Systèmes de communication sécurisés pour les opérations militaires modernes

Cet ouvrage propose un examen complet des systèmes de communication sécurisés pour les opérations militaires modernes, en abordant les défis technologiques et opérationnels de l'échange d'informations sur les champs de bataille contemporains et futurs. Il retrace l'évolution des communications militaires, des systèmes analogiques et numériques aux architectures cryptées, définies par logiciel et améliorées par l'IA, en mettant l'accent sur l'interopérabilité de l'OTAN, les menaces de cybersécurité et la guerre électronique. Les principes fondamentaux tels que la transmission des signaux, le cryptage, l'authentification, les techniques anti-brouillage et les réseaux radio tactiques résilients sont analysés. Les sujets avancés comprennent les communications sécurisées entre les drones et les centres de commandement, le routage et la gestion du spectre pilotés par l'IA, les systèmes satellitaires, les applications militaires 5G/6G, la communication quantique et les réseaux radio cognitifs. Le livre propose également un cadre de communication sécurisée orienté vers l'avenir et intégré aux systèmes C4ISR, étayé par des études de cas pratiques, y compris la recherche doctorale de l'auteur. Il s'adresse aux chercheurs, aux professionnels de l'armée, aux ingénieurs et aux décideurs qui recherchent des solutions de communication résilientes et intelligentes pour la défense.

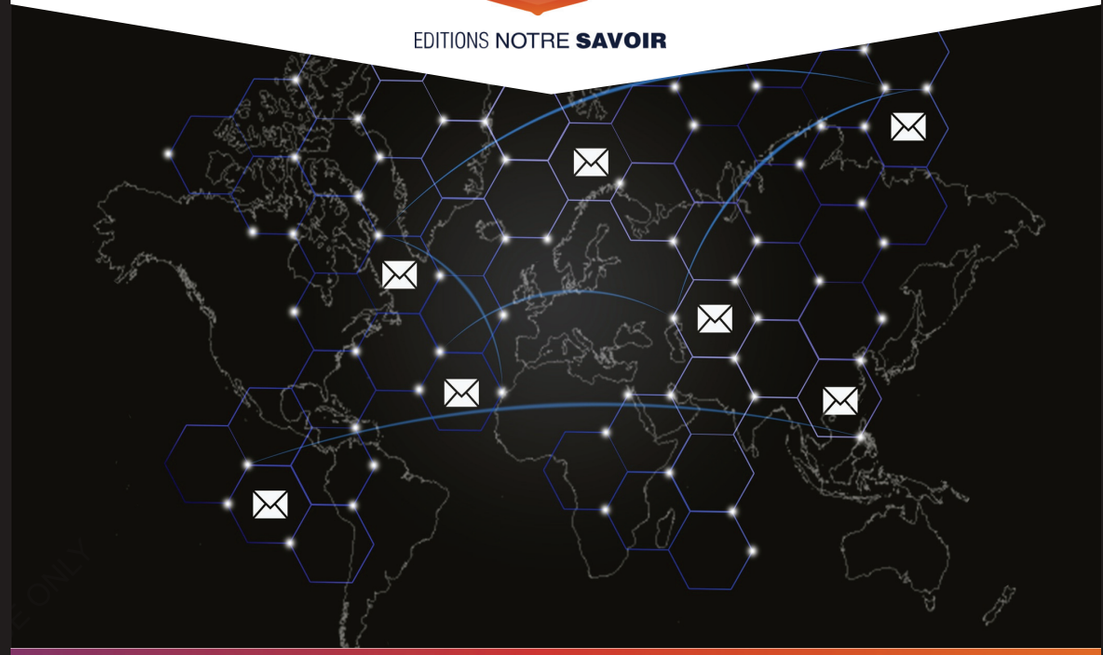
Rexhep Mustafovski, MSc, est officier de transmission et chercheur en communications militaires. Il est titulaire d'une licence de l'Académie militaire "General Mihailo Apostolski" de Skopje et d'une maîtrise en technologies de la communication et de l'information de l'université "Ss. Cyril et Methodius".

9 786209 570445

EDITIONS NOTRE SAVOIR

Rexhep Mustafovski

EDITIONS NOTRE SAVOIR



Systèmes de communication sécurisés pour les opérations militaires modernes

Fondements, technologies et orientations futures

Rexhep Mustafovski

Rexhep Mustafovski

Systèmes de communication sécurisés pour les opérations militaires modernes

Rexhep Mustafovski

Systèmes de communication sécurisés pour les opérations militaires modernes

Fondements, technologies et orientations futures

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: 978-620-9-57044-5

Systèmes de communication sécurisés pour les opérations militaires modernes : fondements, technologies et orientations futures

Table des matières

Préface

Je m'appelle Rexhep Mustafovski, je suis titulaire d'un master en sciences, et cet ouvrage est le fruit de mon engagement académique, professionnel et de recherche dans le domaine des systèmes de communication modernes, avec un accent particulier sur les applications sécurisées à vocation militaire et de défense. La motivation qui m'a poussé à écrire cet ouvrage découle de l'importance croissante des technologies de pointe dans le façonnement de la société contemporaine et, plus précisément, dans la transformation de la manière dont les forces armées communiquent, se coordonnent et opèrent dans des environnements complexes et contestés.

Dans le monde moderne, la technologie n'est plus un élément périphérique de l'activité humaine, mais un moteur central du changement dans les domaines économique, social et sécuritaire. Les technologies de communication, en particulier, sont devenues fondamentales pour la manière dont l'information est générée, transmise, protégée et exploitée. Dans le contexte militaire, la sécurité des communications n'est pas seulement une exigence technique, mais une nécessité stratégique. La capacité à échanger des informations de manière sécurisée, fiable et en temps réel a une influence directe sur l'efficacité opérationnelle, la prise de décision et la protection des forces. Cet ouvrage a été rédigé dans le but de présenter ces réalités à un public universitaire et professionnel plus large, en établissant un lien entre les fondements théoriques et les applications militaires pratiques.

Ma formation universitaire en technologies de la communication et de l'information, combinée à mon engagement professionnel dans l'enseignement et la recherche militaires, a façonné la perspective adoptée dans cet ouvrage. Tout au long de mes études et de mes activités de recherche, j'ai observé un écart récurrent entre les technologies de communication en rapide évolution et leur intégration structurée au niveau des systèmes dans les cadres militaires. Si de nombreux travaux se concentrent sur des technologies isolées ou des solutions techniques spécifiques, rares sont ceux qui tentent de présenter une vision globale et intégrée des systèmes de communication militaire sécurisés en tant qu'architectures en évolution. Cet ouvrage vise à combler cette lacune en proposant un examen cohérent et structuré des technologies, des mécanismes de sécurité et des principes architecturaux qui sous-tendent les communications militaires modernes et futures.

Le livre s'appuie également sur mes recherches doctorales en cours, qui se concentrent sur les cadres de communication sécurisés et les plateformes de communication avancées pour les applications de défense. Une partie de ces recherches est intégrée dans le livre sous la forme d'une étude de cas dédiée, qui présente un exemple pratique de la manière dont les concepts théoriques et les

principes architecturaux peuvent être appliqués à un système réel. Cette étude de cas, issue de mes travaux de doctorat, est incluse afin d'illustrer la transition entre l'analyse conceptuelle et la conception et la mise en œuvre du système. Son objectif n'est pas de fournir une solution définitive, mais plutôt d'illustrer comment les plateformes de communication sécurisées peuvent être structurées pour répondre aux exigences opérationnelles telles que la sécurité, la fiabilité, la latence et l'interopérabilité.

En rédigeant cet ouvrage, j'ai cherché à maintenir un équilibre entre rigueur académique et pertinence pratique. Le contenu s'appuie sur des principes établis en matière d'ingénierie des communications, de cybersécurité et de systèmes militaires, tout en reflétant les tendances technologiques actuelles telles que l'intelligence artificielle, les radios définies par logiciel, les systèmes sans pilote, les communications par satellite et les mécanismes de sécurité émergents. L'intention n'était pas de produire un texte purement théorique, ni un manuel strictement technique, mais un ouvrage académique structuré pouvant servir de référence aux étudiants, chercheurs, ingénieurs et professionnels militaires intéressés par la conception et l'évolution des systèmes de communication sécurisés.

Le public visé par cet ouvrage est donc volontairement large, englobant les étudiants de deuxième et troisième cycles en ingénierie et dans les disciplines liées à la défense, les chercheurs travaillant dans les domaines de la communication et de la sécurité, ainsi que les praticiens impliqués dans la planification des communications militaires, le développement de systèmes et le déploiement opérationnel. Dans le même temps, l'ouvrage est rédigé avec suffisamment de profondeur et d'esprit analytique pour soutenir des études universitaires avancées et contribuer aux discussions en cours au sein de la communauté scientifique.

Enfin, cet ouvrage représente une étape dans un long parcours universitaire et professionnel. Il reflète à la fois des recherches achevées et des investigations en cours, reconnaissant que le domaine des communications militaires est dynamique et en constante évolution. Les technologies, architectures et cadres discutés dans cet ouvrage continueront sans aucun doute à se développer en réponse aux nouvelles exigences opérationnelles et aux menaces émergentes. J'espère que cet ouvrage contribuera à une meilleure compréhension des systèmes de communication sécurisés et encouragera la poursuite des recherches, des discussions et de l'innovation dans ce domaine critique.

Introduction

Les systèmes de communication militaires ont toujours joué un rôle déterminant dans la conduite des opérations militaires, en façonnant la manière dont les forces coordonnent, décident et agissent dans les environnements opérationnels. Depuis les premières formes de signalisation sur le champ de bataille jusqu'aux architectures mondiales en réseau et basées sur les données d'aujourd'hui, la communication est restée un élément central du commandement, du contrôle et de l'efficacité opérationnelle. Dans les opérations militaires contemporaines, cependant, les systèmes de communication ont évolué au-delà de leur rôle traditionnel de soutien et constituent désormais une capacité stratégique à part entière. Des infrastructures de communication sécurisées, résilientes et adaptables sont essentielles pour atteindre la supériorité en matière d'information, maintenir le rythme opérationnel et garantir la survie des forces dans des environnements de plus en plus complexes et contestés.

La transformation de la guerre au XXIe siècle a introduit de nouveaux défis qui modifient fondamentalement les exigences imposées aux systèmes de communication militaires. Les opérations modernes se caractérisent par une grande mobilité, des engagements multidomaines et l'intégration d'activités de guerre conventionnelle, cybernétique et informationnelle. Les forces opèrent sur les domaines terrestre, aérien, maritime, spatial et cybernétique, souvent simultanément et en coordination avec des partenaires interarmées et de coalition. Dans de telles conditions, la capacité à échanger des informations précises, opportunes et protégées détermine non seulement le succès tactique, mais aussi les résultats stratégiques. Les systèmes de communication doivent donc fonctionner de manière fiable dans des conditions d'incertitude, de perturbation et d'interférence active de la part de l'adversaire.

L'une des caractéristiques déterminantes des communications militaires modernes est la place centrale accordée à la sécurité. À mesure que les réseaux de communication deviennent plus interconnectés et pilotés par des logiciels, ils sont de plus en plus exposés aux cyberattaques, à la guerre électronique et à l'exploitation par des adversaires. La confidentialité, l'intégrité, la disponibilité et l'authenticité des informations ne sont plus des concepts techniques abstraits, mais des nécessités opérationnelles. La compromission des systèmes de communication peut entraîner la désinformation, la perte de l'autorité de commandement, l'échec de la mission ou une escalade involontaire. Par conséquent, les considérations de sécurité doivent être intégrées à tous les niveaux de la conception des systèmes de communication, des mécanismes de transmission physique aux architectures réseau et aux services au niveau des applications.

Dans le même temps, l'innovation technologique s'accélère à un rythme sans précédent. Les progrès réalisés dans les domaines des communications numériques, de la cryptographie, de l'intelligence artificielle, des systèmes satellitaires et des technologies émergentes telles que la communication quantique remodèlent rapidement le paysage des communications militaires. Ces développements offrent des opportunités significatives pour améliorer les performances, la résilience et l'adaptabilité, mais ils introduisent également de nouvelles vulnérabilités et complexités. Les institutions militaires doivent donc trouver un équilibre entre l'adoption de technologies avancées et une conception architecturale rigoureuse, une discipline opérationnelle et une responsabilité éthique.

Cet ouvrage est motivé par la nécessité de fournir une analyse complète et intégrée des systèmes de communication militaire sécurisés dans le contexte des opérations de défense modernes et futures. Plutôt que de se concentrer sur des technologies isolées ou des problèmes techniques restreints, l'ouvrage adopte une perspective au niveau du système qui considère la communication comme un cadre interconnecté impliquant le matériel, les logiciels, les mécanismes de sécurité, la doctrine opérationnelle et la prise de décision humaine. L'objectif est de présenter une compréhension cohérente de la manière dont les systèmes de communication sécurisés sont conçus, déployés et évoluent pour répondre aux exigences de la guerre contemporaine.

Les premiers chapitres établissent le contexte fondamental de la discussion. Les communications militaires modernes sont examinées à travers leur évolution historique, depuis les systèmes analogiques et point à point jusqu'aux architectures numériques, cryptées et en réseau. Cette évolution reflète des changements plus larges dans la doctrine militaire, le rythme des opérations et les besoins en matière d'information. L'importance des communications sécurisées est soulignée non seulement en termes de protection des informations, mais aussi pour permettre une action militaire coordonnée et légale. Le rôle de la normalisation, en particulier dans le cadre des alliances, est mis en avant comme un facteur essentiel pour garantir l'interopérabilité et la cohésion opérationnelle entre les forces alliées.

Le livre explore ensuite les principes fondamentaux qui sous-tendent les systèmes de communication sécurisés. La transmission et la propagation des signaux, ainsi que les défis liés à la communication en ligne de mire et hors ligne de mire, sont examinés afin d'établir une base technique. Ces principes restent pertinents malgré les progrès technologiques, car les contraintes physiques et les facteurs environnementaux continuent d'influencer les performances de communication. Sur cette base, l'ouvrage analyse les mécanismes de sécurité fondamentaux tels que le cryptage, l'authentification, le contrôle d'accès et les techniques anti-brouillage. Ces éléments constituent l'épine dorsale des architectures de communication

sécurisées et sont essentiels pour maintenir la fiabilité et la confiance dans des environnements contestés.

La cybersécurité apparaît comme un thème central dans les chapitres suivants. Les réseaux de communication militaires sont de plus en plus la cible de cybermenaces sophistiquées qui cherchent à perturber les opérations, à exfiltrer des informations sensibles ou à manipuler les processus décisionnels. Le livre examine la nature de ces menaces et les stratégies utilisées pour les atténuer, notamment le renforcement des réseaux, la sélection de protocoles cryptographiques, les architectures « zero trust » et les mécanismes de réponse aux incidents. En abordant la cybersécurité à la fois au niveau technique et architectural, le livre souligne l'importance de la résilience et de l'adaptabilité face à des menaces persistantes et en constante évolution.

Les systèmes de communication radio restent la pierre angulaire des opérations tactiques, et leur rôle est examiné en profondeur. Les systèmes VHF, UHF et HF traditionnels continuent de fournir des capacités essentielles, en particulier dans les environnements où les infrastructures sont limitées ou dégradées. L'intégration de ces systèmes avec des radios définies par logiciel et des techniques de réseau maillé illustre comment les technologies existantes peuvent être améliorées grâce à des approches architecturales modernes. L'interopérabilité avec les forces alliées est considérée comme une exigence clé, reflétant les réalités des opérations conjointes et de coalition dans les scénarios de conflit contemporains.

L'utilisation croissante des systèmes aériens sans pilote introduit de nouvelles dimensions dans les communications militaires. Les drones servent de collecteurs de données, de relais de communication et de plates-formes opérationnelles qui étendent la portée et la flexibilité des réseaux militaires. Le livre analyse les défis de sécurité associés à la communication entre les drones et les centres de commandement, notamment le cryptage, l'authentification, la protection de la couche liaison et les contraintes de performance telles que la latence et la fiabilité. Une étude de cas spécifique présente une plateforme de communication sécurisée intégrée, illustrant comment les concepts théoriques peuvent être appliqués dans la pratique pour répondre aux exigences opérationnelles du monde réel.

L'intelligence artificielle représente une force de transformation dans les systèmes de communication militaires. Le livre explore comment les techniques d'IA peuvent améliorer l'efficacité du routage, la détection des intrusions, l'attribution des fréquences et la gestion des réseaux dans les environnements de combat. En permettant aux systèmes de détecter, d'apprendre et de s'adapter, les architectures de communication basées sur l'IA offrent de nouveaux niveaux de résilience et d'efficacité opérationnelle. Dans le même temps, l'intégration de l'IA soulève d'importantes questions liées à la transparence, à la responsabilité et au contrôle,

qui sont abordées à travers une analyse équilibrée et critique.

Les technologies émergentes constituent un autre point central du livre. Les réseaux cellulaires de nouvelle génération, les communications par satellite, la distribution de clés quantiques et les réseaux radio cognitifs sont examinés en tant que catalyseurs des futures capacités de communication militaire. Ces technologies élargissent l'enveloppe opérationnelle en prenant en charge des débits de données plus élevés, une connectivité mondiale, une sécurité renforcée et une utilisation intelligente du spectre. Leur intégration dans les systèmes militaires reflète une évolution vers une architecture hybride qui combine des composants terrestres, aériens, maritimes et spatiaux dans un cadre de communication unifié.

Les derniers chapitres synthétisent ces développements technologiques et conceptuels dans une discussion plus large sur la manière dont des cadres de communication sécurisés peuvent être construits pour l'armée du futur. Les exigences des forces modernes sont analysées en termes de résilience, d'interopérabilité, d'évolutivité et de sécurité. Des principes architecturaux sont présentés pour illustrer comment des systèmes de communication tactique sécurisés peuvent être conçus pour soutenir des opérations complexes et distribuées. L'intégration avec les systèmes C4ISR est soulignée comme un facteur essentiel pour atteindre la supériorité en matière d' s sur la situation et de prise de décision. Les considérations éthiques et juridiques sont abordées afin de garantir que l'innovation technologique s'aligne sur les normes et les responsabilités établies. La discussion sur les tendances futures offre une perspective prospective sur la manière dont les systèmes de communication militaires sont susceptibles d'évoluer en réponse aux menaces émergentes et aux opportunités technologiques.

Ce livre s'adresse aux professionnels de l'armée, aux ingénieurs de la défense, aux chercheurs et aux étudiants diplômés engagés dans l'étude et le développement de systèmes de communication sécurisés. Il est également pertinent pour les responsables politiques et les décideurs impliqués dans la planification de la défense et le développement des capacités. En combinant l'analyse technique avec des perspectives architecturales et opérationnelles, cet ouvrage cherche à combler le fossé entre la théorie et la pratique dans le domaine des communications militaires.

Cet ouvrage vise à contribuer à la compréhension et au développement de systèmes de communication militaires sécurisés en présentant une perspective intégrée et tournée vers l'avenir. Alors que la guerre continue d'évoluer en termes de complexité et d'ampleur, la capacité à communiquer de manière sécurisée, fiable et intelligente restera un facteur décisif dans l'efficacité militaire. Grâce à son examen complet des technologies, de l'architecture et des principes, cet ouvrage vise à fournir une base pour la construction de systèmes de communication qui

soutiennent le succès opérationnel tout en garantissant la sécurité, la résilience et la responsabilité dans les opérations militaires modernes et futures.

Conclusion

Cet ouvrage a examiné l'évolution, la structure et l'orientation future des systèmes de communication militaire sécurisés dans le contexte des opérations de défense modernes et émergentes. Tout au long de ses chapitres, il a démontré que les communications militaires ne sont plus seulement des technologies de soutien, mais constituent un pilier central de l'efficacité opérationnelle, de la prise de décision stratégique et de la supériorité en matière d'information. La complexité croissante de l'environnement sécuritaire, combinée à des progrès technologiques rapides, nécessite des cadres de communication résilients, intelligents, interopérables et fondés sur l'éthique.

Les premiers chapitres ont établi l'importance fondamentale des communications sécurisées dans les opérations militaires. Les forces armées modernes opèrent dans des conditions d'incertitude, de mobilité et de menace persistante, où la capacité à échanger des informations précises et opportunes détermine le succès ou l'échec d'une mission. La transition des systèmes analogiques et isolés vers des architectures de communication numériques, cryptées et en réseau reflète une évolution plus large vers une guerre centrée sur l'information. Cette évolution a transformé les systèmes de communication en facilitateurs actifs du commandement, du contrôle et de la coordination dans tous les domaines d'opération.

Le thème central de cet ouvrage est la relation indissociable entre communication et sécurité. À mesure que les réseaux militaires deviennent plus interconnectés et pilotés par des logiciels, ils sont de plus en plus exposés aux cybermenaces, à la guerre électronique et à l'exploitation hostile. L'analyse du cryptage, de l'authentification, du contrôle d'accès et du renforcement des réseaux a mis en évidence la nécessité d'intégrer des mécanismes de sécurité à tous les niveaux des architectures de communication. Plutôt que de traiter la sécurité comme un ajout, les systèmes militaires modernes doivent adopter une approche de sécurité dès la conception qui garantit la confidentialité, l'intégrité, l'authenticité et la disponibilité dans des conditions difficiles.

La discussion sur les systèmes de communication radio pour les unités tactiques a démontré que les technologies existantes restent pertinentes sur le plan opérationnel lorsqu'elles sont intégrées dans une architecture moderne. Les systèmes VHF, UHF et HF continuent d'offrir des capacités de communication robustes, en particulier dans des environnements dégradés ou interdits. Associées à des radios définies par logiciel et aux principes des réseaux maillés, ces technologies offrent une flexibilité et une résilience essentielles aux opérations tactiques. La capacité à adapter les formes d'onde, les fréquences et les stratégies de routage permet aux forces de

maintenir leur connectivité malgré la mobilité, les contraintes du terrain et les interférences hostiles.

Les systèmes aériens sans pilote et leur intégration dans des cadres de communication sécurisés ont été examinés comme une caractéristique déterminante des opérations militaires contemporaines. Les drones fonctionnent non seulement comme des plateformes de détection, mais aussi comme des nœuds de communication d' s dynamiques qui étendent la portée du réseau et améliorent la connaissance de la situation. L'analyse des communications entre les drones et le centre de commandement a souligné l'importance du cryptage, de l'authentification, de la sécurité de la couche liaison et de l'optimisation des performances. L'étude de cas présentée a illustré comment une plateforme de communication intégrée et sécurisée peut prendre en charge l'échange de données en temps réel tout en répondant aux contraintes de latence, de fiabilité et de débit dans les environnements opérationnels.

L'intelligence artificielle est apparue comme une force de transformation dans les systèmes de communication militaires. L'exploration du routage, de la détection des intrusions, de l'allocation du spectre et de la mise en réseau sur le champ de bataille basés sur l'IA a démontré comment des algorithmes intelligents peuvent améliorer l'adaptabilité et la résilience. L'IA permet aux systèmes de communication de réagir de manière dynamique aux changements environnementaux et aux actions hostiles, réduisant ainsi la charge cognitive des opérateurs humains et améliorant le rythme opérationnel. Dans le même temps, l'intégration de l'IA soulève d'importantes questions liées à la transparence, à la responsabilité et au contrôle, renforçant la nécessité d'une mise en œuvre responsable et bien gérée.

Les technologies émergentes telles que les réseaux cellulaires de nouvelle génération, les communications par satellite, la distribution de clés quantiques et les réseaux radio cognitifs ont été analysées comme des catalyseurs des futures capacités de communication militaire. Ces technologies élargissent l'enveloppe opérationnelle en prenant en charge des débits de données plus élevés, une connectivité mondiale, une sécurité renforcée et une utilisation intelligente du spectre. Leur intégration dans les systèmes militaires reflète une évolution vers des architectures hybrides combinant des composants terrestres, aériens, maritimes et spatiaux. Cette convergence permet des opérations multidomaines tout en introduisant de nouveaux défis architecturaux et sécuritaires qui doivent être abordés de manière holistique.

Les derniers chapitres se sont concentrés sur la mise en place d'un cadre de communication sécurisé pour l'armée du futur. L'analyse a souligné que les progrès technologiques ne suffisent pas à eux seuls sans une conception architecturale cohérente, une intégration avec les systèmes C4ISR et la prise en compte des

implications éthiques et juridiques. Les futurs cadres de communication doivent prendre en charge l'interopérabilité, l'évolutivité et la résilience tout en restant conformes au droit international et aux principes éthiques. L'intégration de considérations relatives à la gouvernance, à la responsabilité et à la durabilité garantit que les systèmes de communication contribuent à la sécurité et à la stabilité à long terme plutôt qu'à un simple avantage tactique à court terme.

L'une des principales conclusions de ce travail est que les futurs systèmes de communication militaires doivent être des écosystèmes adaptatifs plutôt que des infrastructures statiques. La nature dynamique des conflits modernes exige des systèmes capables de se reconfigurer en fonction de l'évolution des exigences des missions, des conditions environnementales et des vecteurs de menace. Cette adaptabilité nécessite une intégration étroite entre les technologies de communication, les mécanismes de sécurité, les systèmes de contrôle intelligents et les décideurs humains. Le succès opérationnel de ces systèmes dépend non seulement de l'excellence technique, mais aussi de l'alignement doctrinal et de la préparation organisationnelle.

Une autre conclusion importante est l'importance croissante de l'interopérabilité et des opérations de coalition. Les missions militaires modernes sont de plus en plus menées dans des contextes multinationaux, ce qui nécessite des systèmes de communication permettant un partage contrôlé des informations tout en préservant les intérêts nationaux en matière de sécurité. La normalisation, les cadres de sécurité partagés et les mécanismes de contrôle d'accès flexibles sont essentiels pour une collaboration efficace. Les architectures de communication qui prennent en charge l'interopérabilité dès leur conception constituent une base pour la confiance et la cohérence opérationnelle entre les forces alliées.

Les dimensions éthiques et juridiques des technologies de communication militaire représentent un domaine de responsabilité crucial pour les concepteurs, les opérateurs et les décideurs politiques. À mesure que les systèmes de communication deviennent plus autonomes et intégrés aux fonctions d'aide à la décision, les conséquences potentielles des défaillances ou des utilisations abusives des systèmes augmentent. L'intégration de considérations éthiques et de la conformité juridique dans la conception des systèmes garantit que la supériorité technologique ne porte pas atteinte à la légitimité ou à la responsabilité. L'innovation responsable dans le domaine des communications militaires doit trouver un équilibre entre l'efficacité opérationnelle et le respect des normes et des valeurs établies.

Cet ouvrage contribue à ce domaine en offrant une perspective globale et intégrée sur les systèmes de communication militaire sécurisés. Plutôt que de se concentrer sur des technologies isolées, il met l'accent sur la cohérence architecturale, l'intégration de la sécurité et la conception orientée vers l'avenir. La combinaison

d'analyses théoriques, de considérations pratiques et d'études de cas offre un cadre structuré pour comprendre et développer les infrastructures de communication militaire modernes.

D'un point de vue académique, cet ouvrage fournit une base pour des recherches plus approfondies sur les architectures de communication adaptatives, la gestion de réseau basée sur l'IA et les systèmes quantiques sécurisés. D'un point de vue opérationnel, il offre un aperçu des défis et des opportunités liés au déploiement de technologies de communication sécurisées dans des environnements complexes. Les concepts présentés peuvent éclairer l'élaboration de doctrines, la conception de systèmes et la formulation de politiques dans les institutions de défense.

En conclusion, les systèmes de communication militaire sécurisés sont un facteur décisif dans la guerre moderne et future. Alors que les forces armées sont confrontées à des environnements opérationnels de plus en plus complexes et contestés, la capacité à échanger des informations de manière sécurisée, fiable et intelligente restera un impératif stratégique. En adoptant des cadres de communication intégrés, adaptatifs et fondés sur l'éthique, les armées futures pourront atteindre la supériorité en matière d'information tout en conservant leur résilience, leur légitimité et leur efficacité opérationnelle. Cet ouvrage vise à contribuer à cet objectif en proposant un examen structuré et prospectif des technologies, de l'architecture et des principes d' s qui façonneront l'avenir des communications militaires.

Références

1. Defence Strategic Communications, *journal officiel du Centre d'excellence pour la communication stratégique de l'OTAN,* vol. 10, printemps-automne 2021, NATO StratCom COE, Riga, Lettonie.
2. Polovic, J., « Challenges of Global Communication: Strategic Competition and Escalation of Tensions in International Relations », *Collected Papers of the Faculty of Philosophy,* vol. 48, n° 1, 2024, p. 51-57. https://doi.org/10.5671/ca.48.1.7
3. Mustafovski, R., « The Use of Communication Platforms in Military Operations: Enhancing Strategic and Tactical Effectiveness », *Database Systems Journal,* vol. XVI, 2025, Faculté d'ingénierie électrique et des technologies de l'information, Université Ss. Cyril et Methodius, Skopje, République de Macédoine du Nord.
4. Rienzi, T. M., *Communications-Electronics 1962-1970,* Vietnam Studies Series, Département de l'armée, Washington, DC, États-Unis, 2002.
5. Mazzenga, F., Landry, R. et Young, K., « Communications militaires », *IEEE Communications Magazine,* octobre 2020, pp. 50-56.
6. Organisation du Traité de l'Atlantique Nord (OTAN), *Doctrine interarmées alliée pour les systèmes de communication et d'information (AJP-6),* édition B, version 1, Bureau de normalisation de l'OTAN (NSO), avril 2024.
7. Département de la Défense des États-Unis, *Stratégie de modernisation C3 : commandement, contrôle et communications,* Washington, DC, États-Unis, septembre 2020.
8. Monteiro Marques, M., « STANAG 4586 - Interfaces standard du système de contrôle des drones (UCS) pour l'interopérabilité des drones de l'OTAN », document technique de l'OTAN, Escola Naval - Afeite, Portugal.
9. Yarnell, A. M., Dullea, C. et Grunberg, N. E., « Communication militaire », dans *Communication militaire et médicale,* chapitre 11, Commandement de la recherche et du développement médicaux de l'armée américaine, États-Unis.
10. Timofte, G., « Modernisation des systèmes de communication militaires conformément aux nouvelles exigences opérationnelles, informationnelles et techniques du champ de bataille », *Bulletin scientifique de l'Académie des scientifiques roumains,* Bucarest, Roumanie.
11. Hayes, C., *Accords de normalisation de l'OTAN (STANAG) pour les commandants et l'état-major,* News from the Front, Centre d'apprentissage de l'armée (CALL), Armée américaine, avril 2019.
12. Sánchez, R., Evans, J. et Minden, G., « Networking on the Battlefield: Challenges in Highly Dynamic Multi-hop Wireless Networks », *Actes de la conférence IEEE MILCOM 1999,* Atlantic City, New Jersey, États-Unis, octobre

1999.
13. Kumar, D., « Challenges of a Digitised Battlefield », *Journal of the United Service Institution of India,* vol. CXLII, n° 590, octobre-décembre 2012.
14. Lipscomb, P., « The Evolution of Communications in the Military as it Relates to Leadership », *Études intégrées,* document n° 90, Murray State University, 2017. Disponible à l'adresse : https://digitalcommons.murraystate.edu/bis437/90
15. Amin, M. G., Lindsey, A. R., Zhao, L., et Zhang, Y., *Anti-Jamming Techniques for GPS Receivers,* Rapport technique final AFRL-IF-RS-TR-2001-186, Laboratoire de recherche de l'armée de l'air, site de recherche de Rome, New York, États-Unis, septembre 2001.
16. Bardis, N. G., Doukas, N. et Ntaikos, K., « Conception et développement d'un système de communication militaire sécurisé basé sur un prototype d'algorithme cryptographique AES et un système avancé de gestion des clés », *WSEAS Transactions on Information Science and Applications,* Université d'éducation militaire, Académie de l'armée hellénique, Grèce.
17. Colbeck, M. J. L., « Le chiffrement quantique dans les communications militaires », *Actes de la conférence de l'EAAW,* 28-29 novembre 2023.
18. Evans, J., Sánchez, R. et Minden, G., « Networking on the Battlefield: Challenges in Highly Dynamic Multi-hop Wireless Networks », *Actes de l'IEEEMILCOM,* Atlantic City, New Jersey, États-Unis, octobre 1999.
19. Hayes, C., « NATO Standardization Agreements (STANAG) for Commanders and Staff », *News from the Front,* Center for Army Lessons Learned (CALL), avril 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, n° 5, octobre 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 », *Journal of the United Service Institution of India,* vol. CXLII, n° 590, octobre-décembre 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., et Gat, K. R., « A Review on Secure Wireless Communication for Military Application », *International Journal of Electrical, Electronics and Data Communication,* vol. 5, n° 11, novembre 2017.
25. Shinde, V., Kulkarni, S. et Malekar, M. R., « Système de communication sécurisé », *International Journal of Innovations in Engineering Research and Technology (IJIERT),* Actes de la conférence TECHNO-2K17.
26. Timofte, G., « Modernisation des systèmes de communication militaires

conformément aux nouvelles exigences opérationnelles, informationnelles et techniques de l'espace de combat de l' », Académie des scientifiques roumains, Bucarest, Roumanie.

27. Département de l'armée des États-Unis, *Signal Communications Doctrine (FM 100-11),* Département de l'armée, Washington, DC, juillet 1948.

28. Alnifie, G., et Simon, R., « A Multi-Channel Defense Against Jamming Attacks in Wireless Sensor Networks », dans *Actes du 3e atelier ACM sur la qualité de service et la sécurité des réseaux sans fil et mobiles,* 2007, pp. 95-104.

29. Alnifie, G., et Simon, R., « MULEPRO : une réponse multicanal aux attaques de brouillage dans les réseaux de capteurs sans fil », *Communications sans fil et informatique mobile,* 2010.

30. Bayraktaroglu, E., King, C., Liu, X., Noubir, G., Rajaraman, R., et Thapa, B., « On the Performance of IEEE 802.11 Under Jamming », dans *Proceedings of the IEEE 27th Conference on Computer Communications,* 2008, pp. 1265-1273.

31. Bellardo, J., et Savage, S., « 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions », dans *Proceedings of the 12th USENIX Security Symposium,* 2003, pp. 15-28.

32. Broustis, I., Pelechrinis, K., Syrivelis, D., Krishnamurthy, S. V., et Tassiulas, L., « FIJI : Fighting Implicit Jamming in 802.11 WLANs », *Security and Privacy in Communication Networks,* vol. 19, 2009, pp. 21-40.

33. Chiang, J. T., et Hu, Y. C., « Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks », *IEEE/ACM Transactions on Networking,* vol. 19, n° 1, 2011, p. 286-298.

34. Commander, C. W., Pardalos, P. M., Ryabchenko, V., Shylo, O. V, Uryasev, S., et Zrazhevsky, G., « Jamming Communication Networks Under Complete Uncertainty », *Optimization Letters*, vol. 2, n° 1, 2008, p. 53-70.

35. Gencer, C., Aydogan, E. K., et Celik, C., « A Decision Support System for Locating VHF/UHF Radio Jammer Systems on the Terrain », *Information Systems Frontiers,* vol. 10, n° 1, 2008, p. 111-124.

36. Gummadi, R., Wetherall, D., Greenstein, B. et Seshan, S., « Comprendre et atténuer l'impact des interférences RF sur les réseaux 802.11 », dans *les actes de la conférence ACM SIGCOMM sur les applications, technologies, architectures et protocoles pour les communications informatiques,* 2007, pp. 385-396.

37. Huang, H., Ahmed, N., et Pulluru, S., « On Limited Range Strategic and Random Jamming Attacks in Wireless Ad Hoc Networks », dans *Proceedings of the IEEE 34th Conference on Local Computer Networks*, 2010, pp. 1-8.

38. Jain, S. K. et Garg, K., « A Hybrid Model of Defense Techniques Against Base Station Jamming Attack in Wireless Sensor Networks », dans *Proceedings of the First International Conference on Computational Intelligence, Communication Systems and Networks*, 2009, pp. 102-107.

39. Kerkez, B., Watteyne, T., Magliocco, M., Glaser, S., et Pister, K., « » (Analyse de faisabilité de la conception d'un contrôleur pour le saut de canal adaptatif), dans *les Actes de la quatrième conférence internationale ICST sur les méthodologies et les outils d'évaluation des performances*, 2009, pp. 76:1-76:6.
40. Khattab, S., Mosse, D. et Melhem, R., « Jamming Mitigation in Multi-Radio Wireless Networks: Reactive or Proactive? », dans *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks,* 2008, pp. 27:1-27:10.
41. Khattab, S., Mosse, D. et Melhem, R., « Modeling of the Channel-Hopping AntiJamming Defense in Multi-Radio Wireless Networks », dans *Proceedings of the 5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services,* 2008, pp. 25:1-25:10.
42. Lazos, L., Liu, S., et Krunz, M., « Mitigating Control Channel Jamming Attacks in MultiChannel Ad Hoc Networks », dans *Proceedings of the 2nd ACM Conference on Wireless Network Security,* 2009, pp. 169-180.
43. Li, M., Koutsopoulos, I., et Poovendran, R., « Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks », dans *Proceedings of the IEEE 26th International Conference on Computer Communications,* 2007, pp. 1307-1315.
44. Liu, H., Liu, Z., Chen, Y., et Xu, W., « Détermination de la position d'un brouilleur à l'aide d'une approche itérative par force virtuelle »*, Wireless Networks,* vol. 17, n° 2, 2011, pp. 531-547.
45. Liu, Z., Liu, H., Xu, W. et Chen, Y., « Exploitation des changements de voisinage causés par le brouillage pour la localisation des brouilleurs », *Transactions IEEE sur les systèmes parallèles et distribués,* 2011.
46. Misra, S., Singh, R. et Mohan, S. V. R., « Mécanisme de détection des attaques de brouillage dignes d'une guerre de l'information pour les réseaux de capteurs sans fil à l'aide d'un système d'inférence floue »*, Sensors,* vol. 10, 2010, pp. 3444-3479.
47. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., et Pantziou, G., « Étude sur les attaques par brouillage et les contre-mesures dans les réseaux de capteurs sans fil », *IEEE Communications Surveys and Tutorials*, vol. 11, n° 4, 2009, pp. 42-56.
48. Muraleedharan, R., et Osadciw, L. A., « Détection des attaques par brouillage et contre-mesures dans les réseaux de capteurs sans fil à l'aide d'un système fourmi », dans *Proceedings of SPIE - The International Society for Optical Engineering,* vol. 6248, 2006, article 62480G.
49. Navda, V, Bohra, A., Ganguly, S., et Rubenstein, D., « Utilisation du saut de canal pour augmenter la résilience 802.11 aux attaques par brouillage », dans *les Actes de la 26e Conférence internationale IEEE sur les communications*

informatiques, 2007, pp. 2526-2530.
50. Panyim, K., Hayajneh, T., Krishnamurthy, P., et Tipper, D., « Jamming Dust: A Low Power Distributed Jammer Network » (Brouillage de poussière : un réseau de brouilleurs distribués à faible puissance), dans *les Actes de la 27e conférence scientifique de l'armée américaine ( )*, 2009, pp. 922-929.
51. Pelechrinis, K., Koufogiannakis, C., et Krishnamurthy, S. V., « Gaming the Jammer: Is Frequency Hopping Effective? », dans *les Actes de la 7e Conférence internationale sur la modélisation et l'optimisation des réseaux mobiles, ad hoc et sans fil,* 2009, pp. 187-196.
52. Pelechrinis, K., Koutsopoulos, I., Broustis, I., et Krishnamurthy, S. V., « Localisation légère des brouilleurs dans les réseaux sans fil : conception et mise en œuvre du système », dans *les Actes de la Conférence mondiale sur les télécommunications de l'IEEE,* 2009, pp. 1-6.
53. Pelechrinis, K., Iliofotou, M., et Krishnamurthy, S. V., « Denial of Service Attacks in Wireless Networks: The Case of Jammers », *IEEE Communications Surveys and Tutorials,* vol. 13, n° 2, 2011, pp. 245-257.
54. Shin, I., Shen, Y., Xuan, Y., Thai, M. T., et Znati, T., « Attaques de brouillage réactif dans les réseaux de capteurs sans fil multiradio : une mesure d'atténuation efficace par l'identification des nœuds déclencheurs », dans *les actes du 2e atelier international ACM sur les fondements des réseaux et du calcul sans fil ad hoc et de capteurs,* 2009, pp. 87-96.
55. Strasser, M., Danev, B. et Čapkun, S., « Détection du brouillage réactif dans les réseaux de capteurs », *Transactions ACM sur les réseaux de capteurs*, vol. 7, n° 2, 2010, article 16.
56. Sun, Y., et Wang, X., « Jammer Localization in Wireless Sensor Networks », dans *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing,* 2009, pp. 1-4.
57. Tague, P., Slater, D., Poovendran, R., et Noubir, G., « Linear Programming Models for Jamming Attacks on Network Traffic Flows », dans *Proceedings of the 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops,* 2008, pp. 207-216.
58. Thamilarasu, G., et Sridhar, R., « Game Theoretic Modeling of Jamming Attacks in Ad Hoc Networks », dans *Proceedings of the 18th International Conference on Computer Communications and Networks*, 2009, pp. 1-6.
59. Wang, H., Zhang, L., Li, T., et Tugnait, J., « Spectrally Efficient Jamming Mitigation Based on Code-Controlled Frequency Hopping », *IEEE Transactions on Wireless Communications,* vol. 10, n° 3, 2011, pp. 728-732.
60. Wilhelm, M., Martinovic, I., Schmitt, J. B., et Lenders, V., « Reactive Jamming in Wireless Networks: How Realistic Is the Threat? », dans *Actes de la quatrième conférence ACM sur la sécurité des réseaux sans fil,* 2011, pp. 47-52.

61. Wood, A., Stankovic, J., et Son, S., « JAM : un service de cartographie des zones brouillées pour les réseaux de capteurs », dans *les actes du 24e symposium IEEE sur les systèmes en temps réel,* 2003, pp. 286-297.
62. Wood, A., Stankovic, J. et Zhou, G., « DEEJAM : Defeating Energy-Efficient Jamming in IEEE 802.15.4-Based Wireless Networks », dans *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2007, pp. 60-69.
63. Xu, W., Wood, T., Trappe, W., et Zhang, Y., « Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service », dans *Proceedings of the 3rd ACM Workshop on Wireless Security*, 2004, pp. 80-89.
64. Xu, W., Trappe, W., Zhang, Y. et Wood, T., « The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks », dans *Proceedings of the 6th ACM International Symposium on Mobile AdHoc Networking and Computing,* 2005, pp. 46-57.
65. Yoon, S. U., Murawski, R., Ekici, E., Park, S., et Mir, Z., « Adaptive Channel Hopping for Interference-Robust Wireless Sensor Networks » (Saut de canal adaptatif pour les réseaux de capteurs sans fil résistants aux interférences), dans *les Actes de la Conférence internationale IEEE sur les communications*, 2010, pp. 1-5.
66. État-major de l'armée italienne - Bureau de la sécurité, *Systèmes logiciels, télécommunications et sécurité - Documents non classifiés,* Rome, Italie, 2008.
67. État-major général de l'armée italienne - Bureau de la sécurité, *Systèmes logiciels, télécommunications et sécurité - Documents classifiés,* Rome, Italie, 2008.
68. ISO/IEC 15408-1, *Technologies de l'information - Techniques de sécurité - Critères d'évaluation de la sécurité informatique - Partie 1 : Introduction et modèle général,* Organisation internationale de normalisation, Genève, 2009.
69. ISO/IEC 15408-2, *Technologies de l'information - Techniques de sécurité - Critères d'évaluation de la sécurité informatique - Partie 2 : Composants fonctionnels de sécurité,* Organisation internationale de normalisation, Genève, 2008.
70. ISO/IEC 15408-3, *Technologies de l'information - Techniques de sécurité - Critères d'évaluation de la sécurité informatique - Partie 3 : Composants d'assurance de la sécurité,* Organisation internationale de normalisation, Genève, 2008.
71. Département américain de la Défense, *Critères d'évaluation des systèmes informatiques fiables,* DoDD 5200.28-STD, Washington, DC, décembre 1985.
72. Département américain de la Défense, *Directive : Assurance de l'information,* DoDD 8500.01E, Washington, DC, octobre 2002.
73. Bundesamt für Sicherheit in der Informationstechnik, *Notes d'application*

et interprétation du schéma (AIS) : ITSEC vers les critères communs avec potentiel d'attaque spécifique, Bonn, Allemagne, 2010. Disponible en ligne : https://www.bsi.bund.de

74. ISO/IEC 27000, *Technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Aperçu et vocabulaire,* Organisation internationale de normalisation, Genève, 2009.

75. Hare, F., « The Cyber Threat to National Security: Why Can't We Agree », dans *Proceedings of the Conference on Cyber Conflicts,* Tallinn, Estonie, 2010, pp. 211-225.

76. Liles, S., « La cyberguerre : une forme de conflit et d'insurrection de faible intensité », dans *Actes de la conférence sur les cyberconflits*, Tallinn, Estonie, 2010, pp. 47-57.

77. Kotenko, I. V., « Multi-Agent Modeling and Simulation of Cyber-Attacks and Cyber Defense for Homeland Security », dans *Proceedings of the IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications,* Dortmund, Allemagne, 6-8 septembre 2008.

78. Kotenko, I. V., et Ulanov, A. V., « Agent-Based Simulation of DDoS Attacks and Defense Mechanisms »*, Journal of Computing,* vol. 4, n° 2, 2005.

79. Gasser, L., « Post-Quantum Cryptography », dans V. Mulder, A. Mermoud, V. Lenders et B. Tellenbach (éd.), *Trends in Data Protection and Encryption Technologies,* Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33386-6.10

80. Radanliev, P., « Artificial Intelligence and Quantum Cryptography », *Journal of Analytical Science and Technology,* vol. 15, article 4, 2024. https://doi.org/10.1186/s40543-024- 00416-6

81. Atutxa, A., Sanz, A., Sasiain, J., Astorga, J. et Jacob, E., « Vers une 5G quantique sécurisée : distribution quantique de clés dans les réseaux centraux », *Computer Communications*, vol. 224, 2024, pp. 145-158. https://doi.org/10.1016Zj.comcom.2024.06.005

82. Ricci, S., Dobias, P., Malina, L., Hajny, J. et Jedlicka, P., « Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography »*, IEEE Access,* vol. 12, 2024, p. 23206-23219. https://doi.org/10.1109/ACCESS.2024.3364520

83. Shim, K.-S., Kim, B. et Lee, W., « Research on Quantum Key, Distribution Key and PostQuantum Cryptography Key Applied Protocols for Data Science and Web Security »*, Journal of Web Engineering,* vol. 23, n° 6, septembre 2024, p. 813-830. https://doi.org/10.13052/jwe1540-9589.2365

84. Dhar, S., Khare, A., Dwivedi, A. D., et Singh, R., « Securing IoT Devices: A Novel Approach Using Blockchain and Quantum Cryptography »*, Internet of*

Things, vol. 25, 2024, article 101019. https:ZZdoi.org/10.1016Zj.iot.2023.101019
85. Schneier, B., « Lattice-Based Cryptosystems and Quantum Cryptanalysis », *Communications of the ACM,* Online First, juin 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 », *npj Quantum Information,* vol. 8, article 104, 2022. https://doi.org/10.1038/s41534-022-00626-z
87. Akçay, L., et Yalçın, B. Ö., « Conception ASIP légère pour les algorithmes de cryptographie post-quantique basés sur les réseaux d' », *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., et Etxezarreta Martinez, J., « Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective », *IEEE Internet of Things Journal,* vol. 11, n° 18, 15 septembre 2024, p. 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.,
et Tafur Monroy, I., « Quantum-Resistant Transport Layer Security », *Computer Communications*, vol. 213, 2024, p. 345-358. https://doi.org/10.1016/j.comcom.2023.11.010
90. Alhakami, H., « Enhancing IoT Security: Quantum-Level Resilience Against Threats », *Computers, Materials and Continua,* vol. 78, n° 1, 2024, p. 329-356. https://doi.org/10.32604/cmc.2023.043439
91. Chawla, D., et Mehra, P. S., « A Survey on Quantum Computing for Internet of Things Security », *Procedia Computer Science*, vol. 218, 2023, p. 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 », *SN Computer Science*, vol. 4, article 365, 2023. https://doi.org/10.1007/s42979-023-01724-1
93. Ji, X., Wang, B., Hu, F., Wang, C., et Zhang, H., « New Advanced Computing Architecture
pour la conception et l'analyse cryptographiques par D-Wave Quantum Annealer », *Tsinghua Science and Technology,* vol. 27, n° 4, août 2022, pp. 751-759. https://doi.org/10.26599/TST.2021.9010022
94. Hasan, K. F., et al., « A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies », *IEEE Access,* vol. 12, 2024, p. 23427-23450. https://doi.org/10.1109/ACCESS.2024.3360412
95. Kong, I., Janssen, M., et Bharosa, N., « Realizing Quantum-Safe Information Sharing: Implementation and Adoption Challenges and Policy Recommendations for Quantum-Safe Transitions », *Government Information*

Quarterly, vol. 41, n° 1, 2024, article 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, n° 3, 2024, p. 1898-1949. https://doi.org/10.1109/COMST.2024.3367535
97. Hoque, S., Aydeger, A., et Zeydan, E., « Exploring Post-Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design », dans *Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems (PECS '24),* ACM, New York, 2024, pp. 9-16. https://doi.org/10.1145/3659997.3660033
98. Piatkowski, J., et Szymoniak, S., « Trivializing Verification of Cryptographic Protocols », *Computer Assisted Methods in Engineering and Science*, vol. 30, n° 4, 2023, pp. 389-406. https://doi.org/10.24423/cames.869
99. Basin, D. A., Cremers, C., et Meadows, C. A., « Model Checking Security Protocols », dans E. Clarke, T. Henzinger, H. Veith, et R. Bloem (éd.), *Handbook of Model Checking,* Springer, Cham, 2018, pp. 727-762. https://doi.org/10.1007/978-3-319-10575-8_22
100. Blanchet, B., « Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif », *Foundations and Trends in Privacy and Security*, vol. 1, n° 12, 2016, p. 1-135. https://doi.org/10.1561/3300000004
101. Blanchet, B., Cheval, V., et Cortier, V., « ProVerif avec lemmes, induction, subsomption rapide et bien plus encore », dans *les actes du symposium IEEE sur la sécurité et la confidentialité (S&P 2022),* IEEE Computer Society, San Francisco, Californie, 2022, pp. 205-222. https://hal.inria.fr/hal-03366962/
102. Bouroulet, R., Devillers, R., Klaudel, H., Pelz, E., et Pommereau, F., « Modeling and Analysis of Security Protocols Using Role-Based Specifications and Petri Nets », dans K. M. van Hee et R. Valk (éd.), *Applications and Theory of Petri Nets,* Springer, Berlin et Heidelberg, 2008, pp. 72-91.
103. Burrows, M., Abadi, M., et Needham, R., « A Logic of Authentication », *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 », dans *Proceedings of the Workshop on Specification and Automated Processing of Security Requirements (SAPS 2004),* Austrian Computer Society, Linz, Autriche, 2004, p. 13.
105. Cortier, V., Delaune, S., et Dreier, J., « Automatic Generation of Source Lemmas in Tamarin: Towards Automatic Proofs of Security Protocols », dans L. Chen, N. Li, K. Liang et S. Schneider (éd.), *Computer Security - ESORICS 2020,* Springer, Cham, 2020, pp. 3-22.

106. David, A., Larsen, K. G., Legay, A., Mikucionis, M., et 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., et Yao, A. C., « On the Security of Public Key Protocols », dans *Proceedings of the 22nd Annual Symposium on Foundations of Computer Science (SFCS '81),* IEEE Computer Society, Washington, DC, 1981, pp. 350-357.

108. Gregor, D., Järvi, J., Siek, J., Reis, G., Stroustrup, B., et Lumsdaine, A., « Concepts: Linguistic Support for Generic Programming in C++ », *ACM SIGPLAN Notices,* vol. 41, n° 10, 2006, pp. 291-310. https://doi.org/10.1145/1167515.1167499

109. Grosser, A., Kurkowski, M., Piatkowski, J. et Szymoniak, S., « ProToc : un langage universel pour les spécifications de protocoles de sécurité », dans A. Wilinski, I. E. Fray et J. Pejas (éd.), *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., et Modersheim, S., « A Typing Result for Stateful Protocols », dans *Proceedings of the IEEE 31st Computer Security Foundations Symposium (CSF 2018),* IEEE, 2018, pp. 374-388. https://doi.org/10.1109/CSF.2018.00034

112. Järvi, J., Gregor, D., Willcock, J., Lumsdaine, A., et Siek, J., « Algorithm Specialization in Generic Programming: Challenges of Constrained Generics in C++ », *ACM SIGPLAN Notices*, vol. 41, n° 6, 2006, pp. 272-282. https://doi.org/10.1145/1133255.1134014

113. Kassem, A., Lafourcade, P., Lakhnech, Y., et Modersheim, S., « Multiple Independent Lazy Intruders », dans *Proceedings of the 1st Workshop on Hot Issues in Security Principles and Trust (HotSpot 2013)*, 2013, 15 pages.

114. Kordy, B., Mauw, S., Radomirovic, S., et Schweitzer, P., « Foundations of AttackDefense Trees », dans P. Degano, S. Etalle et J. Guttman (éd.), *Formal Aspects in Security and Trust (FAST 2010),* Lecture Notes in Computer Science, vol. 6561, Springer, Berlin et Heidelberg, 2010, pp. 80-95. https://doi.org/10.1007/978-3-642-19751-2_6

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

116. Kurkowski, M., *Méthodes formelles pour la vérification des propriétés des protocoles de sécurité dans les réseaux informatiques* (en polonais), Akademicka Oficyna Wydawnicza Exit, Varsovie, 2013.

117. Liang, J., Nguyen, Q., Simoff, S., Huang, M., « Divide and Conquer Treemaps: Visualizing Large Trees with Various Shapes », *Journal of Visual*

Languages and Computing, vol. 31, 2015, p. 104-127. https://doi.org/10.1016/jjvlc.2015.10.009
118. Liu, S., Xiao, T., Liu, J., Wang, X., Wu, J., et Zhu, J., « Visual Diagnosis of Tree Boosting Methods », *IEEE Transactions on Visualization and Computer Graphics,* vol. 24, n° 1, 2017, p. 163-173. https://doi.org/10.1109/TVCG.2017.2744378
119. Mauw, S., et Oostdijk, M., « Foundations of Attack Trees », dans *International Conference on Information Security and Cryptology,* Springer, 2005, pp. 186-198. https://doi.org/10.1007/11734727_17
120. Millen, J. K., « CAPSL : Common Authentication Protocol Specification Language », dans *Actes de l'atelier sur les nouveaux paradigmes de sécurité (NSPW '96),* 1996. https://doi.org/10.1145/304851.304879
121. Morin, P., *Open Data Structures (en C++),* 2013. https://opendatastructures.org/
122. Modersheim, S., Nielson, F., et Nielson, H. R., « Lazy Mobile Intruders », dans D. A. Basin et J. C. Mitchell (éd.), *Principles of Security and Trust (POST),* Lecture Notes in Computer Science, vol. 7796, Springer, 2013, p. 147-166.
123. Needham, R. M., et Schroeder, M. D., « Using Encryption for Authentication in Large Networks of Computers », *Communications of the ACM*, vol. 21, n° 12, 1978, p. 993-999. https://doi.org/10.1145/359657.359659
124. Neuman, B. C., et Ts'o, T., « Kerberos : un service d'authentification pour les réseaux informatiques », *IEEE Communications Magazine*, vol. 32, n° 9, 1994, p. 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, p. 74083-74092. https://doi.org/10.1109/ACCESS.2020.2988358
126. Ryan, P. Y. A., Schneider, S. A., Goldsmith, M. H., Lowe, G., et Roscoe, A. W., *The Modelling and Analysis of Security Protocols: The CSP Approach,* Addison-Wesley Professional, Harlow, Londres, 2000.
127. Siedlecka-Lamch, O., Szymoniak, S., et Kurkowski, M., « A Fast Method for Security Protocols Verification », dans *Proceedings of the 18th International Conference on Computer Information Systems and Industrial Management (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., et Fray, I. E., « Towards the Most Efficient Method for Untimed Security Protocols Verification », dans *Proceedings of the 24th Pacific Asia Conference on Information Systems (PACIS 2020),* Dubaï, Émirats arabes unis, 2020, p. 189.
129. Siek, J. G., et Lumsdaine, A., « A Language for Generic Programming in the Large », *Science of Computer Programming,* vol. 76, n° 5, 2011, p. 423-465.

https://doi.org/10.1016/j.scico.2008.09.009
130. Szymoniak, S., « Amelia : un nouveau protocole de sécurité pour la protection contre les fausses
Links », *Computer Communications*, vol. 179, 2021, p. 73-81.
https://doi.org/10.1016/j.comcom.2021.07.030
131. Szymoniak, S., Kurkowski, M., et Piatkowski, J., « Modèles temporels de protocoles de sécurité
incluant les retards dans le réseau », *Journal of Applied Mathematics and Computational Mechanics,* vol. 14, n° 3, 2015, p. 127-139.
https://doi.org/10.17512/jamcm.2015.3.14
132. Tremblay, J.-P., et Sorenson, P. G., *An Introduction to Data Structures with Applications,* 2e éd., McGraw-Hill, Auckland, 1984.
133. Witten, I. H., Frank, E., et Hall, M. A., *Data Mining: Practical Machine Learning Tools and Techniques,* 3e éd., Morgan Kaufmann, Amsterdam, 2011.
134. R. Mustafovski, A. Petrovski et M. Radovanovic, « Intégration des technologies quantiques dans les systèmes militaires mobiles et les cadres TOC », *Land Forces Academy Review,* vol. XXX, n° 3(119), 2025.
135. R. Mustafovski, « Cadre architectural basé sur des formules de la plateforme SecuDroneComm pour les communications des véhicules aériens sans pilote », *Management Science Advances*, vol. 2, n° 1, pp. 288-303, Scientific Oasis, Skopje, République de Macédoine du Nord, 2025.
136. R. Mustafovski, « Évaluation de l'impact opérationnel de SecuDroneComm : évaluation basée sur la simulation de la communication sécurisée des drones dans les environnements militaires », *Scientific Technical Review,* vol. 75, n° 1, pp. 11-18, 2025, doi : 10.5937/str2500002M.
137. M. Mozaffari, W. Saad, M. Bennis et M. Debbah, « Déploiement efficace de plusieurs véhicules aériens sans pilote pour une couverture sans fil optimale », *IEEE Communications Letters,* vol. 20, n° 8, pp. 1647-1650, 2016.
138. L. Ruan et al., « Déploiement de couverture multi-UAV économe en énergie dans les réseaux UAV : un cadre théorique basé sur la théorie des jeux », *China Communications,* vol. 15, n° 10, pp. 194209, 2018.
139. M. Mozaffari, W. Saad, M. Bennis et M. Debbah, « Mobile unmanned aerial vehicles (UAVs) for energy-efficient Internet of Things communications », *IEEE Transactions on Wireless Communications*, 2017.
140. S.-Y Lien, K.-C. Chen et Y. Lin, « Vers des accès massifs omniprésents dans les communications machine-à-machine 3GPP », *IEEE Communications Magazine*, vol. 49, n° 4, pp. 66-74, avril 2011.
141. M. Malik et S. K. Garg, « Vers la 6G : évolution des réseaux au-delà de la 5G et scénario indien », dans *Proc. 2nd Int. Conf. Innovative Practices in Technology and Management (ICIPTM)*, Gautam Buddha Nagar, Inde, pp. 123-

127, 2022.
142. M. A. Khan et al., « Swarm of UAVs for network management in 6G: A technical review », *IEEE Transactions on Network and Service Management,* vol. 20, n° 1, pp. 741761, mars 2023.
143. S. Dang, O. Amin, B. Shihada et M.-S. Alouini, « What should 6G be? », *Nature Electronics*, vol. 3, n° 1, pp. 20-29, 2020.
144. F. Ronaldo, D. Pramadihanto et A. Sudarsono, « Système de communication sécurisé pour les services de drones utilisant la cryptographie hybride sur le réseau 4G/LTE », dans *Proc. Int. Electronics Symposium (IES),* Surabaya, Indonésie, pp. 116-122, 2020.
145. T. Li et al., « Communications sécurisées entre drones et véhicules », *IEEE Transactions on Communications*, vol. 69, n° 8, pp. 5381-5393, août 2021.
146. S. A. Ayati et H. R. Naji, « A secure mechanism to protect UAV communications », dans *Proc. 9th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS),* Bam, Iran, pp. 1-6, 2022.
147. D. Pirker, T. Fischer, C. Lesjak et C. Steger, « Système d'authentification mondial et sécurisé des drones basé sur la sécurité matérielle », dans *Proc. 8e conférence internationale IEEE sur le cloud computing mobile, les services et l'ingénierie (MobileCloud)*, Oxford, Royaume-Uni, pp. 84-89, 2020.
148. H. Wang, H. Fang et X. Wang, « Authentification décentralisée souple grâce à l'intelligence périphérique dans un essaim de drones », dans *Proc. IEEE/CIC Int. Conf. Communications in China (ICCC)*, Xiamen, Chine, pp. 86-91, 2021.
149. M. Markowski, P. Ryba et K. Puchala, « Laboratoire de recherche sur les réseaux définis par logiciel : topologies et scénarios expérimentaux », dans *Proc. 3rd European Network Intelligence Conf. (ENIC),* Wroclaw, Pologne, pp. 252-256, 2016.
150. M. A. B. S. Abir, M. Z. Chowdhury et Y. M. Jang, « Réseaux d'UAV définis par logiciel pour les systèmes 6G : exigences, opportunités, techniques émergentes, défis et orientations de recherche », *IEEE Open Journal of the Communications Society,* vol. 4, pp. 2487-2547, 2023.
151. M. Ouadah et F. Merazka, « Une approche de codage réseau pour des réseaux de drones fiables basés sur le SDN », dans *Proc. 5th Int. Conf. Electrical Engineering and Control Applications (ICEECA '22),* Khenchela, Algérie, 2022.

Biographie de Rexhep Mustafovski, MSc

Rexhep Mustafovski, MSc, est officier au ministère de la Défense de la République de Macédoine du Nord et assistant d'enseignement et de recherche à l'Académie militaire « Général Mihailo Apostolski » à Skopje, où il travaille au sein du département de cybersécurité et de criminalistique numérique. Il est spécialiste des systèmes de communication sécurisés, de la cybersécurité et de l'intégration des technologies de défense, avec une expérience universitaire et professionnelle couvrant les communications tactiques sécurisées, la sécurité des réseaux et les systèmes d'information émergents.

Il a suivi ses études de premier cycle à l'Académie militaire « Général Mihailo Apostolski » de Skopje, où il a obtenu son diplôme d'officier des transmissions. Au cours de ses études, il a fait preuve de résultats scolaires exceptionnels et d'une discipline professionnelle remarquable, obtenant les meilleurs résultats de sa promotion. En reconnaissance de cette réussite, il a été officiellement désigné meilleur officier de sa promotion, un honneur qui lui a été décerné par le président du pays. Cette distinction reflète à la fois son excellence académique et son engagement en faveur du professionnalisme militaire.

Après avoir été nommé officier, il a poursuivi son développement académique en suivant des études supérieures à la faculté d'ingénierie électrique et des technologies de l'information de l'université « Ss. Cyril et Methodius » de Skopje. Il a obtenu un master en sciences des technologies de la communication et de l'information, avec une spécialisation dans les systèmes de communication modernes, la sécurité de l'information et les concepts avancés de mise en réseau. Ses études de master ont renforcé ses capacités d'analyse et de recherche, en particulier dans les domaines des communications sécurisées et des systèmes de défense basés sur la technologie.

Son parcours universitaire et professionnel combine une formation militaire officielle et des études d'ingénierie avancées, ce qui lui confère une base solide pour la recherche et le travail pratique dans le domaine des communications militaires

sécurisées. Cette expérience influence son approche de la conception des systèmes de communication, qui met l'accent sur la fiabilité, la sécurité, l'interopérabilité de l' s et la pertinence opérationnelle. Les connaissances et l'expérience acquises grâce à sa formation militaire et à ses études d'ingénierie sous-tendent les perspectives présentées tout au long de cet ouvrage.