515.1167499

109. Grosser, A., Kurkowski, M., Piatkowski, J. i Szymoniak, S., „ProToc: uniwersalny język specyfikacji protokołów bezpieczeństwa", w: A. Wilinski, I. E.

Fray i J. Pejas (red.), *Soft Computing in Computer and Information Science,* Advances in Intelligent Systems and Computing, tom 342, Springer, Cham, 2014, s. 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. i Modersheim, S., „A Typing Result for Stateful Protocols" [Wynik typowania dla protokołów stanowych], w: *Proceedings of the IEEE 31st Computer Security Foundations Symposium (CSF 2018) [Materiały z 31. sympozjum IEEE poświęconego podstawom bezpieczeństwa komputerowego (CSF 20*18)], IEEE, 2018, s. 374–388. https://doi.org/10.1109/CSF.2018.00034

112. Järvi, J., Gregor, D., Willcock, J., Lumsdaine, A. i Siek, J., „Algorithm w programowaniu generycznym: wyzwania związane z generycznością ograniczoną w C++", *ACM SIGPLAN Notices*, tom 41, nr 6, 2006, str. 272-282. https://doi.org/10.1145/1133255.1134014

113. Kassem, A., Lafourcade, P., Lakhnech, Y. i Modersheim, S., „Multiple Independent Lazy Intruders" [Wielokrotni niezależni leniwi intruzi], w: *Proceedings of the 1st Workshop on Hot Issues in Security Principles and Trust (HotSpot 2013)*, 2013, 15 stron.

114. Kordy, B., Mauw, S., Radomirovic, S. i Schweitzer, P., „Foundations of AttackDefense Trees" [Podstawy drzew ataku i obrony], w: P. Degano, S. Etalle i J. Guttman (red.), *Formal Aspects in Security and Trust (FAST 2010) [Formalne aspekty bezpieczeństwa i zaufania (FAST 2010)]*, Lecture Notes in Computer Science, tom 6561, Springer, Berlin i Heidelberg, 2010, str. 80-95. https://doi.org/10.1007/978-3-642-19751-2_6

115. Kruse, R. L. i Ryba, A. J., *Struktury danych i projektowanie programów w języku C++,* Prentice-Hall, USA, 1998.

116. Kurkowski, M., *Formalne metody weryfikacji właściwości protokołów bezpieczeństwa w sieciach komputerowych* (w języku polskim), Akademicka Oficyna Wydawnicza Exit, Warszawa, 2013.

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

118. Liu, S., Xiao, T., Liu, J., Wang, X., Wu, J. i Zhu, J., „Visual Diagnosis of Tree Boosting Methods" [Wizualna diagnostyka metod wzmacniania drzew], *IEEE Transactions on Visualization and Computer Graphics*, tom 24, nr 1, 2017, str. 163-173. https://doi.org/10.1109/TVCG.2017.2744378

119. Mauw, S. i Oostdijk, M., „Foundations of Attack Trees" [Podstawy drzew ataków], w: *International Conference on Information Security and Cryptology,* Springer, 2005, , str. 186-198. https://doi.org/10.1007/11734727_17

120. Millen, J. K., „CAPSL: Common Authentication Protocol Specification Language" [CAPSL: wspólny język specyfikacji protokołów uwierzytelniania], w: *Proceedings of the Workshop on New Security Paradigms (NSPW '96) [Materiały z warsztatów dotyczących nowych paradygmatów bezpieczeństwa (NSPW '96)],* 1996. https://doi.org/10.1145/304851.304879
121. Morin, P., *Otwarte struktury danych (w języku C++),* 2013. https://opendatastructures.org/
122. Modersheim, S., Nielson, F. i Nielson, H. R., „Lazy Mobile Intruders" [Leniwi intruzi mobilni], w: D. A. Basin i J. C. Mitchell (red.), *Principles of Security and Trust (POST) [Zasady bezpieczeństwa i zaufania (POST)]*, Lecture Notes in Computer Science, tom 7796, Springer, 2013, str. 147-166.
123. Needham, R. M. i Schroeder, M. D., „Using Encryption for Authentication in Large Networks of Computers" [Wykorzystanie szyfrowania do uwierzytelniania w dużych sieciach komputerowych], *Communications of the ACM*, tom 21, nr 12, 1978, str. 993-999. https://doi.org/10.1145/359657.359659
124. Neuman, B. C. i Ts'o, T., „Kerberos: An Authentication Service for Computer Networks" [*Kerberos: usługa uwierzytelniania* dla sieci komputerowych], *IEEE Communications Magazine*, tom 32, nr 9, 1994, str. 33–38. https://doi.org/10.1109/35.312841
125. Piatkowski, J., „The Conditional Multiway Mapped Tree: Modeling and Analysis of Hierarchical Data Dependencies" [Warunkowe drzewo wielokierunkowe: modelowanie i analiza hierarchicznych zależności danych], *IEEE Access*, tom 8, 2020, str. 74083–74092. https://doi.org/10.1109/ACCESS.2020.2988358
126. Ryan, P. Y. A., Schneider, S. A., Goldsmith, M. H., Lowe, G. i Roscoe, A. W., *The Modelling and Analysis of Security Protocols: The CSP Approach,* Addison-Wesley Professional, Harlow, Londyn, 2000.
127. Siedlecka-Lamch, O., Szymoniak, S. i Kurkowski, M., „Szybka metoda weryfikacji protokołów bezpieczeństwa", w: *Materiały z 18. Międzynarodowej Konferencji poświęconej Systemom Informatycznym i Zarządzaniu Przemysłowemu (CISIM 2019),* Springer, 2019, s. 523-534. https://doi.org/10.1007/978-3-030-28957-7_43
128. Siedlecka-Lamch, O., Szymoniak, S., Kurkowski, M. i Fray, I. E., „W kierunku najbardziej efektywnej metody weryfikacji protokołów bezpieczeństwa bez ograniczeń czasowych", w: *Materiały z 24. konferencji Pacific Asia Conference on Information Systems (PACIS 2020),* Dubaj, Zjednoczone Emiraty Arabskie, 2020, s. 189.
129. Siek, J. G. i Lumsdaine, A., „A Language for Generic Programming in the Large" [Język do programowania generycznego na dużą skalę], *Science of Computer Programming*, tom 76, nr 5, 2011, str. 423-465.

https://doi.org/10.1016/j.scico.2008.09.009
130. Szymoniak, S., „Amelia: nowy protokół bezpieczeństwa chroniący przed fałszywymi
Linkami", *Komunikacja komputerowa*, tom 179, 2021, str. 73-81.
https://doi.org/10.1016/j.comcom.2021.07.030
131. Szymoniak, S., Kurkowski, M. i Piatkowski, J., „Modele czasowe protokołów bezpieczeństwa
uwzględniające opóźnienia w sieci", *Journal of Applied Mathematics and Computational Mechanics,* tom 14, nr 3, 2015, str. 127-139.
https://doi.org/10.17512/jamcm.2015.3.14
132. Tremblay, J.-P. i Sorenson, P. G., *Wprowadzenie do struktur danych z zastosowaniami,* wyd. 2, McGraw-Hill, Auckland, 1984.
133. Witten, I. H., Frank, E. i Hall, M. A., *Data Mining: Practical Machine Learning Tools and Techniques,* wyd. 3, Morgan Kaufmann, Amsterdam, 2011.
134. R. Mustafovski, A. Petrovski i M. Radovanovic, „Integracja technologii kwantowych z mobilnymi systemami wojskowymi i strukturami TOC", *Land Forces Academy Review*, tom XXX, nr 3(119), 2025.
135. R. Mustafovski, „Oparte na formule ramy architektoniczne platformy SecuDroneComm do komunikacji bezzałogowych statków powietrznych", *Management Science Advances*, tom 2, nr 1, str. 288-303, Scientific Oasis, Skopje, Republika Macedonii Północnej, 2025.
136. R. Mustafovski, „Ocena wpływu operacyjnego SecuDroneComm: oparta na symulacji ocena bezpiecznej komunikacji bezzałogowych statków powietrznych w środowiskach wojskowych", *Scientific Technical Review*, tom 75, nr 1, str. 11-18, 2025, doi: 10.5937/str2500002M.
137. M. Mozaffari, W. Saad, M. Bennis i M. Debbah, „Efektywne rozmieszczenie wielu bezzałogowych statków powietrznych w celu uzyskania optymalnego zasięgu sieci bezprzewodowej", *IEEE Communications Letters*, tom 20, nr 8, str. 1647-1650, 2016.
138. L. Ruan i in., „Energooszczędne wdrożenie zasięgu wielu bezzałogowych statków powietrznych w sieciach bezzałogowych statków powietrznych: ramy teorii gier", *China Communications*, tom 15, nr 10, str. 194209, 2018.
139. M. Mozaffari, W. Saad, M. Bennis i M. Debbah, „Mobilne bezzałogowe statki powietrzne (UAV) do energooszczędnej komunikacji w Internecie rzeczy", *IEEE Transactions on Wireless Communications*, 2017.
140. S.-Y Lien, K.-C. Chen i Y. Lin, „W kierunku powszechnego dostępu masowego w komunikacji między maszynami 3GPP", *IEEE Communications Magazine*, tom 49, nr 4, str. 66-74, kwiecień 2011 r.
141. M. Malik i S. K. Garg, „W kierunku 6G: ewolucja sieci poza 5G i scenariusz indyjski", w: *Proc. 2nd Int. Conf. Innovative Practices in Technology and*

Management (ICIPTM), Gautam Buddha Nagar, Indie, str. 123-127, 2022.
142. M. A. Khan i in., „Rój bezzałogowych statków powietrznych do zarządzania siecią w 6G: przegląd techniczny", *IEEE Transactions on Network and Service Management,* tom 20, nr 1, str. 741761, marzec 2023 r.
143. S. Dang, O. Amin, B. Shihada i M.-S. Alouini, „Czym powinno być 6G?", *Nature Electronics*, tom 3, nr 1, str. 20-29, 2020.
144. F. Ronaldo, D. Pramadihanto i A. Sudarsono, „Bezpieczny system komunikacji usług dronów wykorzystujący kryptografię hybrydową w sieci 4G/LTE", w: *Proc. Int. Electronics Symposium (IES),* Surabaya, Indonezja, str. 116-122, 2020.
145. T. Li i in., „Bezpieczna komunikacja między bezzałogowymi statkami powietrznymi a pojazdami", *IEEE Transactions on Communications*, tom 69, nr 8, str. 5381-5393, sierpień 2021 r.
146. S. A. Ayati i H. R. Naji, „Bezpieczny mechanizm ochrony komunikacji UAV", w: *Proc. 9th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS),* Bam, Iran, str. 1-6, 2022.
147. D. Pirker, T. Fischer, C. Lesjak i C. Steger, „Globalny i bezpieczny system uwierzytelniania bezzałogowych statków powietrznych oparty na zabezpieczeniach sprzętowych", w: *Proc. 8th IEEE Int. Conf. Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, Oxford, Wielka Brytania, str. 84-89, 2020.
148. H. Wang, H. Fang i X. Wang, „Edge intelligence enabled soft decentralized authentication in UAV swarm" [Zdecentralizowane uwierzytelnianie oparte na inteligencji brzegowej w roju bezzałogowych statków powietrznych], w: *Proc. IEEE/CIC Int. Conf. Communications in China (ICCC)*, Xiamen, Chiny, str. 86-91, 2021.
149. M. Markowski, P. Ryba i K. Puchala, „Laboratorium badawcze sieci definiowanych programowo: eksperymentalne topologie i scenariusze", w: *Proc. 3rd European Network Intelligence Conf. (ENIC),* Wrocław, Polska, str. 252-256, 2016.
150. M. A. B. S. Abir, M. Z. Chowdhury i Y. M. Jang, „Sieci bezzałogowych statków powietrznych definiowane programowo dla systemów 6G: wymagania, możliwości, nowe techniki, wyzwania i kierunki badań", *IEEE Open Journal of the Communications Society,* tom 4, str. 2487-2547, 2023.
151. M. Ouadah i F. Merazka, „Podejście oparte na kodowaniu sieciowym dla niezawodnych sieci bezzałogowych statków powietrznych opartych na SDN", w: *Proc. 5th Int. Conf. Electrical Engineering and Control Applications (ICEECA '22),* Khenchela, Algieria, 2022.

Biografia Rexhepa Mustafovskiego, mgr

Rexhep Mustafovski, magister, jest urzędnikiem w Ministerstwie Obrony Republiki Macedonii Północnej oraz asystentem dydaktycznym i naukowym w Akademii Wojskowej „Generała Mihailo Apostolskiego" w Skopje, gdzie pracuje w Departamencie Cyberbezpieczeństwa i Kryminalistyki Cyfrowej. Jest specjalistą w dziedzinie bezpiecznych systemów komunikacyjnych, cyberbezpieczeństwa i integracji technologii obronnych, a jego doświadczenie akademickie i zawodowe obejmuje bezpieczną komunikację taktyczną, bezpieczeństwo sieci i nowe systemy informatyczne.

Ukończył studia licencjackie w Akademii Wojskowej im. generała Mihailo Apostolskiego w Skopje, gdzie uzyskał tytuł oficera łączności. Podczas studiów wykazał się wyjątkowymi wynikami w nauce i dyscypliną zawodową, osiągając najwyższe wyniki edukacyjne w swoim roczniku. W uznaniu tego osiągnięcia został oficjalnie wyróżniony tytułem najlepszego oficera swojego rocznika, nadanym przez prezydenta kraju. Wyróżnienie to odzwierciedla zarówno jego doskonałe wyniki w nauce, jak i zaangażowanie w profesjonalizm wojskowy.

Po uzyskaniu stopnia oficerskiego kontynuował rozwój akademicki, podejmując studia magisterskie na Wydziale Elektrotechniki i Technologii Informacyjnych Uniwersytetu „Ss. Cyril and Methodius" w Skopje. Uzyskał tytuł magistra nauk ścisłych w dziedzinie technologii komunikacyjnych i informacyjnych, specjalizując się w nowoczesnych systemach komunikacyjnych, bezpieczeństwie informacji i zaawansowanych koncepcjach sieciowych. Studia magisterskie jeszcze bardziej wzmocniły jego zdolności analityczne i badawcze, szczególnie w obszarach bezpiecznej komunikacji i systemów obronnych opartych na technologii.

Jego kariera akademicka i zawodowa łączy formalne wykształcenie wojskowe z zaawansowanymi studiami inżynierskimi, zapewniając solidne podstawy do badań i praktycznej pracy w zakresie bezpiecznej komunikacji wojskowej. To doświadczenie ma wpływ na jego podejście do projektowania systemów

komunikacyjnych, kładące nacisk na niezawodność, bezpieczeństwo, interoperacyjność i znaczenie operacyjne. Wiedza i doświadczenie zdobyte zarówno podczas szkolenia wojskowego, jak i studiów inżynierskich stanowią podstawę perspektyw przedstawionych w niniejszej książce.