ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

ΕΡΓΑΣΤΗΡΙΟ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Επισκόπηση τεχνολογιών και πρωτοκόλλων τηλεπικοινωνιών για στρατιωτικές εφαρμογές»

"A Review of Military Telecommunications: Technologies and Protocols"

Εμμανουηλίδου Μαρία — **ΤΛ20233**

Πάνου Μαρία — **ΤΛ20288**

Επιβλέπων: Δρ. Ανάργυρος Μπακλέζος
Επικ. Καθηγητής ΕΛ.ΜΕ.ΠΑ.

Χανιά, Νοέμβριος 2025

ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

ΕΡΓΑΣΤΗΡΙΟ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Επισκόπηση τεχνολογιών και πρωτοκόλλων τηλεπικοινωνιών για στρατιωτικές εφαρμογές»

"A Review of Military Telecommunications: Technologies and Protocols"

Εμμανουηλίδου Μαρία
ΤΛ20233

Πάνου Μαρία
ΤΛ20288

Επιβλέπων: Δρ. Ανάργυρος Μπακλέζος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 28η Νοεμβρίου 2025.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Δρ. Ανάργυρος Μπακλέζος	Δρ. Χρήστος Νικολόπουλος	Δρ. Ιωάννης Βαρδιάμπασης
Επίκουρος Καθηγητής	Επίκουρος Καθηγητής	Καθηγητής Α' Βαθμίδας
ΕΛ.ΜΕ.ΠΑ.	ΕΛ.ΜΕ.ΠΑ.	ΕΛ.ΜΕ.ΠΑ.

Χανιά, Νοέμβριος 2025

Copyright © Εμμανουηλίδου Μαρία, Πάνου Μαρία, 2025.

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Ελληνικού Μεσογειακού Πανεπιστημίου.

(Υπογραφή)

…….

Εμμανουηλίδου Μαρία

Ηλεκτρονικός Μηχανικός ΕΛ.ΜΕ.ΠΑ

(Υπογραφή)

……

Πάνου Μαρία

Ηλεκτρονικός Μηχανικός ΕΛ.ΜΕ.ΠΑ

ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

ΕΡΓΑΣΤΗΡΙΟ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΗΛΕΚΤΡΟΜΑΓΝΗΤΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Επισκόπηση τεχνολογιών και πρωτοκόλλων τηλεπικοινωνιών για στρατιωτικές εφαρμογές»

"A Review of Military Telecommunications: Technologies and Protocols"

Εμμανουηλίδου Μαρία — **ΤΛ20233**

Πάνου Μαρία — **ΤΛ20288**

Επιβλέπων: Δρ. Ανάργυρος Μπακλέζος

Χανιά, Νοέμβριος 2025

Αφιερώνουμε την διπλωματική μας

στις οικογένειες μας που μας στήριξαν.

Π ε ρ ί λ η ψ η

Η παρούσα διπλωματική εργασία πραγματεύεται την επισκόπηση των τεχνολογιών, πρωτοκόλλων και αρχιτεκτονικών που συγκροτούν το σύγχρονο πεδίο των στρατιωτικών τηλεπικοινωνιών, με στόχο την ανάλυση των βασικών τεχνολογικών θεμελίων, των πρωτοκόλλων ασφαλείας και των προκλήσεων που αντιμετωπίζουν τα δίκτυα διοίκησης και ελέγχου (C4ISR) στο σημερινό, δυναμικά μεταβαλλόμενο επιχειρησιακό περιβάλλον. Η προσέγγιση της εργασίας είναι βιβλιογραφική, βασισμένη σε σύγχρονες μελέτες, τεχνικές αναφορές και διεθνή πρότυπα.

Αρχικά παρουσιάζεται η ιστορική εξέλιξη των στρατιωτικών επικοινωνιών και η μετάβαση από τις αναλογικές στις ψηφιακές υποδομές, οδηγώντας στη διαμόρφωση των δικτυοκεντρικών επιχειρήσεων. Στη συνέχεια, αναλύονται οι δομές και τα πρωτόκολλα που θεμελιώνουν τα σύγχρονα τακτικά δίκτυα, όπως οι τροποποιήσεις TCP/IP, τα MANETs, τα πρωτόκολλα ασφαλείας IPsec, HAIPE και TACLANE, καθώς και τα δορυφορικά συστήματα SATCOM, που αποτελούν τη ραχοκοκαλιά των στρατιωτικών επικοινωνιών μεγάλης εμβέλειας.

Ιδιαίτερη έμφαση δίνεται στις κυβερνοαπειλές και στις προκλήσεις ασφάλειας που απειλούν τα στρατιωτικά δίκτυα, όπως οι επιθέσεις jamming και spoofing, οι παραβιάσεις IoMT και οι επιθετικές κυβερνοεπιχειρήσεις. Παρουσιάζονται οι στρατηγικές άμυνας και προστασίας, όπως η προσέγγιση Zero Trust, η αρχιτεκτονική πλεονασμού (redundancy) και η αξιοποίηση τεχνητής νοημοσύνης για ανίχνευση και απόκριση σε ανωμαλίες.

Τέλος, εξετάζονται οι καινοτομίες και οι μελλοντικές τάσεις που διαμορφώνουν τη νέα εποχή των στρατιωτικών τηλεπικοινωνιών: τα δίκτυα 5G/6G, η τεχνητή νοημοσύνη, το edge computing και η κβαντική κρυπτογραφία. Τα ευρήματα υπογραμμίζουν ότι η ασφάλεια, η διαλειτουργικότητα και η τεχνολογική καινοτομία αποτελούν τους ακρογωνιαίους λίθους για τη διαμόρφωση των στρατιωτικών επικοινωνιών του μέλλοντος — ενός πεδίου όπου η πληροφορία μετατρέπεται σε στρατηγικό πολλαπλασιαστή ισχύος και καθοριστικό παράγοντα επιχειρησιακής υπεροχής.

Λέξεις-Κλειδιά: Στρατιωτικές τηλεπικοινωνίες, SDR, MANETs, SATCOM, 5G/6G, IoMT, C4ISR, κυβερνοασφάλεια, τεχνητή νοημοσύνη.

Abstract

This thesis presents an extensive review of the technologies, protocols, and architectures that define the modern field of military telecommunications. Its primary objective is to analyze the fundamental technological foundations, security protocols, and challenges faced by Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) networks within today's dynamically evolving operational environment. The study follows a bibliographic research approach, based on contemporary scientific literature, technical reports, and international standards.

The work begins with an overview of the historical evolution of military communications and the gradual transition from analog to digital infrastructures, which paved the way for the development of network-centric operations. It then examines the structures and protocols that underpin modern tactical networks, such as TCP/IP modifications, Mobile Ad-hoc Networks (MANETs), and secure communication protocols including IPsec, HAIPE, and TACLANE, as well as Satellite Communication (SATCOM) systems, which constitute the backbone of long-range military connectivity.

Special emphasis is placed on cybersecurity threats and vulnerabilities that challenge military networks, including jamming and spoofing attacks, IoMT intrusions, and large-scale cyber operations. The study also highlights modern defense strategies such as the Zero Trust approach, redundancy-based architectures, and the use of Artificial Intelligence for anomaly detection and real-time response.

Finally, the thesis explores emerging innovations and future trends that are shaping the next era of military communications, such as 5G/6G networks, Artificial Intelligence, edge computing, and quantum cryptography. The findings underline that security, interoperability, and technological innovation constitute the cornerstones of future military communications — a domain in which information becomes a strategic force multiplier and a decisive factor for operational superiority.

Keywords: Military Telecommunications, SDR, MANET, SATCOM, 5G/6G, IoMT, C4ISR, Cybersecurity, Artificial Intelligence.

Π ε ρ ι ε χ ό μ ε ν α

1 Εισαγωγή 1

2 Ιστορική Εξέλιξη και Θεμελιώδεις Αρχές 3

2.1 Εξέλιξη στρατιωτικών επικοινωνιών 3

2.2 Προ-Ηλεκτρική και Πρώιμη Ηλεκτρική Εποχή 4

2.2.1 Α’ & Β’ Παγκόσμιος Πόλεμος 4
2.2.2 Ψυχρός Πόλεμος και Ψηφιακή Επανάσταση 4
2.2.3 Μετά τον Ψυχρό Πόλεμο – Δικτυοκεντρικές Επιχειρήσεις 5
2.2.4 Σύγχρονες τάσεις και IoMT 6

2.3 Θεμελιώδεις απαιτήσεις : ασφάλεια, αξιοπιστία, ευελιξία 7

2.3.1 Ασφάλεια και το θεμέλιο της κάθε μετάδοσης 8
2.3.2 Αξιοπιστία και διαθεσιμότητα 8
2.3.3 Ευελιξία και διαλειτουργικότητα 9
2.3.4 Χαμηλή καθυστέρηση και ταχύτητα 11
2.3.5 Ιεράρχηση και διαχείριση πόρων 12
2.3.6 Ανθεκτικότητα στο περιβάλλον 12
2.3.7 Ενεργειακή αυτονομία και αποδοτικότητα 13
2.3.8 Επεκτασιμότητα και προσαρμοστικότητα 14

2.4 Διαφορές Στρατιωτικών και Εμπορικών Δικτύων 16

2.4.1 Αρχιτεκτονική 16
2.4.2 Ευελιξία και Διαλειτουργικότητα 17

3 Σύγχρονες Τεχνολογίες Στρατιωτικών Δικτυών 19

3.1 Τεχνολογία 5G στις στρατιωτικές επικοινωνίες 20

3.1.1 Βασικά χαρακτηριστικά του 5G 21
3.1.2 Στρατιωτικές Εφαρμογές του 5G 22
3.1.3 Προκλήσεις και Περιορισμοί 24
3.1.4 Μελλοντικές Κατευθύνσεις 26

3.2 Software Defined Radios(SDRs) και Cognitive Radios στις στρατιωτικές επικοινωνίες 27

3.2.1 Software Defined Radios(SDRs) 27
3.2.2 MANETs σε συνδυασμό με SDRs 29
3.2.3 Cognitive Radios και Cognitive MANETs 31
3.2.4 Προκλήσεις και περιορισμοί των SDR/Cognitive Radios 33

3.3 UAVs/Drones και Tactical Mesh Networks 35

3.3.1 Ρόλος των UAVs στις στρατιωτικές επικοινωνίες 35
3.3.2 Tactical Mesh Networks 37
3.3.3 Ενσωμάτωση UAVs σε Mesh Networks 39
3.3.4 Προκλήσεις και περιορισμοί 41
3.3.5 Μελλοντικές κατευθύνσεις 43

3.4 Δορυφορικές επικοινωνίες και tactical SATCOM 45

3.4.1 Ο ρόλος των δορυφορικών επικοινωνιών στις στρατιωτικές επιχειρήσεις 45
3.4.2 Τεχνολογίες και αρχιτεκτονικές Tactical SATCOM 47
3.4.3 Πλεονεκτήματα και επιχειρησιακές δυνατότητες 49
3.4.4 Περιορισμοί και ευπάθειες των SATCOM 51
3.4.5 Μελλοντικές Τάσεις 52

4 Πρωτόκολλα και Δομές Στρατιωτικών Δικτυών 55

4.1 Τροποποιήσεις TCP/IP για τα τακτικά δίκτυα 55

4.1.1 Βελτιωμένες εκδόσεις TCP για τα τακτικά δίκτυα 56

4.1.2 Cross-layer βελτιστοποίηση και ECN 57
4.1.3 Εναλλακτικά πρωτόκολλα 59
4.1.4 Split TCP : Αρχή λειτουργίας και πραγματικές εφαρμογές 59
4.1.5 Μελλοντικές τάσεις στα πρωτόκολλα στρατιωτικών τακτικών δικτύων 61

4.2 MANETs & Ad-Hoc Αρχιτεκτονικές 62
4.2.1 Πλεονεκτήματα στα τακτικά δίκτυα 63
4.2.2 Δομή και τύποι MANETs 64
4.2.3 Σύγκριση MANET με παραδοσιακά δίκτυα 65
4.2.4 Πρωτόκολλα δρομολόγησης σε MANETs 66
4.2.5 Εφαρμογές σε στρατιωτικά συστήματα 67
4.2.6 Προκλήσεις και τεχνολογικές κατευθύνσεις 68

4.3 Πρωτόκολλα Ασφαλούς Επικοινωνίας(IPsec,HAIPE,TACLANE) 69
4.3.1 IPsec-Το θεμέλιο της ασφάλειας σε επίπεδο IP 70
4.3.2 HAIPE-Στρατιωτική επέκταση του IPsec 73
4.3.3 TACLANE-Πρακτική εφαρμογή του HAIPE 76
4.3.4 Σύγχρονες απειλές και μελλοντικές κατευθύνσεις 78

4.4 Δορυφορικά Συστήματα Επικοινωνιών(SATCOM) σε στρατιωτικές εφαρμογές 79
4.4.1 Κατηγορίες στρατιωτικών δορυφορικών συστημάτων 80
4.4.2 Στρατιωτικά συστήματα SATCOM 81
4.4.3 STANAG και δορυφορικά συστήματα 82
4.4.4 Εφαρμογές στο πεδίο επιχειρήσεων 83
4.4.5 Τεχνικές προκλήσεις και ανάγκες ασφάλειας 84
4.4.6 Τεχνολογικές λύσεις & μελλοντικές τάσεις 85

5 Κυβερνοαπειλές & Προκλήσεις 87

5.1 Jamming, Spoofing και Ηλεκτρονικός Πόλεμος 87
5.1.1 Jamming : Τύποι και Επιχειρησιακή επίδραση 88
5.1.2 Spoofing : GPS και δικτυακές επιθέσεις 91
5.1.3 Συνδυασμένες επιθέσεις(EW,Cyber) 94
5.1.4 Μέτρα Αντιμετώπισης και σύγχρονες τεχνολογίες 96

5.2 Επιθέσεις σε IoMT & Data Leakage 98
5.2.1 Μορφές επιθέσεων και τεχνικές παρέμβασης 99
5.2.2 Διαρροή δεδομένων και επιχειρησιακό ρίσκο 100
5.2.3 Zero Trust: Στρατηγική μηδενικής εμπιστοσύνης 103
5.2.4 Μέτρα αντιμετώπισης και πολιτικές ασφάλειας 106

5.3 Επιθετικές Κυβερνοεπιχειρήσεις και Άμυνα 107
5.3.1 Μορφές επιθετικών κυβερνοεπιχειρήσεων 108
5.3.2 Στρατιωτικές δομές και διεθνής διάσταση 110
5.3.3 Διεθνής διάσταση, κανόνες και νομιμότητα 112
5.3.4 Παραδείγματα επιθετικών επιχειρήσεων 114
5.3.5 Στρατηγικές άμυνας 117

5.4 Redundancy και προστασία δεδομένων 118
5.4.1 Βασικές έννοιες και επιχειρησιακοί στόχοι εφεδρείας και προστασίας δεδομένων 118
5.4.2 Redundancy :Εφεδρικές αρχιτεκτονικές και διαθεσιμότητα 120
5.4.3 Στρατηγικές backup & disaster recovery 122
5.4.4 Ασφάλεια και προστασία δεδομένων 123
5.4.5 Καταγραφή, έλεγχος και ακεραιότητα 125

6 Καινοτομία & Μελλοντικές Τάσεις 129

6.1 AI και ML σε τακτικά στρατιωτικά δίκτυα 129
6.1.1 Προσαρμοστική δρομολόγηση και διαχείριση κυκλοφορίας 129
6.1.2 Ανίχνευση και απόκριση σε απειλές 130
6.1.3 Ενεργειακή βελτιστοποίηση 131

6.1.4 Real Time Decision Support 131
6.1.5 Ενδεικτική Εφαρμογή: DAPRA OFFSET 132

6.2 Κβαντικές επικοινωνίες και Entanglement 133
6.2.1 Quantum Key Distribution(QKD) 133
6.2.2 Κβαντική διεμπλοκή(Entanglement) 134
6.2.3 Στρατιωτικές εφαρμογές και προγράμματα 135
6.2.4 Προκλήσεις και μελλοντικές κατευθύνσεις 136

6.3 IoMT : Εξέλιξη και Πρόκληση 137
6.3.1 Αρχιτεκτονική και Λειτουργία 137
6.3.2 Ενδεικτικές εφαρμογές 138
6.3.3 Προκλήσεις και κίνδυνοι 139
6.3.4 Στρατηγική σημασία 140

6.4 Τεχνολοηική σύγκλιση και ολοκληρωμένες πλατφόρμες 141
6.4.1 Ορισμός και ανάγκη για σύγκλιση 141
6.4.2 Ολοκληρωμένες πλατφόρμες C4ISR 142
6.4.3 Τεχνολογικές προϋποθέσεις για ολοκλήρωση 143
6.4.4 Τεχνολογικές προϋποθέσεις για ολοκλήρωση 145

7 Συμπεράσματα & Προτάσεις 147

Βιβλιογραφία 151

Ευρετήριο Σχημάτων

Σχήμα 1- Εξέλιξη στρατιωτικών επικοινωνιών στο χρόνο 4
Σχήμα 2- Εμβληματικά συστήματα στρατιωτικών επικοινωνιών([8], [7], [9]) 5
Σχήμα 3- Στρατιωτικό σενάριο ασύρματης επικοινωνίας [1] 6
Σχήμα 4-Παράδειγμα δικτύου Link-16 για τακτική διαλειτουργική επικοινωνία μεταξύ εναέριων, επίγειων και αντιαεροπορικών μονάδων(L3Harris Technologies, “Link-16 Tactical Data Links”). 10
Σχήμα 5 - Στρατιωτικά σενάρια χρήσης 5G με έμφαση σε εφαρμογές χαμηλής καθυστέρησης και υψηλής αξιοπιστίας [12] 12
Σχήμα 6 - Δομή πεδίου αισθητήρων με master-slave αρχιτεκτονική[25] 14
Σχήμα 7 - Παράδειγμα γνωσιακού τακτικού δικτύου με gateway και non-gateway κόμβους[27] 15
Σχήμα 8 - Συγκριτική εξέλιξη ρυθμών μετάδοσης σε εμπορικά και στρατιωτικά δίκτυα 17
Σχήμα 9 - Αρχιτεκτονική SDR με modular σχεδιασμό για υποστήριξη πολλαπλών πρωτοκόλλων επικοινωνίας [14] 18
Σχήμα 10 - Οι τρεις κατηγορίες υπηρεσιών του 5G [12] 22
Σχήμα 11-Αρχιτεκτονική Network based Defence[38] 24
Σχήμα 12-Παράδειγμα επίθεσης spoofing/jamming σε drone στο πεδίο μάχης[39] 25
Σχήμα 13-Στρατηγικό μοντέλο υβριδικού δικτύου(HSTN) που ενσωματώνει δορυφόρους, UAVs και επίγειες 5G/6G υποδομές[42] 27
Σχήμα 14-Φορητό στρατιωτικό SDR με ανθεκτικό σχεδιασμό πεδίου μάχης[46] 28
Σχήμα 15-Ενσωμάτωση SDR σε MANET για τακτική επικοινωνία 30
Σχήμα 16 - Δίκτυο πεδίου μάχης με nodes που λειτουργούν ως κόμβοι Cognitive MANETs[58] 32
Σχήμα 17-Παράδειγμα επίθεσης jamming σε στρατιωτικό ad-hoc δίκτυο Cognitive Radio/SDR [61]. 34
Σχήμα 18-UAV που λειτουργεί ως εναέριος σταθμός βάσης[62] 35
Σχήμα 19-Στρατιωτικό TMN και εργαστηριακή προσομοίωση[68] 38
Σχήμα 20-Τρισδιάστατο στρατιωτικό mesh δίκτυο UAVs[72] 40
Σχήμα 21- Επίθεση GPS spoofing[76] 42
Σχήμα 22-Ορισμένες τυπικές εφαρμογές σμηνών UAV [78] 44
Σχήμα 23-Στρατιωτικό δίκτυο SATCOM με συνδεσιμότητα ξηράς, θάλασσας και αέρα μέσω GEO/MEO/LEO δορυφόρων[81] 46
Σχήμα 24-Πολυεπίπεδη αρχιτεκτονική στρατιωτικών SATCOM[84] 48
Σχήμα 25-Συνύπαρξη GEO και LEO δορυφόρων για υποστήριξη real-time και υψηλής χωρητικότητας υπηρεσιών σε επίγειους, ναυτικούς και UAV χρήστες[85] 50
Σχήμα 26-Παράδειγμα επίθεσης jamming σε δορυφορικές επικοινωνίες, όπου ο δορυφόρος διακόπτεπαι από σήματα παρεμβολής[86] 51
Σχήμα 27-Ενσωμάτωση δορυφορικών και επίγειων δικτύων για μελλοντικές εφαρμογές [87] 54
Σχήμα 28-Γραφική απεικόνιση επιλεγμένων TCP τροποποιήσεων για ασύρματα και τακτικά δίκτυα57
Σχήμα 29-Εφαρμογή του Delay-Tolerant Networking(DTN) σε διαστημικές αποστολές 58
Σχήμα 30-Απλή αναπαράσταση του Split-TCP σε τακτικό δίκτυο [113] 61
Σχήμα 31-Εφαρμογή MANET σε στρατιωτική αποστολή [108] 63
Σχήμα 32-Τυπολογία MANETs 64
Σχήμα 33-Δομή πακέτων IPsec με AH και ESP(χωρίς modes) 71
Σχήμα 34-Απεικόνιση των δύο λειτουργικών τάσεων(Transport & Tunnel Mode) του IPsec [123] 72
Σχήμα 35-Απεικόνιση ασφαλούς μετάδοσης δεδομένων UAV μέσω IPsec σε πλατφόρμες ISR. 72
Σχήμα 36-Αρχιτεκτονική δικτύου HAIPE [134] 75

Σχήμα 37-TACLANE-Nano(KG-175N) [112] 78
Σχήμα 38-Zero-Trust vs. Παραδοσιακό δίκτυο [139] 79
Σχήμα 39- Στρατιώτης εξοπλισμένος με φορητό SATCOM manpack τερματικό [159] 84
Σχήμα 40- Αρχιτεκτονικά μοντέλα δορυφορικών επικοινωνιών star topology, mesh topology, bent-pipe και double-hop αρχιτεκτονικές [140] 86
Σχήμα 41- Παράδειγμα GPS spoofing σε UAV [83] 94
Σχήμα 42- Παράδειγμα τεχνικής beamforming με συστοιχίες κεραιών για την απόρριψη παρεμβολών [166] 97
Σχήμα 43- Αρχιτεκτονική IoMT για στρατιωτικά δίκτυα με πολυεπίπεδη διάρθρωση [176] 103
Σχήμα 44- Επτά στάδια μιας τυπικής κυβερνοεπίθεσης σύμφωνα με το μοντέλο Cyber Kill Chain [179] 105
Σχήμα 45- Αναπαράσταση της λειτουργίας του Stuxnet : μόλυνση μέσω USB [199] 114
Σχήμα 46- Διαδρομή μόλυνσης από την επίθεση [200] 115
Σχήμα 47- Το UAV-RQ-170 Sentinel [201] 116
Σχήμα 48- Live Cyber Threat Map : Διεθνής ροή επιθέσεων 116
Σχήμα 49- Διάταξη active 122
Σχήμα 50- Αρχιτεκτονική SIEM σε στρατιωτικό δίκτυο[205] 126
Σχήμα 51- Απεικόνιση καταγραφών τύπου blockchain[206] 127
Σχήμα 52- Swarm drones σε πειραματικό πεδίο προγράμματος DAPRA OFFSET [214] 132
Σχήμα 53- Μετάδοση κβαντικής εμπλοκής μέσω του δορυφόρου Micius ανάμεσα στους σταθμούς Nanshan και Delingha [217] 135

Ευρετήριο Πινάκων

Πίνακας 1-Σύγκριση αναλογικών, ψηφιακών και δικτυοκεντρικών συστημάτων 7
Πίνακας 2-Τύποι στρατιωτικών επικοινωνιών και βασικές παράμετροι 10
Πίνακας 3-Σύγκριση MANETs και παραδοσιακών δικτύων 65

Π ί ν α κ α ς Α κ ρ ω ν υ μ ί ω ν

ΑΚΡΩΝΥΜΙΟ	ΑΓΓΛΙΚΟΣ ΟΡΟΣ	ΕΛΛΗΝΙΚΗ ΑΠΟΔΟΣΗ
AEHF	Advanced Extremely High Frequency	Προηγμένο Σύστημα Εξαιρετικά Υψηλών Συχνοτήτων
AODV	Ad-Hoc-On-Demand Distance Vector	Πρωτόκολλο Δρομολόγησης
AI	Artificial Intelligence	Τεχνητή Νοημοσύνη
API	Application Programming Interface	Διεπαφή Προγραμματισμού Εφαρμογών
APT	Advanced Persistent Threat	Εξελιγμένη Επίμονη Απειλή
ARPANET	Advanced Research Projects Agency Network	Δίκτυο Οργανισμών Προηγμένων Ερευνητικών Έργων
ASN.1	Abstract Syntax Notation One	Σημειογραφία Αφηρημένης Σύνταξης Ένα
BB84	Benett & Brassard 1984(Quantum Key Distribution Protocol)	Πρωτόκολλο Κβαντικής Διανομής Κλειδιού
C2	Command and Control	Διοίκηση και Έλεγχος
C3	Command, Control and Communications	Διοίκηση, Έλεγχος και Επικοινωνίες
C4ISR	Command, Control, Computers, Intelligence, Surveillance and Reconnaissance	Διοίκηση, Έλεγχος, Υπολογιστές, Πληροφορίες, Επιτήρηση και Αναγνώριση
CIA	Confidentiality, Integrity, Availability	Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα
CVE	Common Vulnerabilities and Exposures	Συνήθειες, Ευπάθειες και Εκθέσεις
DARPA	Defense Advanced Research Projects Agency	Οργανισμός Προηγμένων Αμυντικών Ερευνητικών Προγραμμάτων
DDos	Distributed Denial of Service	Κατανεμημένη Επίθεση Άρνησης Υπηρεσίας

DoD	Department of Defense	Υπουργείο Άμυνας των ΗΠΑ
DR	Disaster Recovery	Ανάκαμψη από καταστροφές
DSS	Dynamic Spectrum Sharing	Δυναμική Κοινή Χρήση Φάσματος
DSSS	Direct Sequence Spread Spectrum	Άμεση Αλληλουχία Διασποράς Φάσματος
DTN	Delay Tolerant Networking	Δικτύωση με Ανοχή Καθυστέρησης
DSR	Dynamic Source Routing	Δυναμική Δρομολόγηση Πηγής
ECN	Explicit Congestion Notification	Ρητή Ειδοποίηση Συμφόρησης
eMBB	Enhanced Mobile Broadband	Βελτιωμένο Κινητό Ευρυζωνικό Δίκτυο
EMCON	Encapsulating Security Payload	Ενθυλάκωση ωφέλιμου φορτίου ασφαλείας
EU	European Union	Ευρωπαϊκή Ένωση
FEC	Forward Error Correction	Διόρθωση Σφάλματος Προώθησης
FHSS	Frequency Hopping Spread Spectrum	Φάσμα Εξάπλωσης με Μεταπήδηση Συχνότητας
FM	Frequency Modulation	Διαμόρφωση Συχνότητας
FMN	Federated Mission Networking	Ομοσπονδιακό Δίκτυο Αποστολών
GBS	Global Broadcast Service	Υπηρεσία Παγκόσμιας Εκπομπής
GEO	Geostationary Earth Orbit	Γεωστατική Τροχιά
GDMS	General Dynamics Mission Systems	Συστήματα Αποστολής Γενικής Δυναμικής
GPS	Global Positioning System	Παγκόσμιο Σύστημα Εντοπισμού Θέσης

HAIPE	High Assurance Internet Protocol Encryptor	Μακράς Εμβέλειας Δίκτυο
HAPs	High-Altitude Platforms	Πλατφόρμα Υψηλού Υψομέτρου
HF	High Frequency	Υψηλή Συχνότητα
IDS	Intrusion Detection System	Σύστημα Ανίχνευσης Εισβολών
IoMT	Internet of Military Things	Στρατιωτικό Διαδίκτυο των Πραγμάτων
IT	Internet of Things	Διαδίκτυο Πραγμάτων
IPsec	Internet Protocol Security	Ασφάλεια Πρωτοκόλλου Διαδικτύου
ISR	Intelligence, Surveillance and Reconnaissance	Πληροφορίες, Επιτήρηση και Αναγνώριση
ITN	Integrated Tactical Network	Ολοκληρωμένο Τακτικό Δίκτυο
JADC2	JavaScript Object Notation	Διακλαδική Διοίκηση και Έλεγχος Πολλαπλών Πεδίων
LEO	Low Earth Orbit	Χαμηλή Γήινη Τροχιά
LTE	Long Term Evolution	Πρότυπο Κινητής Ευρυζωνικότητας
MAC	Medium Access Control	Έλεγχος Πρόσβασης Μέσου
MANET	Mobile Ad-hoc Network	Κινητό Αυτό-οργανωμένο Δίκτυο
M-code	Military Code(Encrypted GPS code)	Στρατιωτικός Κώδικας(Κρυπτογραφημένος Κωδικός GPS)
MEC	Multi-access Edge-Computing	Πολλαπλής Πρόσβασης Edge Computing
MEO	Medium Earth Orbit	Μεσαία Τροχιά Γης
MLNET	Military Network	Στρατιωτικό Δίκτυο
MILSTAR	Military Strategic and Tactical Relay	Στρατιωτική Στρατηγική και Τακτική Σκυταλοδρομία

ML	Machine Learning	Μηχανική Μάθηση
MLOps	Machine Learning Operations	Λειτουργίες Διαχείρισης Μοντέλων Μηχανικής Μάθησης
MIMO	Multiple Input Multiple Output	Πολλαπλή Είσοδος-Πολλαπλή Έξοδος
MPLS	Multiprotocol Label Switching	Εναλλαγή ετικετών πολλαπλών πρωτοκόλλων
MPTCP	Multipath Transmission Control Protocol	Πρωτόκολλο Ελέγχου Μετάδοσης Πολλαπλών Διαδρομών
MTBF	Mean Time Between Failures	Μέσος Χρόνος Μεταξύ Βλαβών
MTTD	Mean Time to Repair	Μέσος Χρόνος Επισκευής
MTTR	Mean Time to Detect	Μέσος Χρόνος Ανίχνευσης
mMTC	Massive Machine Type Communications	Μαζικές επικοινωνίες Τύπου Μηχανής
NCO	Network Centric Operations	Λειτουργίες με επίκεντρο το δίκτυο
NATO	North Atlantic Treaty Organization	Οργανισμός Βορειοατλαντικού Συμφώνου
NFV	Network Function Virtualization	Εικονοποίηση Λειτουργιών Δικτύου
NIAP/CC	National Information Assurance Partnership/ Common Criteria	Εθνική Συνεργασία για την Ασφάλιση Πληροφοριών/ Κοινά Κριτήρια
NICS	National Institute of Standards and Technology	Ολοκληρωμένο Σύστημα Επικοινωνιών του ΝΑΤΟ
NTP	Network Time Protocol	Πρωτόκολλο Χρόνου Δικτύου

NSA	National Security Agency	Εθνική Υπηρεσία Ασφαλείας
OLSR	Optimized Link State Routing	Βελτιστοποιημένη Δρομολόγηση Κατάστασης Ζεύξης
OSI	Open Systems Interconnection	Διασύνδεση Ανοικτών Συστημάτων
OT	Operational Technology	Επιχειρησιακή Τεχνολογία
QoS	Quality of Service	Ποιότητα Υπηρεσίας
QKD	Quantum Key Distribution	Κατανομή Κβαντικού Κλειδιού
RAN	Radio Access Network	Δίκτυο Ραδιοπρόσβασης
RBAC	Role-Based Access Control	Έλεγχος Πρόσβασης Βάσει Ρόλων
RF	Radio Frequency	Ραδιοφωνική Συχνότητα
RPO	Recovery Point Objective	Στόχος Σημείου Ανάκαμψης
RTO	Recovery Time Objective	Στόχος Χρόνου Ανάρρωσης
SCPS	Space Communications Protocol Standards	Πρότυπα Πρωτοκόλλου Διαστημικών Επικοινωνιών
SDR	Software Defined Radio	Ραδιοσύστημα Οριζόμενο από Λογισμικό
SDN	Software Defined Networking	Δικτύωση Οριζόμενο από Λογισμικό
SHF	Super High Frequency	Πολύ Υψηλή Συχνότητα
SIEM	Security Information and Event Management	Διαχείριση Πληροφοριών και Συμβάντων Ασφαλείας
SIGINT	Signals Intelligence	Συλλογή Πληροφοριών μέσω Σημάτων
SINCGARS	Signal Channel Ground Airborne Radio Systems	Μονοκάναλο Ραδιοσύστημα Χερσαίας και Εναέριας Χρήσης
SOAR	Security Orchestration, Automation and Response	Ορχήστρωση, Αυτοματοποίηση και Απόκριση Ασφάλειας
SSL/TLS	Secure Sockets Layer/ Transport Layer Security	Επίπεδο Ασφαλών Υποδοχών/ Επίπεδο Μεταφοράς Ασφάλεια
STANAG	Standardization Agreement	Συμφωνία Τυποποίησης
TACLANE	Tactical Local Area Network Encryptor	Κρυπτογράφος Τοπικού Δικτύου
TCP/IP	Transmission Control Protocol/ Internet Protocol	Πρωτόκολλο Ελέγχου Μετάδοσης/ Πρωτόκολλο Διαδικτύου
TMN	Tactical Mesh Network	Τακτικό Δίκτυο Πλέγματος

TS/SCI	Top Secret/ Sensitive Compartmented Information	Άκρως Απόρρητες/ Ευαίσθητες Διαμερισμένες Πληροφορίες
UAV	Unmanned Aerial Vehicle	Μη Επανδρωμένο Αεροσκάφος
UGV	Unmanned Ground Vehicle	Μη Επανδρωμένο Επίγειο Όχημα
UHF	Ultra High Frequency	Υπερυψηλή συχνότητας
URLLC	Ultra Reliable Low Latency Communications	Εξαιρετικά Αξιόπιστες Επικοινωνίες Χαμηλής Καθυστέρησης
VHF	Very High Frequency	Πολύ Υψηλή Συχνότητα
VPN	Virtual Private Network	Εικονικό Ιδιωτικό Δίκτυο
WGS	Wideband Global SATCOM	Παγκόσμια Ευρυζωνικό SATCOM
WIN-T	Warfighter Information Network Tactical	Τακτικό Πληροφοριακό Δίκτυο Αμερικανικού Στρατού
Zero Trust	Zero Trust Security Architecture	Αρχιτεκτονική Ασφάλειας Μηδενικής Εμπιστοσύνης

ΚΕΦΑΛΑΙΟ 1

1 Εισαγωγή

Οι τηλεπικοινωνίες στις ένοπλες δυνάμεις διαδραματίζουν διαχρονικά καθοριστικό ρόλο στον επιχειρησιακό σχεδιασμό και στην αποτελεσματικότητα των αποστολών. Η δυνατότητα να επικοινωνούν άμεσα και με ασφάλεια οι στρατιωτικές μονάδες, να μεταδίδονται εντολές, να συλλέγονται πληροφορίες και να λαμβάνονται αποφάσεις σε πραγματικό χρόνο, επηρεάζει άμεσα την αποτελεσματικότητα κάθε επιχείρησης [1]. Ειδικά στο σύγχρονο πεδίο μάχης, όπου τα δεδομένα κινούνται με αστραπιαίους ρυθμούς, η επικοινωνία γίνεται όχι μόνο τεχνικό εργαλείο, αλλά και κρίσιμο στρατηγικό πλεονέκτημα.

Τα τελευταία χρόνια, η ραγδαία εξέλιξη της τεχνολογίας έχει αλλάξει ριζικά το τοπίο στον τομέα των στρατιωτικών επικοινωνιών. Από τα κλασσικά ραδιοσυστήματα, έχουμε περάσει σε πιο ευέλικτες και έξυπνες λύσεις, όπως τα Software Defined Radios(SDRs) και τα κινητά Ad-hoc δίκτυα(MANETs). Παράλληλα, τεχνολογίες όπως το 5G/6G, η τεχνητή νοημοσύνη (AI), αλλά και οι γνωσιακές δικτυακές αρχιτεκτονικές (cognitive networks) αρχίζουν να ενσωματώνονται σταδιακά σε στρατιωτικές εφαρμογές, δίνοντας νέες δυνατότητες, αλλά και ανοίγοντας καινούρια πεδία κινδύνων όπως ηλεκτρονικές παρεμβολές(jamming) και κυβερνοεπιθέσεις [2].

Η αυξανόμενη ψηφιοποίηση φέρνει στο προσκήνιο και σοβαρές προκλήσεις. Τα στρατιωτικά δίκτυα δεν είναι πλέον απομονωμένα, αλλά συνδέονται ή πρέπει να συνδέονται με άλλες υποδομές, πλατφόρμες και ακόμα και συμμαχικές δυνάμεις. Αυτό δημιουργεί αυξημένες απαιτήσεις για ασφάλεια, διαλειτουργικότητα, προστασία απέναντι σε κυβερνοεπιθέσεις και προσαρμογή σε πολύπλοκα περιβάλλοντα. Παραβιάσεις ασυρμάτων επικοινωνιών, ακόμη και η απλή απώλεια πληροφορίας μπορούν να έχουν καταστροφικές συνέπειες [3].

Είναι σημαντικό να αναγνωριστεί ότι οι τηλεπικοινωνίες δεν αποτελούν πλέον απλώς ένα τεχνικό μέσο υποστήριξης των επιχειρήσεων, αλλά και έναν πυλώνα επιχειρησιακής ισχύος, στον οποίο επενδύουν διαρκώς οι σύγχρονες ένοπλες δυνάμεις. Η έγκαιρη μετάδοση δεδομένων, η ασφαλής διαχείριση πληροφοριών και η δυνατότητα συνεργασίας μεταξύ ετερογενών συστημάτων καθορίζουν σε μεγάλο βαθμό την επιτυχία ή αποτυχία μιας αποστολής. Παράλληλα, η ανάπτυξη νέων τεχνολογιών όπως η κβαντική κρυπτογράφηση και τα δίκτυα πολλαπλών επιπέδων ασφαλείας(multi-layered security) υπόσχεται να ενισχύσει περαιτέρω την ανθεκτικότητα και την αξιοπιστία των επικοινωνιών.

Εντός αυτού του πλαισίου, η παρούσα διπλωματική εργασία στοχεύει στην ολοκληρωμένη επισκόπηση των τεχνολογιών και των πρωτοκόλλων τηλεπικοινωνιών που χρησιμοποιούνται σε στρατιωτικά περιβάλλοντα. Η προσέγγιση είναι κυρίως βιβλιογραφική, βασισμένη δηλαδή σε μελέτες,

τεχνικές αναφορές και ερευνητικά άρθρα για να συγκεντρωθούν οι βασικές πληροφορίες και να οργανωθούν σε μια ολοκληρωμένη παρουσίαση. Συγκεκριμένα, ερευνώνται :

- Οι βασικές αρχές και λειτουργίες των τεχνολογιών SDR, MANETs, 5G/6G και AI-based communications
- Τα κυρίαρχα πρωτόκολλα και πρότυπα (STANAGs, IPsec, routing protocols) που εφαρμόζονται
- Οι σύγχρονες απειλές που αντιμετωπίζουν τα στρατιωτικά πληροφοριακά δίκτυα
- Οι αρχιτεκτονικές και τεχνολογικές προσεγγίσεις για την ασφάλεια, τη διαλειτουργικότητα και την ευελιξία των επικοινωνιών

Η εργασία χωρίζεται σε επτά κεφάλαια. Ξεκινάει από μία σύντομη αναδρομή στην εξέλιξη των στρατιωτικών επικοινωνιών και τα βασικά χαρακτηριστικά που απαιτούνται από αυτά τα συστήματα. Στη συνέχεια, εστιάζει στις τεχνολογίες που χρησιμοποιούνται σήμερα, όπως τα δίκτυα 5G, τα SDR και οι επικοινωνίες μέσω drones. Έπειτα, μελετάται η δομή και τα πρωτόκολλα των στρατιωτικών δικτύων, ενώ ακολουθεί ανάλυση των κινδύνων και των απειλών που προκύπτουν, όπως οι επιθέσεις σε κρίσιμες υποδομές και η διαρροή πληροφοριών. Στο προτελευταίο κεφάλαιο, αναφέρονται οι καινοτομίες που έρχονται, όπως η τεχνητή νοημοσύνη και η κβαντική επικοινωνία. Τέλος, φαίνονται τα βασικά συμπεράσματα που προκύπτουν από την μελέτη και προτάσεις για περαιτέρω σκέψη ή έρευνα.

Η συμβολή της εργασίας έγκειται τόσο στην συγκέντρωση και ανάλυση τεχνολογικών δεδομένων όσο και στην αποτύπωση της αλληλεπίδρασης μεταξύ επιχειρησιακών αναγκών και τεχνολογικών μέσων. Με αυτόν τον τρόπο, ο αναγνώστης αποκτά μια σφαιρική εικόνα για το πώς οι τεχνολογίες επικοινωνιών εξελίσσονται, προσαρμόζονται και τελικά μεταμορφώνουν το πεδίο των στρατιωτικών επιχειρήσεων.

Σκοπός της εργασίας είναι να αποτελέσει μια χρήσιμη αναφορά για όποιον θέλει να κατανοήσει καλύτερα τον ρόλο των τηλεπικοινωνιών στο στρατιωτικό περιβάλλον και να αναδείξει την πολυπλοκότητα και τη σημασία του θέματος, ειδικά μέσα στον κόσμο που διαμορφώνεται σήμερα.

ΚΕΦΑΛΑΙΟ 2

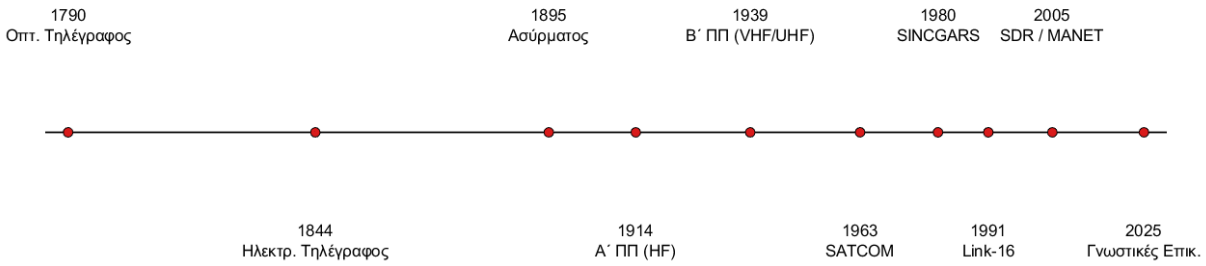
2 Ιστορική Εξέλιξη και Θεμελιώδεις Αρχές

Οι στρατιωτικές τηλεπικοινωνίες έχουν μακρά και ιδιαίτερη κρίσιμη ιστορία, καθώς αποτελούσαν πάντα βασικό παράγονται για την επιτυχία των επιχειρήσεων στο πεδίο. Από τα σήματα καπνού και τους κώδικες Μορς, μέχρι τα δίκτυα υψηλής τεχνολογίας που χρησιμοποιούνται σήμερα, η ανάγκη για γρήγορη, ασφαλή και αξιόπιστη μετάδοση εντολών και πληροφοριών είναι διαχρονική. Στο κεφάλαιο αυτό, εξετάζεται πώς εξελίχθηκαν οι στρατιωτικές επικοινωνίες στο πέρασμα του χρόνου, πώς οι τεχνολογίες επηρέασαν τις τακτικές και την οργάνωση των ένοπλων δυνάμεων, αλλά και ποια είναι τα βασικά χαρακτηριστικά που πρέπει να πληροί κάθε στρατιωτικό επικοινωνιακό σύστημα.

Σκοπός του κεφαλαίου είναι η κατανόηση όχι μόνο με την χρονολογική πορεία της τεχνολογίας αλλά και τις θεμελιώδεις απαιτήσεις που παραμένουν σταθερές μέχρι σήμερα : ασφάλεια, αξιοπιστία, ευελιξία, ταχύτητα και λειτουργικότητα σε αντίξοες συνθήκες. Επιπλέον, γίνεται μια σύντομη αναφορά στις βασικές διαφορές που υπάρχουν ανάμεσα στις στρατιωτικές και τις εμπορικές τηλεπικοινωνιακές λύσεις, ώστε να γίνει σαφές γιατί ο στρατιωτικός τομέας απαιτεί εξειδικευμένες προσεγγίσεις.

2.1 Εξέλιξη στρατιωτικών επικοινωνιών

Η εξέλιξη των στρατιωτικών επικοινωνιών αποτελεί μια συνεχόμενη διαδικασία που αντικατοπτρίζει την πρόοδο της τεχνολογίας και τις μεταβαλλόμενες επιχειρησιακές ανάγκες των ένοπλων δυνάμεων. Από την αρχαιότητα έως τις σύγχρονες δικτυοκεντρικές επιχειρήσεις, η αποστολή παραμένει η ίδια : έγκαιρη, αξιόπιστη και ασφαλής μετάδοση πληροφοριών, η οποία να επιτρέπει την αποτελεσματική διοίκηση και τον έλεγχο (Command and Control- C2) ακόμη και στις πιο αντίξοες συνθήκες [4]. Η πορεία αυτή δεν είναι γραμμική αλλά χαρακτηρίζεται από τεχνολογικά άλματα που επηρέασαν καθοριστικά το δόγμα και τις τακτικές μάχης, δημιουργώντας ένα πολυστρωματικό πεδίο επικοινωνιακών λύσεων που λειτουργούν συμπληρωματικά. Η συνολική αυτή εξέλιξη απεικονίζεται στο Σχήμα 1, όπου παρουσιάζονται οι βασικές τεχνολογικές περίοδοι και τα αντίστοιχα μέσα επικοινωνίας που σημάδεψαν κάθε εποχή.



Σχήμα 1- Εξέλιξη στρατιωτικών επικοινωνιών στο χρόνο

2.2 Προ-Ηλεκτρική και Πρώιμη Ηλεκτρική Εποχή

Στην προ-ηλεκτρική εποχή, οι στρατιωτικές επικοινωνίες βασίζονταν σε οπτικά και ηχητικά μέσα. Φρυκτωρίες, σημαίες, καπνοσήματα και κώδωνες αποτελούσαν κύρια εργαλεία μετάδοσης, με περιορισμένη εμβέλεια και υψηλή εξάρτηση από τις περιβαλλοντικές συνθήκες. Η ανάπτυξη του οπτικού τηλεγράφου από τον Claude Chappe το 1790 [5] έφερε την πρώτη «επανάσταση», επιτρέποντας κωδικοποιημένη εφεύρεση του ηλεκτρικού τηλεγράφου στα μέσα του 19^{ου} αιώνα άλλαξε δραστικά στην επιχειρησιακή εικόνα, επιτρέποντας σχεδόν άμεση μετάδοση στρατιωτικών διαταγών σε μεγάλες αποστάσεις, ενώ το ραδιόφωνο και η ασύρματη τηλεγραφία στα τέλη του αιώνα επέτρεψαν για πρώτη φορά επικοινωνία χωρίς φυσική σύνδεση. Αυτή η περίοδος σηματοδότησε την απαρχή της μετάβασης από τις «γραμμές θέας» (line-of-sight) στις ασύρματες ζεύξεις, ανοίγοντας τον δρόμο για ευέλικτες και γρήγορες επιχειρήσεις μεγάλης κλίμακας.

2.2.1 Α’ & Β’ Παγκόσμιος Πόλεμος

Κατά τον Α’ Παγκόσμιο Πόλεμο, οι ένοπλες δυνάμεις εισήγαγαν εκτεταμένα το ενσύρματο τηλέφωνο πεδίου και τους ασυρμάτους HF(3-30MHz), που παρείχαν επικοινωνία μεγάλων αποστάσεων αλλά επηρεάζονταν έντονα από τις καιρικές και γεωμαγνητικές συνθήκες[6]. Χρησιμοποιήθηκαν επίσης περιστέρια ταχυδρομείου και σηματοφόρα οχήματα για ειδικές αποστολές, αναδεικνύοντας την ανάγκη για πολυεπίπεδη επικοινωνιακή υποδομή. Στον Β’ Παγκόσμιο Πόλεμο, η εξέλιξη των ραδιοεπικοινωνιών σε συχνότητες YHF(30-300MHz) και UHF(300 MHz-3GHz) βελτίωσε την ποιότητα μετάδοσης και την αντοχή σε παρεμβολές. Παράλληλα, η χρήση της κρυπτογραφικής μηχανής Enigma από τις δυνάμεις του Άξονα και η αποκρυπτογράφησή της από τους Συμμάχους [6] ανέδειξαν τον ρόλο της κρυπτογραφίας στην εξασφάλιση του πληροφοριακού πλεονεκτήματος. Η ανάπτυξη ολοκληρωμένων δικτύων επικοινωνίας που συνέδεαν μονάδες ξηράς, αέρα και θάλασσας αποτέλεσε τον πρόδρομο των σύγχρονων πολυκλαδικών επιχειρήσεων.

2.2.2 Ψυχρός Πόλεμος και Ψηφιακή Επανάσταση

Η περίοδος 1950-1990 χαρακτηρίστηκε από τεχνολογική έκρηξη στις στρατιωτικές επικοινωνίες, με την εισαγωγή των πρώτων δορυφορικών συστημάτων και την ανάπτυξη ασφαλών, πολυκαναλικών ραδιοζεύξεων. Το Defense Satellite Communications System(DSCS) και αργότερα το MILSTAR [7] παρείχαν παγκόσμια κάλυψη, ανθεκτικότητα σε παρεμβολές και κρυπτογράφηση επιπέδου NSA. Στο τακτικό επίπεδο , το Signal Channel Ground and Airborne Radio System (SINCGARS) εισήγαγε frequency hopping για αποφυγή ανίχνευσης και παρεμβολών, ενώ η χρήση κρυπτογραφημένων UHF δορυφορικών επικοινωνιών (SATCOM) επέτρεψε διακλαδικές επιχειρήσεις σε παγκόσμια κλίμακα. Παράλληλα, η δημιουργία του MILNET-πρόδρομου του ARPANET-έθεσε τις βάσεις για τη σημερινή δικτυοκεντρική φιλοσοφία επιχειρήσεων, συνδέοντας κέντρα διοίκησης, βάσεις και απομακρυσμένα θέατρα επιχειρήσεων σε ένα ενιαίο πληροφοριακό δίκτυο. Τα σημαντικότερα συστήματα αυτής της περιόδου, που σηματοδότησαν την πορεία από την αναλογική επικοινωνία και την κρυπτογράφηση Enigma έως τα σύγχρονα δορυφορικά δίκτυα, παρουσιάζονται συνοπτικά στο Σχήμα 2, όπου αποτυπώνεται η τεχνολογική εξέλιξη των στρατιωτικών επικοινωνιών μέσα σε τέσσερις χαρακτηριστικές δεκαετίες.



Σχήμα 2- Εμβληματικά συστήματα στρατιωτικών επικοινωνιών([8], [7], [9])

2.2.3 Μετά τον Ψυχρό Πόλεμο - Δικτυοκεντρικές Επιχειρήσεις

Ο πόλεμος του Κόλπου το 1991 αποτέλεσε σημείο καμπής για την επιχειρησιακή χρήση της τεχνολογίας. Το Link-16 [9], ένα τυποποιημένο τακτικό δίκτυο δεδομένων (STANAG5516), επέτρεψε την ανταλλαγή δεδομένων σε πραγματικό χρόνο μεταξύ αεροσκαφών, πλοίων και επίγειων μονάδων, αυξάνοντας την επίγνωση κατάστασης και μειώνοντας τον χρόνο απόφασης. Σταδιακά, η έννοια των Network-Centric Operations (NCO) αντικατέστησε τα απομονωμένα συστήματα, επιτρέποντας την ενοποίηση διαφορετικών πλατφορμών μέσω κοινών πρωτοκόλλων. Στις αρχές του 21ου αιώνα, το

Integrated Tactical Network(ITN) συνδύασε εμπορικές και στρατιωτικές τεχνολογίες, χρησιμοποιώντας SATCOM, επίγειες ασύρματες ζεύξεις και κινητούς αναμεταδότες, εξασφαλίζοντας επικοινωνία ακόμη και σε περιβάλλοντα έντονου ηλεκτρονικού πολέμου ή απώλειας υποδομών. Η λειτουργία αυτών των δικτύων βασίζεται στην πλήρη διασύνδεση εναέριων, επίγειων, ναυτικών και δορυφορικών πλατφορμών, ώστε να επιτυγχάνεται ενιαία εικόνα τακτικής κατάστασης και συνεχής ροή δεδομένων. Ένα χαρακτηριστικό παράδειγμα αυτής της αρχιτεκτονικής παρουσιάζεται στο Σχήμα 3, όπου απεικονίζεται ένα ολοκληρωμένο στρατιωτικό σενάριο ασύρματης επικοινωνίας με ταυτόχρονη χρήση SATCOM, UAVs και τακτικών επίγειων κόμβων.



Σχήμα 3- Στρατιωτικό σενάριο ασύρματης επικοινωνίας [1]

2.2.4 Σύγχρονες τάσεις και IoMT

Η τρέχουσα εποχή χαρακτηρίζεται από την υιοθέτηση ευέλικτων, επεκτάσιμων και ανθεκτικών επικοινωνιακών υποδομών. Τα Software Defined Radios(SDRs) επιτρέπουν την αλλαγή συχνοτήτων και πρωτοκόλλων μέσω λογισμικού, ενώ τα Mobile Ad-Hoc Networks (MANETs) προσφέρουν δυναμική αυτό-οργάνωση χωρίς σταθερή υποδομή. Η έννοια του Internet of Military Things(IoMT) συνδέει αισθητήρες, οχήματα, UAVs και στρατιωτικό εξοπλισμό σε ένα ενιαίο, ασφαλές δίκτυο, παρέχοντας πληροφορίες σε πραγματικό χρόνο για τη βελτίωση της επίγνωσης κατάστασης και λήψης αποφάσεων [10]. Οι γνωστικές (Cognitive Radios) προσθέτουν αυτονομία στη διαχείριση φάσματος, επιλέγοντας δυναμικά βέλτιστες διαδρομές μετάδοσης και αντιμετωπίζοντας ενεργά παρεμβολές, ακόμη και σε έντονα ανταγωνιστικά ηλεκτρομαγνητικά περιβάλλοντα.

Πίνακας 1-Σύγκριση αναλογικών, ψηφιακών και δικτυοκεντρικών συστημάτων

Χαρακτηριστικό	Αναλογικά Συστήματα	Ψηφιακά Συστήματα	Δικτυοκεντρικά Συστήματα
Ρυθμός Μετάδοσης Δεδομένων	Πολύ χαμηλός	Μεσαίος-Υψηλός	Πολύ υψηλός
Ποιότητα σήματος	Επηρεάζεται έντονα από θόρυβο	Βελτιωμένη λόγω κωδικοποίησης	Βέλτιστη με δυναμική βελτιστοποίηση
Ανθεκτικότητα σε παρεμβολές	Χαμηλή	Μέτρια-Χρήση spread spectrum και κρυπτογράφησης	Υψηλή με frequency hopping και cognitive radios
Διαλειτουργικότητα	Πολύ περιορισμένη	Περιορισμένη σε συμβατά πρωτόκολλα	Υψηλή με τυποποιημένα πρότυπα(π.χ. STANAG)
Ασφάλεια επικοινωνίας	Ελάχιστη	Μέτρια-Βασική κρυπτογράφηση	Πολύ υψηλή-End-to-end κρυπτογράφηση, ασφαλή πρωτόκολλα
Απαιτήσεις υποδομής	Απλή	Μέτρια	Σύνθετη, πολυεπίπεδη
Ευελιξία	Σχεδόν Μηδενική	Περιορισμένη	Πολύ υψηλή-Προσαρμογή μέσω λογισμικού

Ο συγκριτικός Πίνακας 1 συνοψίζει την τεχνολογική μετάβαση από τα παραδοσιακά αναλογικά συστήματα, στα ψηφιακά και τελικά στα σύγχρονα δικτυοκεντρικά συστήματα επικοινωνιών, επισημαίνοντας τις διαφορές τους ως προς την απόδοση, την ασφάλεια και την ευελιξία.

2.3 Θεμελιώδεις απαιτήσεις : ασφάλεια, αξιοπιστία, ευελιξία

Οι στρατιωτικές επικοινωνίες δεν είναι απλώς μια τεχνική υποδομή. Είναι μία κρίσιμη ικανότητα που στηρίζει κάθε επίπεδο διοίκησης και επιχειρησιακής δράσης- από τον απλό στρατιώτη μέχρι το ανώτατο επίπεδο. Για να μπορέσουν να ανταποκριθούν στις απαιτήσεις του σύγχρονου και μελλοντικού πεδίου μάχης, οι στρατιωτικές τηλεπικοινωνίες πρέπει να βασίζονται σε ένα σύνολο

θεμελιωδών αρχών και αυστηρών τεχνικών απαιτήσεων. Αυτές οι αρχές δεν διαμορφώνονται τυχαία είναι προϊόν εμπειρίας, επιχειρησιακών δοκιμών και σκληρής πραγματικότητας.

2.3.1 Ασφάλεια και το θεμέλιο της κάθε μετάδοσης

Η ασφάλεια αποτελεί αδιαπραγμάτευτη προτεραιότητα στις στρατιωτικές επικοινωνίες. Η υποκλοπή ή παραποίηση κρίσιμων δεδομένων μπορεί να οδηγήσει σε σοβαρές επιχειρησιακές αποτυχίες [11]. Για τον λόγο αυτό, εφαρμόζονται προηγμένα συστήματα κρυπτογράφησης, όπως το Advanced Encryption Standard(AES) , που προσφέρουν προστασία επιπέδου έως και 256 bit [12]. Η ασφάλεια, όμως, δεν περιορίζεται μόνο στην κρυπτογράφηση του περιεχομένου. Επεκτείνεται και στην προστασία της ταυτότητας των χρηστών, στην ανθεκτικότητα σε ηλεκτρονικές επιθέσεις (π.χ. jamming, spoofing) και στην ακεραιότητα της πληροφορίας κατά την μετάδοση [13]. Σε ένα περιβάλλον που χαρακτηρίζεται από την αυξανόμενη σημασία του ηλεκτρονικού πολέμου, η ασφαλής επικοινωνία αποτελεί προϋπόθεση για κάθε είδους επιχειρησιακή ενέργεια [14].

Πολλά σύγχρονα τακτικά συστήματα, όπως το Joint Tactical Radio System(JTRS), ενσωματώνουν κρυπτογράφηση πολλαπλών επιπέδων, authentication μηχανισμούς και δυνατότητες secure over-the-air updates, ώστε να προστατεύεται το δίκτυο σε όλη τη διάρκεια μιας αποστολής , ακόμη και όταν κινείται [15].Επιπλέον, η χρήση τεχνολογιών frequency hopping και direct-sequence spread spectrum, όπως εφαρμόζονται στα πρότυπα STANAG, καθιστούν δυσκολότερη την ανίχνευση και υποκλοπή των σημάτων, ενώ αυξάνουν την αντοχή απέναντι σε σκόπιμες παρεμβολές [13], [12].

Η προστασία της ακεραιότητας και της εμπιστευτικότητας των επικοινωνιών ενισχύεται από την υιοθέτηση προηγμένων μηχανισμών διαχείρισης κλειδιών(key management), με δυνατότητα δυναμικής ανανέωσης και ακύρωσης σε πραγματικό χρόνο, ώστε να αποτρέπεται η εκμετάλλευση παραβιασμένων κλειδιών [12]. Επίσης, η υλοποίηση πολυεπίπεδων Intrusion Detection Systems(IDS) σε κρίσιμα δίκτυα επιτρέπει τον εντοπισμό ασυνήθιστης δραστηριότητας και την άμεση απομόνωση πιθανών επιθέσεων [14].

Τέλος, η ασφάλεια δεν είναι μόνο τεχνολογικό ζήτημα αλλά και οργανωτικό. Οι στρατιωτικές δυνάμεις εφαρμόζουν αυστηρές πολιτικές πρόσβασης, πολυπαραγοντική ταυτοποίηση(muti-factor authentication) και συνεχή εκπαίδευση προσωπικού, ώστε να μειωθεί η πιθανότητα παραβιάσεων που προέρχονται από ανθρώπινα λάθη [13], [15].

2.3.2 Αξιοπιστία και διαθεσιμότητα

Η αξιοπιστία είναι εξίσου κρίσιμη. Στο πεδίο μάχης, δεν υπάρχει περιθώριο για διακοπές ή απώλειες σύνδεσης [1]. Τα στρατιωτικά δίκτυα πρέπει να λειτουργούν με ελάχιστο ποσοστό αστοχίας- συχνά με το στόχο το λεγόμενο “five-nines”(99.999% διαθεσιμότητα) [2]. Για να επιτευχθεί αυτό, σχεδιάζονται με ενσωματωμένους μηχανισμούς εφεδρείας(redundancy), δυνατότητες

επαναδρομολόγησης(rerouting) και αυτόματης αποκατάστασης(self-healing). Παράλληλα, οι επικοινωνίες πρέπει να λειτουργούν ακόμη και σε συνθήκες φυσικών καταστροφών, παρεμβολών ή όταν ο εξοπλισμός υφίσταται ζημιές ή απώλειες [13].

Ιδιαίτερη σημασία έχει η ανοχή σε σφάλματα(fault tolerance) μέσω χρήσης πολλαπλών εφεδρικών διαδρομών και εναλλακτικών μέσων μετάδοσης. Για παράδειγμα, σε περιβάλλοντα με περιορισμένη επίγεια υποδομή, τα δίκτυα βασισμένα σε δορυφορικές επικοινωνίες(SATCOM) λειτουργούν ως εφεδρικά κανάλια σε περιοχές χωρίς επίγεια υποδομή, προσφέροντας διαθεσιμότητα ακόμη και σε αποστολές μεγάλης ακτίνας ή διεθνούς συνεργασίας [16].

Η αξιοπιστία δεν αφορά μόνο τη διαθεσιμότητα του δικτύου, αλλά και την ποιότητα της μετάδοσης(Quality of Service-QoS). Στρατιωτικά συστήματα, όπως το Joint Tactical Radio Systems(JTRS), ενσωματώνουν μηχανισμούς συνεχούς παρακολούθησης της απόδοσης, ώστε να εντοπίζονται και να διορθώνονται έγκαιρα προβλήματα που ενδέχεται να επηρεάσουν κρίσιμες επικοινωνίες [17].

Επιπλέον, η χρήση Software Defined Networking(SDN) σε στρατιωτικές εφαρμογές επιτρέπει την κεντρική και δυναμική διαχείριση των πόρων, μειώνοντας τον χρόνο απόκρισης σε περιστατικά βλάβης και αυξάνοντας την ανθεκτικότητα του δικτύου [13]. Η δυνατότητα αυτή είναι καθοριστική σε επιχειρήσεις υψηλής έντασης, όπου η επικοινωνία πρέπει να παραμένει αξιόπιστη παρά τις συνεχιζόμενες απειλές ή φυσικές καταστροφές.

2.3.3 Ευελιξία και διαλειτουργικότητα

Το σύγχρονο επιχειρησιακό περιβάλλον είναι δυναμικό και απρόβλεπτο. Οι δυνάμεις μετακινούνται συνεχώς, επιχειρούν σε άγνωστα ή απομακρυσμένα σημεία και καλούνται να συνεργαστούν με συμμαχικές ή πολυεθνικές μονάδες. Αυτό απαιτεί δίκτυα που να είναι ευέλικτα, προσαρμόσιμα και να υποστηρίζουν την λεγόμενη διαλειτουργικότητα [1]. Δηλαδή να μπορούν να διασυνδέονται με διαφορετικά πρωτόκολλα, εξοπλισμό και δομές, χωρίς να απαιτείται πλήρης επανασχεδίαση κάθε φορά. Η ευελιξία αφορά την ικανότητα ενός δικτύου να προσαρμόζεται γρήγορα σε μεταβαλλόμενες συνθήκες, είτε αυτές αφορούν γεωγραφικές μετακινήσεις, είτε αλλαγές στο φάσμα επικοινωνίας, είτε διαφοροποιήσεις στον τύπο και στον όγκο των δεδομένων που μετακινούνται. Για την επίτευξη αυτής της ικανότητας, αξιοποιούνται τεχνολογίες όπως τα Software Defined Radios(SDR), που επιτρέπουν την αλλαγή των χρησιμοποιούμενων waveforms και πρωτοκόλλων χωρίς την ανάγκη αντικατάστασης υλικού [17].

Η διαλειτουργικότητα αναφέρεται στη δυνατότητα των συστημάτων να συνεργάζονται απρόσκοπτα, ανεξάρτητα από τον κατασκευαστή ή το πρωτόκολλο λειτουργίας. Στρατιωτικά πρότυπα όπως το Link-16 έχουν σχεδιαστεί ώστε να επιτρέπουν σε αεροσκάφη, πλοία και επίγειες μονάδες

διαφορετικών χωρών να ανταλλάσσουν δεδομένα σε πραγματικό χρόνο, διατηρώντας παράλληλα υψηλά επίπεδα ασφαλείας [18].Το Link-16 χρησιμοποιεί κρυπτογράφηση, συγχρονισμό χρόνου και τεχνικές frequency hopping για να εξασφαλίζει αδιάλειπτη και προστατευμένη επικοινωνία ακόμη και σε συνθήκες ηλεκτρονικού πολέμου. Ένα χαρακτηριστικό παράδειγμα αρχιτεκτονικής Link-16 παρουσιάζεται στο Σχήμα 4, όπου φαίνεται η τακτική διαλειτουργική επικοινωνία μεταξύ εναέριων, επίγειων και ναυτικών μονάδων.

Η τεχνολογία Software Defined Networking(SDN) προσφέρει ένα επιπλέον επίπεδο ευελιξίας, επιτρέποντας την κεντρική διαχείριση του δικτύου και την δυναμική ανακατανομή των πόρων ανάλογα με τις επιχειρησιακές ανάγκες [13].Σε πολυεθνικές επιχειρήσεις, η χρήση τυποποιημένων διεπαφών και πρωτοκόλλων διευκολύνει τη διασύνδεση διαφορετικών δικτύων χωρίς εκτεταμένες τροποποιήσεις, μειώνοντας τον χρόνο ανάπτυξης και αυξάνοντας την αποδοτικότητα.

Η ευελιξία και η διαλειτουργικότητα δεν αποτελούν πολυτέλεια, αλλά βασική απαίτηση για να μπορούν οι δυνάμεις να ανταποκρίνονται αποτελεσματικά σε ρευστές και απρόβλεπτες καταστάσεις. Η έλλειψή τους μπορεί να οδηγήσει σε καθυστερήσεις, απώλεια κρίσιμων πληροφοριών και επιχειρησιακή αποτυχία.



Σχήμα 4-Παράδειγμα δικτύου Link-16 για τακτική διαλειτουργική επικοινωνία μεταξύ εναέριων, επίγειων και αντιαεροπορικών μονάδων(L3Harris Technologies, "Link-16 Tactical Data Links").

Οι παρακάτω τύποι στρατιωτικών επικοινωνιών αναδεικνύουν την ανάγκη για δικτυακή προσαρμοστικότητα ανάλογα με το περιβάλλον, το επίπεδο της αποστολής και τις γεωγραφικές απαιτήσεις. Το εύρος των εφαρμογών- από τις επίγειες και ναυτικές μονάδες μέχρι διαλειτουργικά δίκτυα συμμαχικών δυνάμεων- αποτυπώνεται συγκεντρωτικά στον Πίνακα 2.

Πίνακας 2-Τύποι στρατιωτικών επικοινωνιών και βασικές παράμετροι

Παράμετρος	Τύπος

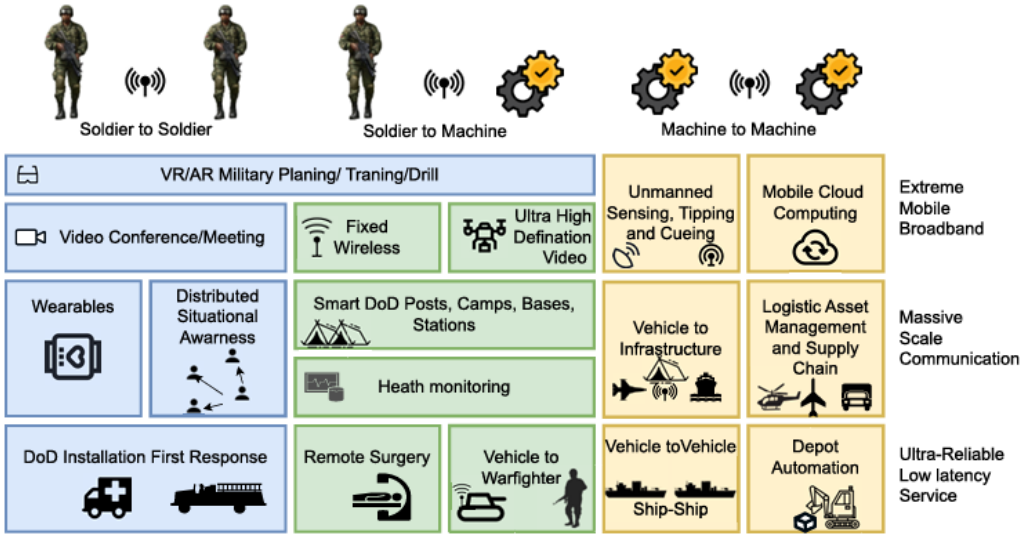
Επικοινωνία	Εναέριες, Υποβρύχιες, Επίγειες, Αέρος-εδάφους, Επιβιβασμένες σε πλοία
Συνιστώσα	Συστήματα SATCOM, Συστήματα Ασφαλείας. Ραδιοσυστήματα, Συστήματα διαχείρισης επικοινωνιών
Εφαρμογή	Επιχειρήσεις ρουτίνας, Διοίκηση και Έλεγχος(C2), Επίγνωση κατάστασης
Χρήστες	Χερσαίες δυνάμεις, Αεροπορία και Ναυτικές δυνάμεις
Γεωγραφία	Βόρεια Αμερική, Νότια Αμερική, Ευρώπη, Ασία-Ειρηνικός, Μέση Ανατολή και Αφρική

2.3.4 Χαμηλή καθυστέρηση και ταχύτητα

Η χρονική καθυστέρηση στη μετάδοση πληροφορίας μπορεί να είναι κρίσιμη σε επιχειρησιακά περιβάλλοντα όπου ακόμη και χιλιοστά του δευτερολέπτου μπορεί να καθορίσουν την επιτυχία ή αποτυχία μιας αποστολής. Ειδικά όταν μιλάμε για συντονισμό πυρών, τηλεχειριζόμενα συστήματα ή επιχειρήσεις με UAVs, η επιθυμητή καθυστέρηση(latency) πρέπει να είναι όσο το δυνατόν πιο κοντά στο μηδέν. Σε πολλές περιπτώσεις, ο στόχος είναι η καθυστέρηση να βρίσκεται κάτω από 1 ms. Η ικανότητα αυτή καθιστά δυνατή τη λήψη αποφάσεων σχεδόν σε πραγματικό χρόνο και προσφέρει συγκριτικό πλεονέκτημα στο τακτικό επίπεδο [12].

Οι τεχνολογίες 5G και 6G προσφέρουν το πλαίσιο για Ultra-Reliable Low Latency Communications(URLLC), επιτυγχάνοντας τόσο υψηλές ταχύτητες όσο και εξαιρετικά χαμηλό latency ακόμη και σε κινητά ή τακτικά δίκτυα. Σε στρατιωτικά περιβάλλοντα, η URLLC υλοποιείται σε συνδυασμό με edge computing και τοπικούς κόμβους προώθησης(forward-deployed nodes), μειώνοντας την απόσταση που πρέπει να διανύσει το σήμα και επομένως το χρόνο απόκρισης(βλέπε Σχήμα 5) [19], [3].

Στα tactical MANETs, η ελαχιστοποίηση της καθυστέρησης επιτυγχάνεται με τεχνικές βελτιστοποίησης δρομολόγησης(routing optimization) και προσαρμογής του φάσματος μετάδοσης στις επικρατούσες συνθήκες(adaptive spectrum use). Επίσης, η ενσωμάτωση Software-Defined Networking(SDN) επιτρέπει την κεντρική διαχείριση των διαδρομών διασφαλίζοντας ότι τα πιο σημαντικά δεδομένα μεταδίδονται χωρίς καθυστέρηση [20].



Σχήμα 5 - Στρατιωτικά σενάρια χρήσης 5G με έμφαση σε εφαρμογές χαμηλής καθυστέρησης και υψηλής αξιοπιστίας [12]

2.3.5 Ιεράρχηση και διαχείριση πόρων

Σε στρατιωτικά δίκτυα, κάθε μετάδοση δεν έχει την ίδια βαρύτητα. Ένα τακτικό μήνυμα που αφορά εμπλοκή σε πραγματικό χρόνο πρέπει να έχει την προτεραιότητα σε σχέση με διοικητικές πληροφορίες ή ενημερώσεις ρουτίνας. Η διαχείριση αυτής της ιεράρχησης επιτυγχάνεται μέσω μηχανισμών Quality of Service(QoS), όπου τα πακέτα δεδομένων επισημαίνονται με επίπεδα προτεραιότητας και δρομολογούνται αναλόγως [1], [19].

Η τεχνική υλοποίηση περιλαμβάνει traffic classification, priority queuing και bandwidth reservation για κρίσιμες εφαρμογές. Σε τακτικά δίκτυα ad hoc (MANETs), όπου οι συνθήκες και η διαθέσιμη χωρητικότητα μεταβάλλονται συνεχώς, η ιεράρχηση βασίζεται σε δυναμική κατανομή πόρων(dynamic resource allocation) και προσαρμοστική χρήση φάσματος(adaptive spectrum allocation) [11].

Σε μια αποστολή SAR μετά από φυσική καταστροφή, το δίκτυο διαχειρίζεται ταυτόχρονα δεδομένα από UAVs που σαρώνουν την περιοχή, επικοινωνίες ομάδων εδάφους και διοικητικές ενημερώσεις. Οι εικόνες και τα σήματα θέσης που μεταδίδουν τα UAVs χαρακτηρίζονται ως “mission-critical” και αποκτούν την υψηλότερη προτεραιότητα, ώστε να φτάσουν άμεσα στο κέντρο επιχειρήσεων για ανάλυση. Αντίθετα, η αναφορά κατάστασης αποθήκης υλικού λαμβάνει χαμηλότερη προτεραιότητα, ώστε να μην επιβαρύνει την ήδη περιορισμένη χωρητικότητα του δικτύου. Μέσω των μηχανισμών QoS, το σύστημα εξασφαλίζει ότι οι κρίσιμες πληροφορίες διακινούνται με το μικρότερο δυνατό latency, διασφαλίζοντας την αποτελεσματικότητα της αποστολής [20].

2.3.6 Ανθεκτικότητα στο περιβάλλον

Οι στρατιωτικές επιχειρήσεις εκτελούνται σε περιβάλλοντα που είναι αντίξοα για κάθε τεχνολογία. Έρημοι, δάση, βουνά, υποθαλάσσιοι χώροι ή πυκνοκατοικημένες περιοχές απαιτούν απόλυτη ανθεκτικότητα του εξοπλισμού και του δικτύου [21].

Η σχεδίαση των στρατιωτικών τηλεπικοινωνιών περιλαμβάνει προστασία από κραδασμούς και δονήσεις, αντοχή σε ηλεκτρομαγνητικές παρεμβολές(EMI/EMC shielding) και λειτουργία σε ευρύ θερμοκρασιακό εύρος, σύμφωνα με στρατιωτικά πρότυπα όπως το MIL-STD-810G [22]. Επιπλέον, απαιτείται στεγανότητα και προστασία από σκόνη και υγρασία(IP ratings) για την αποφυγή βλαβών σε κρίσιμα εξαρτήματα.

Η ανθεκτικότητα δεν αφορά μόνο φυσικές συνθήκες. Τα δίκτυα πρέπει να συνεχίζουν να λειτουργούν ακόμη και σε συνθήκες ηλεκτρονικού πολέμου, όπου απειλές όπως το jamming και το spoofing μπορούν να διαταράξουν ή να παραποιήσουν τη ροή πληροφοριών. Τεχνικές όπως frequency hopping spread spectrum(FHSS), direct sequence spread spectrum(DSSS) και adaptive beamforming χρησιμοποιούνται για την αποφυγή και την εξουδετέρωση παρεμβολών [23].

Επιπρόσθετα, η ανθεκτικότητα επεκτείνεται και στην κυβερνοασσφάλεια. Σε περιπτώσεις αποκοπής από τα δίκτυα κορμού, η χρήση αποκεντρωμένων μηχανισμών ελέγχου και self-healing networking εξασφαλίζει ότι οι επικοινωνίες παραμένουν διαθέσιμες και ασφαλείς, ακόμη και υπό συνθήκες κυβερνοεπιθέσεων [20].

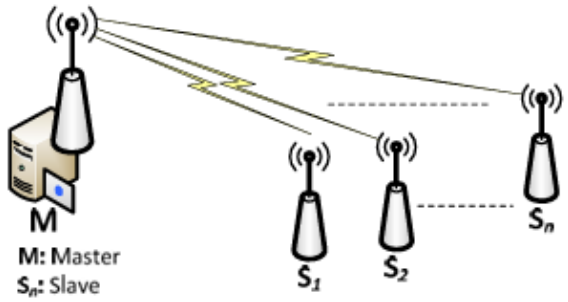
Η ανθεκτικότητα στο περιβάλλον είναι επομένως ένα πολυδιάστατο χαρακτηριστικό που συνδυάζει φυσική προστασία, αντοχή και ηλεκτρονικές απειλές και διασφάλιση συνεχούς λειτουργίας, καθιστώντας το θεμέλιο για την αξιοπιστία των στρατιωτικών επικοινωνιών στο πεδίο.

2.3.7 Ενεργειακή αυτονομία και αποδοτικότητα

Ένα σημαντικό αλλά συχνά παραγνωρισμένο στοιχείο είναι η ενεργειακή αποδοτικότητα των συστημάτων. Επειδή πολλές αποστολές εκτελούνται σε περιοχές χωρίς σταθερή τροφοδοσία, τα μέσα επικοινωνίας (ειδικά UAVs ή φορητοί ασύρματοι) πρέπει να λειτουργούν με περιορισμένη ενέργεια, χωρία να χάνουν απόδοση [24]. Οι σχεδιαστικές προσεγγίσεις επικεντρώνονται σε ελαφρύ εξοπλισμό, χαμηλή κατανάλωση και αυτονομία, που να εξασφαλίζει συνεχή επιχειρησιακή ικανότητα για αρκετές ώρες ή μέρες.

Η ενεργειακή αποδοτικότητα στα στρατιωτικά δίκτυα δεν αφορά μόνο τη βελτίωση της κατανάλωσης σε επίπεδο συσκευής, αλλά και τη δομή του ίδιου του δικτύου. Η αρχιτεκτονική τύπου master-slave, όπως φαίνεται στο Σχήμα 6 επιτρέπει τους κόμβους-αισθητήρες(slaves) να λειτουργούν με χαμηλή ισχύ, μεταδίδοντας μόνο βασικά δεδομένα προς τον master κόμβο, ο οποίος αναλαμβάνει την επεξεργασία και την προώθησή τους. Με αυτόν τον τρόπο μειώνεται σημαντικά η κατανάλωση

ενέργειας στους επιμέρους κόμβους και αυξάνεται η συνολική διάρκεια ζωής του δικτύου, στοιχείο κρίσιμο για επιχειρήσεις μεγάλης διάρκειας και σε απομονωμένα πεδία μάχης [25].



Σχήμα 6 - Δομή πεδίου αισθητήρων με master-slave αρχιτεκτονική[25]

Οι σύγχρονες τεχνικές που εφαρμόζονται σε τέτοιες αρχιτεκτονικές περιλαμβάνουν :

- Dynamic Power Control : Ρύθμιση της ισχύος εκπομπής ανάλογα με την απόσταση του παραλήπτη, ώστε να μειώνεται η κατανάλωση ενέργειας.
- Duty Cycling : Ενεργοποίηση και απενεργοποίηση υποσυστημάτων ανάλογα με τις επιχειρησιακές ανάγκες.
- Energy Harvesting : Αξιοποίηση ηλιακής ενέργειας ή δονήσεων περιβάλλοντος για την τροφοδοσία μικρών αισθητήρων στο πλαίσιο του Internet of Military Things [25].

Στα UAVs, για παράδειγμα, η βελτιστοποίηση της κατανάλωσης ενέργειας επιτρέπει μεγαλύτερη διάρκεια πτήσης και παρακολούθηση ευρύτερων περιοχών χωρίς ανεφοδιασμό. Σε φορητούς ασυρμάτους, η χρήση energy-efficient πρωτοκόλλων και έξυπνων αλγορίθμων δρομολόγησης εξασφαλίζει επικοινωνίες μεγάλης διάρκειας, κρίσιμες σε αποκομμένα περιβάλλοντα [26].

Η ενεργειακή αποδοτικότητα δεν αποτελεί μόνο ζήτημα επιβίωσης για το ίδιο το σύστημα, αλλά και στρατηγικό πλεονέκτημα όπου μειώνει την ανάγκη ανεφοδιασμού, περιορίζει την εξάρτηση από ευάλωτες αλυσίδες εφοδιασμού και ενισχύει την επιχειρησιακή ευελιξία. Στο πλαίσιο του μελλοντικού πεδίου μάχης, όπου αναμένονται δίκτυα χιλιάδων αισθητήρων και συσκευών IoMT, η ενεργειακή αποδοτικότητα θα αποτελέσει βασική προϋπόθεση για τη διατηρήσιμη λειτουργία και την ανθεκτικότητα των στρατιωτικών επικοινωνιών [24].

2.3.8 Επεκτασιμότητα και προσαρμοστικότητα

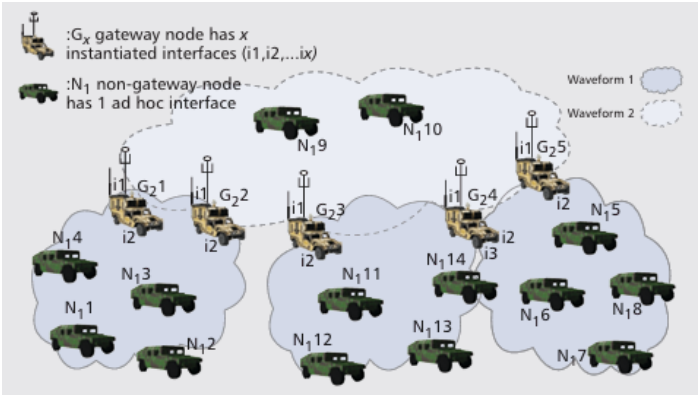
Ένα σύγχρονο στρατιωτικό δίκτυο δεν πρέπει να είναι στατικό. Καθώς μια αποστολή εξελίσσεται, μπορεί να απαιτείται η προσθήκη νέων κόμβων, υποσυστημάτων ή λειτουργιών χωρίς να διαταράσσεται η υφιστάμενη λειτουργία. Η επεκτασιμότητα αφορά την ικανότητα ενός δικτύου να

αυξάνει τις δυνατότητές του, σε αριθμό χρηστών, όγκο δεδομένων ή γεωγραφική κάλυψη χωρίς απώλεια απόδοσης. Από την άλλη, η προσαρμοστικότητα αναφέρεται στην ικανότητα του δικτύου να τροποποιεί δυναμικά τη λειτουργία του ανάλογα με τις επιχειρησιακές απαιτήσεις [25].

Στην πράξη, αυτό σημαίνει ότι τα στρατιωτικά δίκτυα πρέπει να έχουν modular αρχιτεκτονική, όπου κάθε υποσύστημα μπορεί να ενσωματωθεί ή να αντικατασταθεί με ελάχιστο κόστος και καθυστέρηση. Οι τεχνολογίες Software-Defined Networking(SDN) και Network Function Virtualization(NFV) έχουν καθοριστικό ρόλο σε αυτή τη μετάβαση, καθώς επιτρέπουν την ευέλικτη ανακατανομή πόρων και την εισαγωγή νέων υπηρεσιών χωρίς αλλαγές στον φυσικό εξοπλισμό [14].

Ένα χαρακτηριστικό παράδειγμα προσαρμοστικής αρχιτεκτονικής είναι τα γνωστικά τακτικά δίκτυα(Cognitive Tactical Networks). Σε αυτά, η επικοινωνιακή δομή διαθέτει μηχανισμούς αντίληψης του περιβάλλοντος, λήψης αποφάσεων και μάθησης, ώστε να μπορεί να βελτιστοποιεί δυναμικά την κατανομή πόρων και τα πρωτόκολλα δρομολόγησης. Έτσι, επιτυγχάνεται ταυτόχρονα επεκτασιμότητα, αφού το δίκτυο μπορεί να υποστηρίξει περισσότερους κόμβους χωρίς ανασχεδιασμό και προσαρμοστικότητα, αφού η λειτουργία του προσαρμόζεται σε πραγματικό χρόνο για επιχειρησιακές συνθήκες.

Το Σχήμα 7 παρουσιάζει ένα παράδειγμα γνωσιακού τακτικού δικτύου με κόμβους gateway και non-gateway, που αξιοποιούν πολλαπλά waveforms για τη διατήρηση αξιόπιστης επικοινωνίας και την υποστήριξη επεκτασιμότητας και προσαρμοστικότητας [27].



Σχήμα 7 - Παράδειγμα γνωσιακού τακτικού δικτύου με gateway και non-gateway κόμβους[27]

Η αυξανόμενη χρήση του Internet of Military Things(IoMT) ενισχύει περαιτέρω την ανάγκη επεκτασιμότητας. Δίκτυα με εκατοντάδες ή χιλιάδες αισθητήρες και UAVs απαιτούν πρωτόκολλα που να μπορούν να διαχειριστούν ραγδαία αύξηση της κυκλοφορίας, χωρίς να επηρεάζεται η απόδοση [12]. Η προσαρμοστικότητα εξασφαλίζεται μέσα από cognitive tactical networks, τα οποία αξιοποιούν μηχανισμούς μάθησης για να βελτιστοποιούν δυναμικά το routing, τη χρήση συχνοτήτων και την κατανομή ισχύος [11].

Η επεκτασιμότητα και η προσαρμοστικότητα δεν είναι πολυτέλεια, αλλά επιχειρησιακή απαίτηση. Χωρίς αυτές, ένα δίκτυο μπορεί να αποτύχει να ανταποκριθεί σε μεταβαλλόμενες συνθήκες ή σε ξαφνικές αυξήσεις φορτίου, με άμεσο αντίκτυπο στην αποτελεσματικότητα των επιχειρήσεων.

2.4 Διαφορές Στρατιωτικών και Εμπορικών Δικτύων

2.4.1 Αρχιτεκτονική

Στα εμπορικά δίκτυα(3G/4G/5G), ο σχεδιασμός είναι κατεξοχήν κεντροβαρής, δηλαδή οι χρήστες συνδέονται με σταθερούς σταθμούς βάσης(BS), οι οποίοι ενορχηστρώνονται από ελεγκτές(BSC) και τροφοδοτούνται από έναν πυρήνα (core network) μέσω σαφώς ορισμένων διεπαφών και προτύπων(π.χ. 3GPP, ανοιχτά ICDs). Το μοντέλο αυτό, με καθαρές οντότητες και διεπαφές, ευνοεί την τυποποίηση, τον ανταγωνισμό προμηθευτών και την ταχεία και οικονομική κλιμάκωση υπηρεσιών [2].

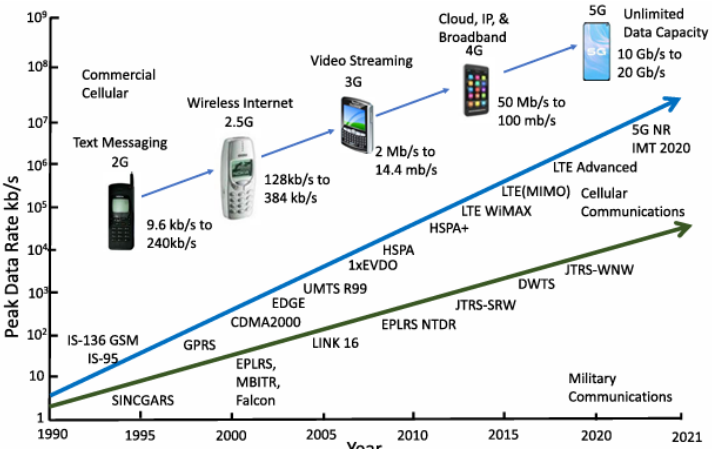
Αντιθέτως, τα στρατιωτικά δίκτυα, είναι κατανεμημένα, με έμφαση στη δυνατότητα αυτό-οργάνωσης με ιεραρχικά «στρώματα» από MANETs(π.χ. SRW για στρατιώτη/αισθητήρες, WNW για οχήματα/ευρύτερη συνδεσιμότητα) και επιλεγμένους κόμβους πολλαπλών διεπαφών που λειτουργούν ως πύλες μεταξύ υποδικτύων. Το «τακτικό core» μπορεί να είναι κινητό/μικτό (π.χ. WIN-T), να αξιοποιεί δορυφορικές/μικροκυματικές ζεύξεις και να υποστηρίζει επικοινωνίες OTM [2].

Η αρχιτεκτονική των τακτικών κόμβων υπακούει σε αυστηρές απαιτήσεις ασφάλειας(π.χ. HAIPE, red/black separation), γεγονός που επηρεάζει την οργάνωση των επιπέδων IP, τη διαχείριση κλειδιών και την ευχέρεια περιαγωγής/επανένταξης σε νέα υποδίκτυα. Αυτοί οι περιορισμοί διαφοροποιούν ουσιαστικά την αρχιτεκτονική από τα εμπορικά δίκτυα, όπου η ασφάλεια δεν επιβάλλει τόσο σκληρό λειτουργικό διαχωρισμό [2].

Παράλληλα, νεότερες αρχές όπως SDN/NFV εξετάζονται ως μέσα επαναπρογραμματιζόμενου ελέγχου και ταχύτερης αποκατάστασης/προσαρμογής σε στρατιωτικά περιβάλλοντα με πρόκληση όμως την ανθεκτικότητα του control plane επάνω από ασθενείς/ασταθείς ασύρματες ζεύξεις και την ανάγκη διασύνδεσης πολλαπλών εθνικών domains [27].

Τέλος, ακόμη και όταν αξιοποιούνται εμπορικές τεχνολογίες 5G/5GB, οι στόχοι και τα συμφραζόμενα αποκλίνουν, τα εμπορικά δίκτυα στοχεύουν σε υψηλές ταχύτητες/χαμηλή καθυστέρηση για αστικές χρήσης, ενώ τα στρατιωτικά πρέπει να λειτουργούν σε δυναμικά και εχθρικά περιβάλλοντα, με προτεραιότητες ανθεκτικότητας, ασφάλειας και διαλειτουργικότητας συμμαχικών δυνάμεων [12]. Οι διαφορές αυτές αποτυπώνονται στο Σχήμα 8, όπου παρουσιάζονται συγκριτικά η εξέλιξη των ρυθμών μετάδοσης στα εμπορικά και στα στρατιωτικά δίκτυα, αναδεικνύοντας την

ταχύτερη τεχνολογική πρόοδο του εμπορικού τομέα σε σχέση με την πιο συντηρητική, αλλά ιδιαίτερα ασφαλή, προσέγγιση των στρατιωτικών υποδομών.



Σχήμα 8 - Συγκριτική εξέλιξη ρυθμών μετάδοσης σε εμπορικά και στρατιωτικά δίκτυα

2.4.2 Ευελιξία και Διαλειτουργικότητα

Στον εμπορικό τομέα, η έννοια της ευελιξίας και της διαλειτουργικότητας σχετίζεται κυρίως με τη συμμόρφωση σε διεθνή πρότυπα , όπως το LTE, Wi-Fi καιBluetooth που εξασφαλίζουν ότι οι συσκευές διαφορετικών κατασκευαστών μπορούν να λειτουργούν απρόσκοπτα σε παγκόσμια κλίμακα. Η στρατηγική αυτή επιτρέπει τη μαζική παραγωγή, την ελαχιστοποίηση κόστους και την διαρκή αναβάθμιση των υπηρεσιών σύμφωνα με τις ανάγκες της αγοράς [2].

Αντίθετα, στα στρατιωτικά δίκτυα, η διαλειτουργικότητα έχει πιο σύνθετη και κρίσιμη σημασία. Αφορά όχι μόνο την τεχνική συμβατότητα συστημάτων, αλλά και τη συνεργασία πολυεθνικών δυνάμεων σε δυναμικά και απρόβλεπτα επιχειρησιακά περιβάλλοντα. Σε αποστολές όπου συμμετέχουν δυνάμεις του NATO ή άλλων συμμαχιών, απαιτείται η δυνατότητα σύνδεσης ετερογενών υποδομών, διαφορετικών πρωτοκόλλων και κατασκευαστών, χωρίς να θυσιάζεται η ασφάλεια ή η αποδοτικότητα [9]. Χαρακτηριστικό παράδειγμα αποτελεί το πρόγραμμα Joint Tactical Radio System(JTRS), το οποίο αναπτύχθηκε ώστε να παρέχει Software Defined Radios(SDRs) με δυνατότητα προσαρμογής σε πολλαπλά κύματα επικοινωνίας και μορφές κρυπτογράφησης μέσα από ενιαίο εξοπλισμό [14]. Η αρχιτεκτονικών αυτών των SDRs, βασισμένη σε modular σχεδιασμό που επιτρέπει την εύκολη προσαρμογή σε διαφορετικά πρότυπα και αποστολές, παρουσιάζεται στο Σχήμα 9.

Περαιτέρω, το NATO έχει θεσπίσει την πρωτοβουλία Federated Mission Networking(FMN), που καθορίζει προδιαγραφές για την επίτευξη διαλειτουργικότητας μεταξύ των συμμαχικών δυνάμεων. Μέσω του FMN, επιτυγχάνεται η γρήγορη ενσωμάτωση διαφορετικών εθνικών δικτύων σε κοινές επιχειρήσεις, μειώνοντας τον χρόνο ανάπτυξης και αυξάνοντας την επιχειρησιακή ευελιξία [26].Οι

αρχές του Software Defined Networking(SDN) και του Network Function Virtualization(NFV), που ήδη δοκιμάζονται σε στρατιωτικά περιβάλλοντα , προσφέρουν δυνατότητες κεντρικού ελέγχου και δυναμικής ανακατανομής των διαθέσιμων πόρων, αυξάνοντας ακόμη περισσότερο τη διαλειτουργικότητα [27].

Η απουσία αυτών των χαρακτηριστικών μπορεί να οδηγήσει σε καθυστερήσεις, απώλειες κρίσιμων δεδομένων ή ακόμα και επιχειρησιακή αποτυχία. Γι' αυτόν τον λόγο, η ευελιξία και η διαλειτουργικότητα δεν αποτελούν προαιρετικά στοιχεία, αλλά βασικές επιχειρησιακές απαιτήσεις για τα στρατιωτικά δίκτυα.



Σχήμα 9 - Αρχιτεκτονική SDR με modular σχεδιασμό για υποστήριξη πολλαπλών πρωτοκόλλων επικοινωνίας [14]

ΚΕΦΑΛΑΙΟ 3

3 Σύγχρονες Τεχνολογίες Στρατιωτικών Δικτυών

Οι σύγχρονες τηλεπικοινωνίες έχουν εξελιχθεί ραγδαία τα τελευταία χρόνια, καθώς οι επιχειρησιακές απαιτήσεις αυξάνονται διαρκώς και τα παραδοσιακά μέσα δεν επαρκούν πλέον. Οι σύγχρονες στρατιωτικές αποστολές απαιτούν συνεχή συνδεσιμότητα, ασφαλή και αξιόπιστη μετάδοση μεγάλου όγκου δεδομένων και δυνατότητα λειτουργίας σε εχθρικά ή τεχνικά δύσκολα περιβάλλοντα [1], [14]. Σε αυτό το πλαίσιο, η ενσωμάτωση νέων τεχνολογιών είναι όχι μόνο επιθυμητή, αλλά απολύτως απαραίτητη. Το παρόν κεφάλαιο εξετάζει τις βασικές τεχνολογίες που χρησιμοποιούνται ή δοκιμάζονται σήμερα στις στρατιωτικές τηλεπικοινωνίες, όπως τα δίκτυα 5G [12], τα Software Defined Radios(SDRs) [28],τα MANETs [29], τα UAV-based communication nodes, τα γνωστικά δίκτυα και το Internet of Military Things(IoMT).

Μία από τις πιο συζητημένες τεχνολογίες των τελευταίων ετών είναι το 5G. Αν και πρόκειται για εξέλιξη του εμπορικού τομέα, η στρατιωτική αξιοποίηση του 5G φέρνει σημαντικές δυνατότητες στο προσκήνιο. Χαμηλή καθυστέρηση(latency < 1 ms), υψηλό bandwidth, δυναμικό slicing του δικτύου, υποστήριξη για μαζικά συνδεδεμένες συσκευές(massive MIMO), καθώς και βελτιωμένες δυνατότητες ασφάλειας. Όλα αυτά μεταφράζονται σε πρακτικά πλεονεκτήματα για το πεδίο :πιο γρήγορη επικοινωνία μεταξύ διοίκησης και μονάδων, δυνατότητα real-time video μετάδοσης από UAVs και υποστήριξη για augmented reality σε εκπαιδευτικά ή επιχειρησιακά σενάρια.

Ωστόσο, η υιοθέτηση του 5G σε στρατιωτικά περιβάλλοντα δεν είναι απλή υπόθεση. Η ανάγκη για λειτουργία σε δυναμικά και εχθρικά περιβάλλοντα,, η ανάγκη για απόλυτη ασφάλεια, αλλά και η απουσία σταθερής υποδομής, απαιτούν τροποποιήσεις. Στο πλαίσιο αυτό, αναπτύσσονται private 5G δίκτυα, προσαρμοσμένα στις απαιτήσεις του στρατεύματος. Ένα παράδειγμα είναι η δυνατότητα δημιουργίας προσωρινών 5G κόμβων σε αποστολές πεδίου, με χρήση αυτόνομων σταθμών ή ακόμη και UAVs, τα οποία λειτουργούν ως εναέριες μονάδες επικοινωνίας.

Μία άλλη κατηγορία τεχνολογιών με τεράστια εφαρμογή στον στρατό είναι τα Software Defined Radios(SDRs). Τα SDRs επιτρέπουν στο ίδιο υλικό (hardware) να υποστηρίζει πολλαπλά ραδιοκύματα και πρωτόκολλα, απλώς αλλάζοντας το λογισμικό του. Αυτό λύνει πολλά προβλήματα διαλειτουργικότητας, ειδικά όταν μονάδες διαφορετικών χωρών καλούνται να συνεργαστούν. Το SDR είναι ήδη ενσωματωμένο σε πολλές στρατιωτικές πλατφόρμες, όπως το πρόγραμμα JTRS(Joint Tactical Radio System), που επιχειρεί να ενώσει σε μια ενιαία λύση τακτικής επικοινωνίας ασυρμάτους διαφόρων τύπων και χρήσεων.

Ακόμα πιο κρίσιμα είναι τα δίκτυα MANETs(Mobile Ad Hoc Networks), τα οποία επιτρέπουν σε μονάδες να συνδέονται μεταξύ τους χωρίς την ύπαρξη προκαθορισμένης υποδομής. Κάθε κόμβος λειτουργεί ταυτόχρονα ως πομπός και αναμεταδότης, δημιουργώντας ένα δυναμικό, αυτό - οργανωμένο δίκτυο που προσαρμόζεται στο πεδίο. Σε συνδυασμό με UAVs ή επίγεια οχήματα, τα MANETs προσφέρουν μεγάλη ευελιξία και αποτελούν τη βάση για πολλές σύγχρονες στρατιωτικές εφαρμογές [30].

Η τεχνολογία των UAVs ως κόμβων επικοινωνίας προσφέρει τη δυνατότητα κάλυψης περιοχών όπου το έδαφος είναι δυσπρόσιτο ή επικίνδυνο. Σε συνθήκες όπως βουνά, αστικές μάχες ή επιχειρήσεις ερήμου, η χρήση UAVs ως relay nodes επιτρέπει τη διατήρηση της επικοινωνίας ακόμα και σε πλήρη απουσία δικτυακής υποδομής. Ένα UAV μπορεί να πετάξει πάνω από τις μονάδες και να λειτουργεί ως “ιπτάμενος αναμεταδότης”, είτε σε δίκτυο mesh είτε ως mobile hotspot.

Επιπλέον, αναπτύσσεται ραγδαία το λεγόμενο Internet of Military Things(IoMT), που βασίζεται στην ιδέα ότι κάθε κομμάτι του στρατιωτικού εξοπλισμού μπορεί να συνδεθεί και να στέλνει πληροφορίες σε πραγματικό χρόνο [22]. Συσκευές, στολές , αισθητήρες, οχήματα, ακόμη και πυρομαχικά, αποκτούν διασύνδεση και ενσωματώνονται σε ένα ενιαίο επιχειρησιακό δίκτυο. Το IoMT βελτιώνει την επίγνωση κατάστασης, τη λήψη αποφάσεων και την αναποτελεσματικότητα των μονάδων σε πραγματικό χρόνο. Κλασσικό παράδειγμα είναι οι αισθητήρες που τοποθετούνται σε στρατιώτες για την παρακολούθηση ζωτικών ενδείξεων, ή σε οχήματα για εντοπισμό βλαβών και αυτόματη αναφορά [11].

Τέλος, τα γνωστικά δίκτυα (Cognitive Tactical Networks) φέρνουν στο προσκήνιο την τεχνητή νοημοσύνη ως εργαλείο στις τηλεπικοινωνίες. Τα γνωστικά δίκτυα παρακολουθούν ενεργά το φάσμα, προσαρμόζουν συχνότητες, ανιχνεύουν παρεμβολές και επιλέγουν βέλτιστες διαδρομές για τα πακέτα δεδομένων, χωρίς ανθρώπινη παρέμβαση. Πρόκειται για μια τεχνολογία που αναπτύσσεται ακόμη, αλλά έχει ήδη αρχίσει να εφαρμόζεται σε προχωρημένα πειραματικά σενάρια. Η ενσωμάτωση των γνωστικών δυνατοτήτων στα SDRs θεωρείται το επόμενο μεγάλο βήμα στις τακτικές επικοινωνίες.

Όλες αυτές οι τεχνολογίες παρουσιάζουν ιδιαίτερα πλεονεκτήματα, αλλά και προκλήσεις. Η ένταξή τους στο ν στρατιωτικό σχεδιασμό απαιτεί στρατηγική σκέψη, τεχνική προσαρμογή και κυρίως αξιολόγηση σε ρεαλιστικές συνθήκες [1], [14]. Στο υπόλοιπο κεφάλαιο, θα γίνει αναλυτική παρουσίαση καθεμίας από τις παραπάνω τεχνολογίες, με στόχο να αναδειχθεί ο ρόλος τους, οι δυνατότητές τους και οι περιορισμοί που πρέπει να ληφθούν υπόψη στο σχεδιασμό ενός σύγχρονου στρατιωτικού δικτύου.

3.1 Τεχνολογία 5G στις στρατιωτικές επικοινωνίες

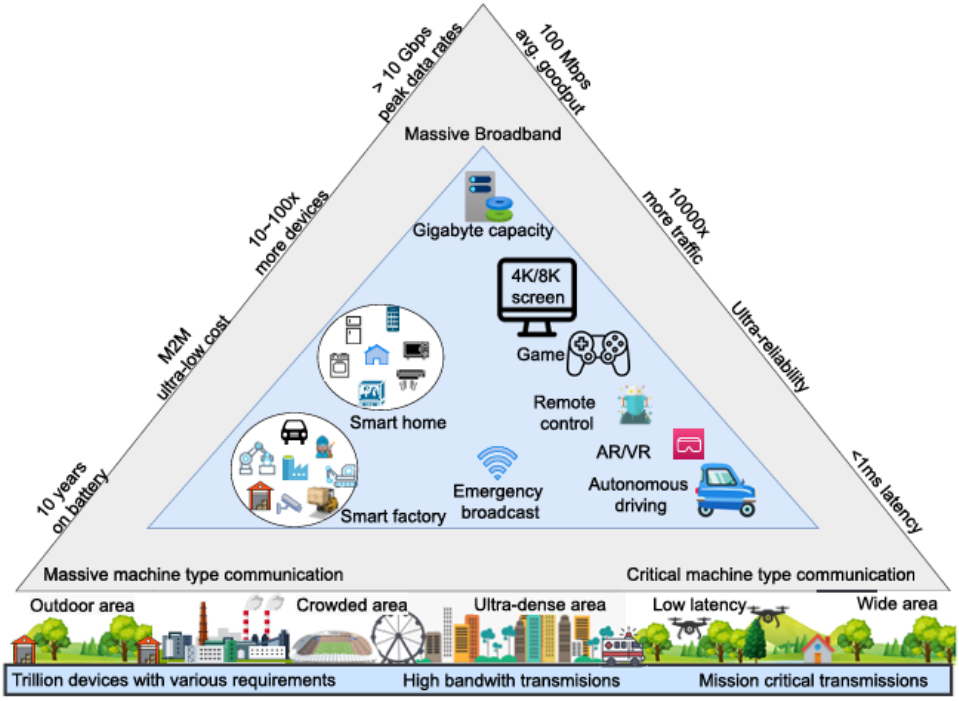
3.1.1 Βασικά χαρακτηριστικά του 5G

Η Πέμπτη γενιά κινητών επικοινωνιών(5G) δεν αποτελεί απλώς μια γραμμική εξέλιξη σε σχέση με τις προηγούμενες τεχνολογίες, αλλά μια ριζική αναδιάρθρωση του τρόπου με τον οποίο σχεδιάζονται και υλοποιούνται τα δίκτυα. Σε αντίθεση με το 4G, που είχε ως κύριο στόχο την αύξηση της ταχύτητας πρόσβασης στο διαδίκτυο για τους καταναλωτές, το 5G εισάγει μια εντελώς αρχιτεκτονική βασισμένη σε έννοιες όπως η εικονικοποίηση(virtualization), το δικτυακό τεμαχισμό (networking slicing), η υπολογιστική ισχύος στο άκρο του δικτύου(edge computing) και η δυναμική διαχείριση φάσματος. Αυτά τα χαρακτηριστικά το καθιστούν όχι απλώς μια εμπορική τεχνολογίας, αλλά ένα εργαλείο που μπορεί να αλλάξει ριζικά το δόγμα των στρατιωτικών επικοινωνιών [12], [31].

Κεντρικό στοιχείο του 5G είναι οι τρεις κατηγορίες υπηρεσιών που τυποποιήθηκαν από τον οργανισμό 3GPP και αποτυπώνονται σχηματικά στο γνωστό «τρίγωνο 5G” : η ενισχυμένη ευρυζωνικότητα(Enhanced Mobile Broadband-eMBB), οι εξαιρετικά αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης(Ultra-Reliable Low-Latency Communications-URLLC) και οι μαζικές επικοινωνίες μηχανών(Massive Machine-Type Communications-mMTC). Η πρώτη επικεντρώνεται σε ρυθμούς μετάδοσης που μπορούν να φτάσουν τα 20Gbps, γεγονός που επιτρέπει, για παράδειγμα, τη ζωντανή μετάδοση βίντεο υψηλής ανάλυσης από μη επανδρωμένα αεροσκάφη ή δορυφορικά συστήματα σε πραγματικό χρόνο. Η δεύτερη στοχεύει σε καθυστέρηση μικρότερη του 1 ms με αξιοπιστία που υπερβαίνει το 99.999%, προϋπόθεση απαραίτητα για τηλεχειρισμό οπλικών συστημάτων, συνεργασία αυτόνομων ρομποτικών πλατφορμών και συγχρονισμό πυρών στο πλαίσιο C4ISR. Η Τρίτη επιτρέπει τη διασύνδεση εκατοντάδων χιλιάδων αισθητήρων και συσκευών ανά τετραγωνικό χιλιόμετρο, κάτι που αποτελεί τη βάση για το Internet of Military Things(IoMT), όπου κάθε στρατιώτης, όχημα ή εξάρτημα μπορεί να συνδεθεί και να μεταδίδει δεδομένα στο δίκτυο [12], [32]. Οι τρεις αυτές κατηγορίες υπηρεσιών, που αποτελούν τον πυρήνα του οικοσυστήματος 5G, συνοψίζονται σχηματικά στο Σχήμα 10.

Η αρχιτεκτονική του 5G υλοποιείται μέσω του δικτύου πρόσβασης(Radio Access Network-RAN) και του νέου πυρήνα(5G Core-5GC).Σε αυτό το περιβάλλον, το massive Multiple Input Multiple Output(massive MIMO) και το beamforming αξιοποιούνται ώστε το σήμα να κατευθύνεται στοχευμένα προς τον χρήστη, μειώνοντας τις παρεμβολές και αυξάνοντας τόσο την ενεργειακή αποδοτικότητα όσο και την ανθεκτικότητα έναντι υποκλοπών. Ο νέος πυρήνας είναι πλήρως βασισμένος σε λογισμικό και επιτρέπει τον δυναμικό καταμερισμό πόρων μέσω network slicing. Ένα στρατιωτικό δίκτυο μπορεί έτσι να `διαθέτει ένα slice αποκλειστικά για κρίσιμες επικοινωνίες διοίκησης και ελέγχου, ένα άλλο για ροές δεδομένων από αισθητήρες και ένα τρίτο για εφαρμογές χαμηλότερης προτεραιότητας. Η λογική αυτή προσφέρει εγγυημένη ποιότητας υπηρεσίας(QoS) ακόμη και σε συνθήκες έντονης πίεσης στο δίκτυο [33], [31].

Ιδιαίτερο ενδιαφέρον παρουσιάζουν τα ποσοτικά χαρακτηριστικά απόδοσης του 5G, τα οποία αποκαλούνται Key Performance Indicators(KPIs). Σε αυτά περιλαμβάνονται ρυθμοί μετάδοσης που φτάνουν τα 20 Gbps στο downlink, καθυστέρηση της τάξης του 1 ms σε εφαρμογές URLLC, αξιοπιστία άνω του 99.999%, υποστήριξη κινητικότητας έως και 500km/h και δυνατότητα σύνδεσης έως 1 εκατομμυρίου συσκευών ανά km^2 [34].Οι δείκτες αυτοί, που καθορίστηκαν από την ITU και δοκιμάζονται ήδη σε πειραματικά περιβάλλοντα, καταδεικνύουν ότι το 5G μπορεί να ανταποκριθεί στις ανάγκες ταχέως μεταβαλλόμενων στρατιωτικών επιχειρήσεων, όπου απαιτείται συνδυασμός υψηλής χωρητικότητας, αξιοπιστίας και ανθεκτικότητας.



Σχήμα 10 - Οι τρεις κατηγορίες υπηρεσιών του 5G [12]

Τέλος, το 5G εισάγει τη δυνατότητα δυναμικής διαχείρισης φάσματος (Dynamic Spectrum Sharing-DSS), με αποτέλεσμα την παράλληλη αξιοποίηση των ίδιων συχνοτήτων από πολιτικά και στρατιωτικά δίκτυα. Σε πολυεθνικές επιχειρήσεις, όπου συχνά συνυπάρχουν διαφορετικά πρότυπα και κατανομές συχνοτήτων, αυτή η ευελιξία μπορεί να αποδειχθεί καθοριστική για τη διαλειτουργικότητα [33], [34]. Συνολικά, το 5G δεν προσφέρει μόνο βελτιωμένες ταχύτητες, αλλά μια ολιστική, επαναπρογραμματιζόμενη υποδομή επικοινωνίας που μπορεί να αποτελέσει τη βάση για τις μελλοντικές στρατιωτικές δικτυακές αρχιτεκτονικές.

3.1.2 Στρατιωτικές Εφαρμογές του 5G

Η αξιοποίηση του 5G στις στρατιωτικές επικοινωνίες δεν περιορίζεται στη βελτίωση της ταχύτητας μετάδοσης, αλλά συνδέεται άμεσα με την αναβάθμιση της επιχειρησιακής ικανότητας στο πεδίο. Το χαμηλό latency, η υψηλή αξιοπιστία και δυνατότητα μαζικής διασύνδεσης επιτρέπουν την

ανάπτυξη νέων δογμάτων μάχης, βασισμένων στη δικτυοκεντρική φιλοσοφία(network centric warfare) [12].

Μία από τις πιο κρίσιμες εφαρμογές αφορά τα συστήματα διοίκησης και ελέγχου(Command and Control-C2). Στις σύγχρονες επιχειρήσεις, η έγκαιρη μετάδοση εντολών και η λήψη δεδομένων από πολλαπλές πηγές καθορίζουν την επιτυχία ή αποτυχία της αποστολής. Το 5G, με καθυστέρηση μικρότερη του 1 ms και αξιοπιστία που υπερβαίνει το 99.999%, καθιστά δυνατή την επικοινωνία σε σχεδόν πραγματικό χρόνο, μειώνοντας σημαντικά τον κύκλο λήψης αποφάσεων(decision-making loop) [32].

Ιδιαίτερη σημασία έχει και η χρήση του 5G σε μη επανδρωμένα εναέρια οχήματα(UAVs), τα οποία μπορούν να λειτουργούν τόσο ως φορείς αισθητήρων όσο και ως ιπτάμενοι σταθμοί βάσης. Με αυτόν τον τρόπο, παρέχουν προσωρινή κάλυψη σε απομακρυσμένες ή εχθρικές περιοχές όπου δεν παρέχει σταθερή υποδομή. Σε πρόσφατες δοκιμές του ΝΑΤΟ, χρησιμοποιήθηκαν private 5G δίκτυα για τη μετάδοση εικόνας υψηλής ευκρίνειας από UAVs, υποστηρίζοντας επιχειρήσεις επιτήρησης και τακτικής αναγνώρισης [35].

Παράλληλα, η έννοια του IoMT ενδυναμώνεται από τις δυνατότητες του 5G. Στρατιώτες, οχήματα, αισθητήρες και συστήματα όπλων μπορούν να καταγραφούν βιομετρικά δεδομένα, όπως παλμό ή επίπεδα στρες, προσφέροντας δυνατότητες για εξατομικευμένη παρακολούθηση της φυσικής κατάστασης των μαχητών.

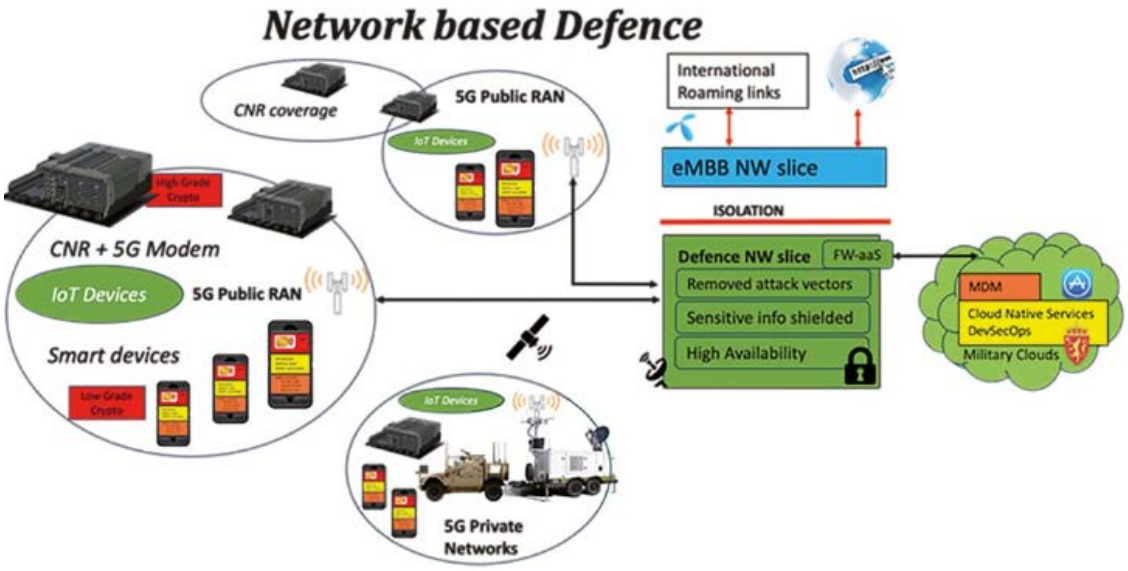
Στον τομέα της εκπαίδευσης, το 5G καθιστά δυνατή τη χρήση τεχνολογιών Επαυξημένης και Εικονικής Πραγματικότητας(AR/VR) σε στρατιωτικά γυμνάσια. Η χαμηλή καθυστέρηση είναι καθοριστική ώστε οι εκπαιδευόμενοι να βιώνουν ρεαλιστικά σενάρια μάχης, μειώνοντας την ανάγκη για ακριβές ασκήσεις πεδίου και περιορίζοντας τους κινδύνους [36].

Τέλος, το 5G μπορεί να παίξει καταλυτικό ρόλο στην υποστήριξη logistics. Συστήματα μεταφορών, αποθήκευσης και ανεφοδιασμού μπορούν να παρακολουθούνται σε πραγματικό χρόνο μέσω IoT αισθητήρων, διασφαλίζοντας ότι οι γραμμές ανεφοδιασμού παραμένουν λειτουργικές ακόμα και σε περίπλοκα επιχειρησιακά περιβάλλοντα [37].

Συνολικά, οι στρατιωτικές εφαρμογές του 5G δεν περιορίζονται σε ένα πεδίο αλλά εκτείνονται σε όλες τις διαστάσεις της στρατιωτικής δράσης, από τον έλεγχο και την επίγνωση κατάστασης μέχρι την εκπαίδευση και την επιμελητεία. Αυτή η πολυδιάστατη συνεισφορά του 5G εξηγεί γιατί μεγάλες δυνάμεις όπως οι ΗΠΑ, η Κίνα και η Νότια Κορέα επενδύουν ήδη σε πειραματικά έργα ανάπτυξης private 5G δικτύων για στρατιωτική χρήση [12].

Η ανάπτυξη στρατιωτικών private 5G δικτύων δεν αφορά μόνο την επιλογή φάσματος, αλλά κυρίως και την ενσωμάτωση μηχανισμών ασφάλειας, απομόνωσης και ανθεκτικότητας που

υπερβαίνουν τα εμπορικά πρότυπα. Όπως φαίνεται και στο Σχήμα 11, τα στρατιωτικά δίκτυα βασίζονται σε συνδυασμό δημόσιων και private 5G υποδομών, με αξιοποίηση τεχνικών όπως το network slicing για την απομόνωση κρίσιμων υπηρεσιών, τη διαχείριση επιθέσεων και την προστασία ευαίσθητων πληροφοριών. Παράλληλα, η χρήση edge computing και στρατιωτικών cloud ενισχύει την αυτονομία στο πεδίο μάχης, ενώ τα IoT συστήματα και οι κινητού σταθμοί βάσης(π.χ. σε οχήματα) επιτρέπουν τη συνεχή επιχειρησιακή συνδεσιμότητα.



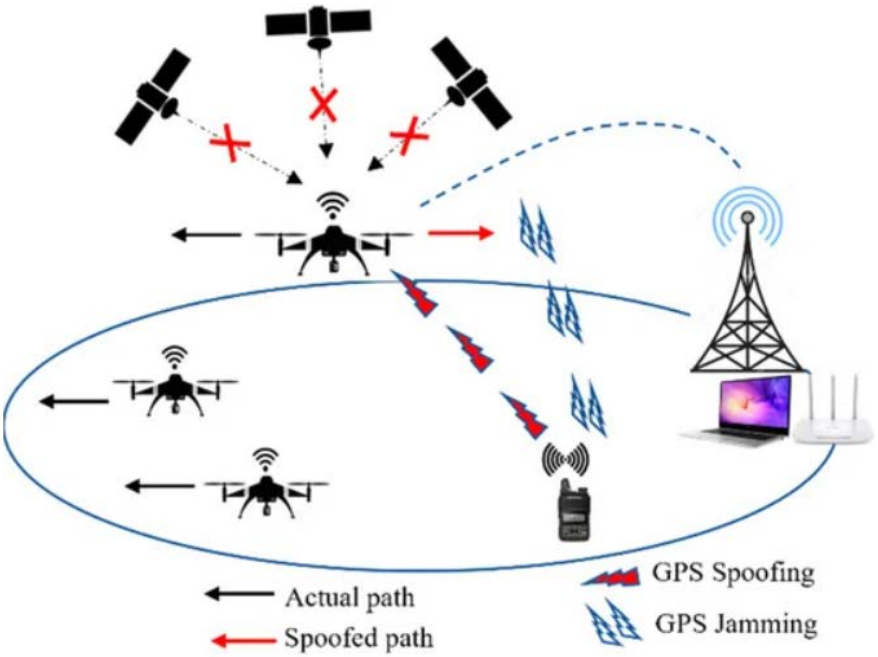
Σχήμα 11-Αρχιτεκτονική Network based Defence[38]

3.1.3 Προκλήσεις και Περιορισμοί

Παρά τα πολλά χαρακτηριστικά του 5G, η εφαρμογή του σε στρατιωτικά περιβάλλοντα δεν είναι ούτε απλή ούτε άμεση. Οι ιδιαιτερότητες του πεδίου μάχης, οι αυξημένες απαιτήσεις ασφάλειας και η ανάγκη για ανθεκτικότητα σε ακραίες συνθήκες δημιουργούν σημαντικές προκλήσεις που πρέπει να αντιμετωπιστούν πριν το 5G ενσωματωθεί πλήρως στα τακτικά δίκτυα.

Η πρώτη και πιο σημαντική πρόκληση αφορά την ασφάλεια. Τα δίκτυα 5G είναι σε μεγάλο βαθμό βασισμένα σε λογισμικό και virtualization γεγονός που καθιστά ιδιαίτερα ευάλωτα σε κυβερνοεπιθέσεις, όπως επιθέσεις τύπου denial-of-service, spoofing ή εισαγωγή κακόβουλου λογισμικού στον πυρήνα του δικτύου [12], [20].Ένα παράδειγμα τέτοιων επιθέσεων και ειδικότερα των spoofing/jamming σε μη-επανδρωμένα συστήματα , απεικονίζεται στο Σχήμα 12. Σε ένα στρατιωτικό περιβάλλον, η απώλεια εμπιστευτικότητας ή ακεραιότητας δεδομένων μπορεί να μεταφραστεί σε απώλεια ανθρώπινων ζωών ή αποτυχία ολόκληρης επιχείρησης. Για το λόγο αυτό, απαιτούνται επιπλέον επίπεδα κρυπτογράφησης, πιστοποίησης και ελέγχου πρόσβασης, πέρα από αυτά που συναντώνται στα εμπορικά δίκτυα.

Εξίσου σοβαρό πρόβλημα αποτελεί το φάσμα συχνοτήτων. Το 5G λειτουργεί σε μεγάλο βαθμό σε ζώνες υψηλών συχνοτήτων(mmWave), οι οποίες έχουν περιορισμένη εμβέλεια και είναι ευάλωτες σε εμπόδια, καιρικές συνθήκες ή ακόμη και σκόπιμες παρεμβολές(jamming). Αυτό συνεπάγεται την ανάγκη για πυκνό δίκτυο κεραιών ή κινητών σταθμών βάσης, κάτι που σε πολεμικές επιχειρήσεις είναι δύσκολο να εξασφαλιστεί [37]. Επιπλέον, η χρήση εμπορικού φάσματος δημιουργεί ζητήματα συνύπαρξης με πολιτικά δίκτυα και πιθανής αλληλοπαρεμβολής.



Σχήμα 12-Παράδειγμα επίθεσης spoofing/jamming σε drone στο πεδίο μάχης[39]

Ένα άλλο ζήτημα είναι η ανθεκτικότητα και αξιοπιστία. Ενώ τα εμπορικά δίκτυα θεωρείται αποδεκτό να υπάρχουν μικρές διακοπές υπηρεσίας, στα στρατιωτικά περιβάλλοντα η επικοινωνία πρέπει να είναι συνεχής και αδιάλειπτη. Η απώλεια ενός σταθμού βάσης ή η διακοπή σύνδεσης δεν μπορεί να αντιμετωπιστεί με τον ίδιο τρόπο που γίνεται σε αστικά περιβάλλοντα. Για τον λόγο αυτό, αναπτύσσονται λύσεις όπως τα hardened 5G δίκτυα, με πρόσθετους μηχανισμούς αυτόματης επανεκκίνησης, redundancy και προστασία φάσματος [35].

Σημαντικός περιορισμός αφορά επίσης την κατανάλωση ενέργειας. Οι στρατιωτικές επιχειρήσεις εκτελούνται συχνά σε περιοχές χωρίς σταθερή παροχή ρεύματος και η ενεργειακή αυτονομία του εξοπλισμού επικοινωνιών είναι κρίσιμη. Τα δίκτυα 5G, με την αυξημένη υπολογιστική ισχύ που απαιτούνται(π.χ. για massive MIMO, beamforming και edge computing), ενδέχεται να δημιουργήσουν μεγαλύτερες ανάγκες σε κατανάλωση ενέργειας σε σχέση με προηγούμενες τεχνολογίες [32].

Τέλος, η εξάρτηση από εμπορικούς παρόχους αποτελεί στρατηγικό πρόβλημα. Ενώ στα πολιτικά δίκτυα η συνεργασία με τηλεπικοινωνιακούς παρόχους είναι δεδομένη, στο στρατιωτικό

πεδίο κάτι τέτοιο εγκυμονεί κινδύνους. Η διακοπή πρόσβασης ή η στοχευμένη κυβερνοεπίθεση σε υποδομές τρίτων μπορεί να οδηγήσει σε κατάρρευση κρίσιμων στρατιωτικών επικοινωνιών. Αυτός ο λόγος που διεθνώς εξετάζεται η ανάπτυξη ανεξάρτητων private 5G δικτύων, παράλληλα με υφιστάμενες τεχνολογίες όπως τα SDRs και τα MANETs [12], [35].

Συνολικά, το 5G προσφέρει σημαντικές δυνατότητες για το στρατιωτικό περιβάλλον, αλλά η πρακτική του εφαρμογή απαιτεί την αντιμετώπιση πολύπλοκων τεχνικών και επιχειρησιακών περιορισμών. Η επιτυχία του θα εξαρτηθεί από την ικανότητα των Ένοπλων Δυνάμεων να προσαρμόσουν την τεχνολογία αυτή σε συνθήκες που ξεπερνούν κατά πολύ τις απαιτήσεις των εμπορικών δικτύων.

3.1.4 Μελλοντικές Κατευθύνσεις

Παρότι το 5G εισάγει σημαντικές καινοτομίες, θεωρείται πλέον μεταβατικό στάδιο προς ακόμη πιο προηγμένες τεχνολογίες. Στο στρατιωτικό περιβάλλον, το 5G δεν πρόκειται να αντικαταστήσει πλήρως τα υπάρχοντα συστήματα επικοινωνιών, όπως τα δίκτυα δορυφορικών επικοινωνιών(SATCOM), τα Software Defined Radios(SDRs) και τα Mobile Ad Hoc(MANETs). Αντιθέτως, η μελλοντική πορεία δείχνει προς την κατεύθυνση υβριδικών αρχιτεκτονικών, όπου διαφορετικές τεχνολογίες συνδυάζονται ώστε να προσφέρουν μέγιστη ανθεκτικότητα και ευελιξία [12], [35].

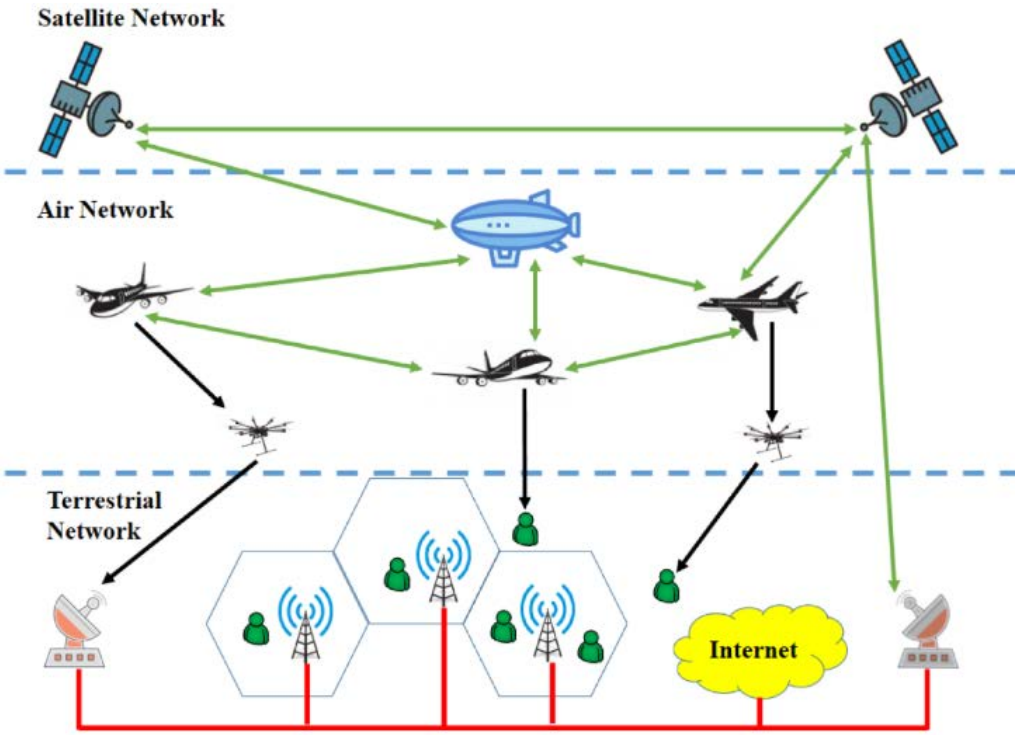
Μία από τις πλέον υποσχόμενες κατευθύνσεις είναι η ενσωμάτωση του 5G με το 6G, το οποίο βρίσκεται ήδη σε φάση ερευνητικής ανάπτυξης. Οι στόχοι του 6G περιλαμβάνουν εξαιρετικά χαμηλές καθυστερήσεις(<0.1ms), ρυθμούς μετάδοσης της τάξης των Tbps και την ενσωμάτωση τεχνητής νοημοσύνης (AI) στον ίδιο τον πυρήνα του δικτύου [40].Σε στρατιωτικές εφαρμογές, αυτό θα μπορούσε να σημαίνει πλήρη αυτοματοποίηση της διαχείρισης φάσματος, δυναμική ενίσχυση και εξουδετέρωση παρεμβολών, καθώς και self-healing networks σε περίπτωση κυβερνοεπιθέσεων.

Επιπλέον, η συνδυασμένη χρήση του 5G με μη γήινες επικοινωνίες(Non-Terrestrial Networks-NTN), όπως δορυφόροι χαμηλής τροχιάς(LEO), αερόπλοια υψηλού υψομέτρου(HAPs) και UAV relays, ανοίγει τον δρόμο για ένα πανταχού παρόν στρατιωτικό δίκτυο. Σε ένα τέτοιο σενάριο, στρατιωτικές μονάδες σε ξηρά, θάλασσα, αέρα και διάστημα θα παραμένουν συνεχώς συνδεδεμένες, ανεξαρτήτως γεωγραφικών περιορισμών [41]. Η αρχιτεκτονική αυτή, που συνδέει δορυφορικές, εναέριες και επίγειες υποδομές σε ένα ενιαίο και ευφυές σύστημα επικοινωνιών, παρουσιάζεται στο Σχήμα 13, το οποίο απεικονίζει ένα στρατηγικό μοντέλο υβριδικού δικτύου(HSTN) βασισμένο στη συνεργασία LEO δορυφόρων,UAVs και 5G/6G υποδομών.

Μια άλλη σημαντική προοπτική είναι η αξιοποίηση του edge computing και των AI-driven cognitive networks. Η μεταφορά της υπολογιστικής ισχύος κοντά στο πεδίο μάχης μειώνει την εξάρτηση από κεντρικά data centers και επιτρέπει την επεξεργασία δεδομένων σε πραγματικό χρόνο, κάτι κρίσιμο για εφαρμογές όπως η αυτόνομη πλοήγηση UAVs ή η αναγνώριση απειλών μέσω

αισθητήρων. Η τεχνητή νοημοσύνη θα αποτελέσει επίσης βασικό παράγοντα στην αυτοματοποίηση της διαχείρισης του δικτύου, καθώς θα μπορεί να προβλέπει συμφόρηση, να προσαρμόζει slices δυναμικά και να λαμβάνει αποφάσεις χωρίς ανθρώπινη παρέμβαση.

Τέλος, η ερευνητική κοινότητα εστιάζει σε λύσεις που συνδυάζουν το 5G με το Quantum Key Distribution(QKD) και άλλες κβαντικές τεχνολογίες, ώστε να διασφαλιστεί το μέγιστο επίπεδο ασφάλειας στις στρατιωτικές επικοινωνίες [43]. Παρότι τέτοιες τεχνολογίες βρίσκονται ακόμη σε πρώιμο στάδιο, θεωρούνται ιδιαίτερα υποσχόμενες για ένα περιβάλλον όπου η κυβερνοασφάλεια αποτελεί θεμέλιο επιβίωσης.



Σχήμα 13-Στρατηγικό μοντέλο υβριδικού δικτύου(HSTN) που ενσωματώνει δορυφόρους, UAVs και επίγειες 5G/6G υποδομές[42]

Συνοψίζοντας, το 5G αποτελεί τη βάση για ένα νέο οικοσύστημα στρατιωτικών επικοινωνιών, αλλά το μέλλον ανήκει σε υβριδικά δίκτυα που θα συνδυάζουν 5G,6G, δορυφορικές υποδομές, γνωστικά δίκτυα και κβαντική ασφάλεια. Ο δρόμος προς τις τεχνολογίες αυτές θα καθορίσει όχι μόνο την αποδοτικότητα των στρατιωτικών επιχειρήσεων, αλλά και τη στρατηγική ισορροπία ισχύος τις επόμενες δεκαετίες.

3.2 Software Defined Radios(SDRs) και Cognitive Radios στις στρατιωτικές επικοινωνίες

3.2.1 Software Defined Radios(SDRs)

Η μετάβαση από τα παραδοσιακά ραδιοσυστήματα στα Software Defined Radios(SDRs) αποτελεί μία από τις πιο σημαντικές τεχνολογικές εξελίξεις στον χώρο των στρατιωτικών επικοινωνιών.

Σε αντίθεση με τα συμβατικά ραδιόφωνα, στα οποία οι λειτουργίες, όπως η επιλογή συχνότητας, το εύρος ζώνης ή το πρωτόκολλο μετάδοσης, είναι ενσωματωμένες σε υλικό (hardware), τα SDRs βασίζονται σε λογισμικό για τον ορισμό των παραμέτρων λειτουργίας [44]. Με αυτόν τον τρόπο, το ίδιο φυσικό σύστημα μπορεί να τροποποιηθεί ώστε να υποστηρίξει διαφορετικά πρότυπα και λειτουργίες, χωρίς την ανάγκη αλλαγής εξοπλισμού.

Το βασικό πλεονέκτημα αυτής της προσέγγισης είναι η ευελιξία. Ένα SDR μπορεί να προσαρμοστεί άμεσα στις απαιτήσεις της αποστολής, αλλάζοντας απλώς το λογισμικό που «τρέχει». Για παράδειγμα, ένα φορητό τερματικό μπορεί να λειτουργήσει ως VHF για φωνητικές επικοινωνίες, στη συνέχεια να μεταβεί σε UHF για τακτικά δεδομένα και αργότερα να υποστηρίξει SATCOM για επικοινωνία μεγάλης εμβέλειας [45]. Αυτή η δυνατότητα ενισχύει σημαντικά την διαλειτουργικότητα μεταξύ δυνάμεων που χρησιμοποιούν διαφορετικά πρωτόκολλα, καθώς η συμβατότητα επιτυγχάνεται στο επίπεδο του λογισμικού. Η πρακτική εφαρμογή αυτής της ευελιξίας σε πεδία επιχειρήσεων φαίνεται καθαρά σε ένα τυπικό φορητό SDR(βλέπε Σχήμα 14).



Σχήμα 14-Φορητό στρατιωτικό SDR με ανθεκτικό σχεδιασμό πεδίου μάχης[46]

Σημαντικό παράδειγμα εφαρμογής αποτελεί το πρόγραμμα Joint Tactical Radio System(JTRS) των Ηνωμένων Πολιτειών, το οποίο σχεδιάστηκε για να αντικαταστήσει δεκάδες διαφορετικά ραδιοσυστήματα με μια ενοποιημένη πλατφόρμα. Το JTRS χρησιμοποιεί SDRs που μπορούν να

υποστηρίξουν πολλαπλά waveforms, όπως SINCGARS, EPLRS, WNW και SATCOM, προσφέροντας μια κοινή υποδομή επικοινωνίας για τον στρατό, το ναυτικό, την αεροπορία και το σώμα πεζοναυτών [47]. Με αυτόν τον τρόπο, μειώνεται η ανάγκη για ξεχωριστό εξοπλισμό, ενώ ταυτόχρονα αυξάνεται η επιχειρησιακή ευελιξία.

Εκτός από τη διαλειτουργικότητα, τα SDRs συμβάλλουν και στην παραγωγικότητα της ανάπτυξης. Νέα πρωτόκολλα και waveform μπορούν να ενσωματωθούν μέσω ενημερώσεων λογισμικού(software updates), μειώνοντας το κόστος ανάπτυξης νέων συστημάτων και επιτρέποντας την ταχύτερη ενσωμάτωση τεχνολογικών εξελίξεων. Στρατιωτικά προγράμματα σε χώρες του ΝΑΤΟ αξιοποιούν ήδη SDRs για την ενίσχυση της συνεργασίας σε πολυεθνικές επιχειρήσεις, καθώς το λογισμικό μπορεί να προσαρμόζεται ανάλογα με τα εκάστοτε πρότυπα επικοινωνίας [48].

Συνολικά, τα SDRs αποτελούν τη βάση για ένα πιο ευέλικτο και προσαρμόσιμο οικοσύστημα στρατιωτικών επικοινωνιών, που όχι μόνο βελτιώνει την τακτική αποτελεσματικότητα, αλλά ανοίγει και τον δρόμο για την υιοθέτηση πιο εξελιγμένων τεχνολογιών, όπως τα Cognitive Radios,τα οποία θα αναλυθούν παρακάτω.

3.2.2 MANETs σε συνδυασμό με SDRs

Η ανάγκη για ευέλικτες και αυτόνομες μορφές επικοινωνίας στο πεδίο των επιχειρήσεων οδήγησε στην ανάπτυξη των Mobile Ad Hoc Networks(MANETs), τα οποία λειτουργούν χωρίς να απαιτούν σταθερή υποδομή. Σε αντίθεση με τα παραδοσιακά δίκτυα που βασίζονται σε σταθμούς βάσης και κεντρικούς ελεγκτές, τα MANETs σχηματίζονται δυναμικά από τους ίδιους τους κόμβους. Κάθε κόμβος λειτουργεί ταυτόχρονα ως πομπός, δέκτης και αναμεταδότης, επιτρέποντας τη δημιουργία ενός κατανεμημένου, αυτό-οργανωμένου δικτύου που μπορεί να επεκτείνεται ή να αναδιαμορφώνεται ανάλογα με την επιχειρησιακή κατάσταση [49].

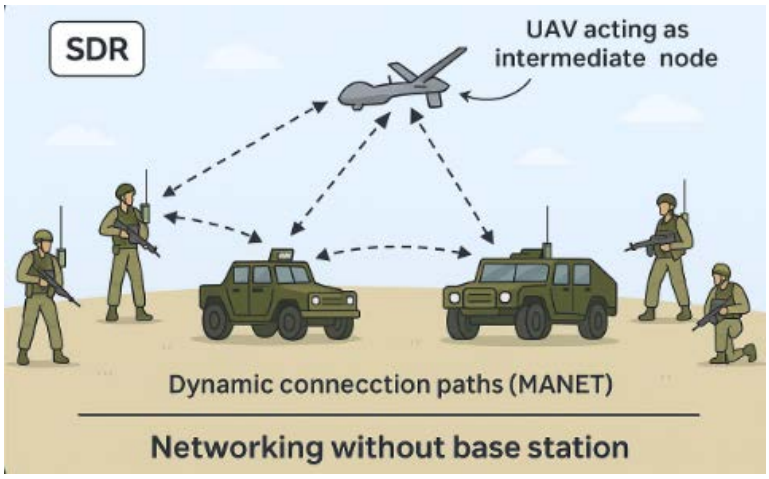
Η συμβολή των SDRs στην ανάπτυξη των MANETs είναι καθοριστική. Μέσω των SDRs, κάθε κόμβος μπορεί να προσαρμόζεται άμεσα σε διαφορετικά πρότυπα επικοινωνίας, να αλλάζει συχνότητες και να υποστηρίζει διαφορετικά πρωτόκολλα, απλώς με την αναβάθμιση του λογισμικού. Με αυτόν τον τρόπο , τα MANETs αποκτούν διαλειτουργικότητα που επιτρέπει σε ετερογενείς δυνάμεις όπως στρατιώτες, οχήματα και UAVs διαφορετικών χωρών να συνδέονται σε κοινό δίκτυο, χωρίς να απαιτείται συμβατός εξοπλισμός [50].

Ένα από τα χαρακτηριστικά των MANETs είναι η self-healing. Όταν ο κόμβος αποκοπεί ή τεθεί εκτός λειτουργίας, το δίκτυο ανακατανέμει δυναμικά τις διαδρομές των δεδομένων ώστε να διατηρείται η επικοινωνία. Αυτό καθιστά τα MANETs ιδιαίτερα ανθεκτικά σε συνθήκες μάχης ή φυσικών καταστροφών, όπου οι υποδομές μπορεί να καταστραφούν ή να μην υπάρχουν. Στο στρατιωτικό πλαίσιο, η δυνατότητα αυτή σημαίνει ότι ακόμη και αν μια ομάδα αποκοπεί από το κέντρο, μπορεί να συνεχίσει να επικοινωνεί τοπικά, διατηρώντας την επιχειρησιακή της αυτονομία [51].

Η χρήση UAVs ως κόμβων-αναμεταδοτών (relay nodes) ενισχύει περαιτέρω τις δυνατότητες των MANETs. Ένα UAV μπορεί να λειτουργήσεις ως «εναέριος κόμβος» που επεκτείνει την ακτίνα του δικτύου πέρα από τα γεωγραφικά όρια των επίγειων μονάδων, εξασφαλίζοντας επικοινωνία ακόμη και σε δύσβατα ή εχθρικά περιβάλλοντα. Σε σενάρια NATO, UAVs εξοπλισμένα με SDRs έχουν χρησιμοποιηθεί ως ενδιάμεσοι κόμβοι για τη διατήρηση επικοινωνίας μεταξύ διασκορπισμένων ομάδων ειδικών δυνάμεων, επιτρέποντας τον συντονισμό σε πραγματικό χρόνο. Η λογική αυτής της αρχιτεκτονικής απεικονίζεται στο Σχήμα 15, όπου παρουσιάζεται η ενσωμάτωση των SDRs σε MANET για την επίτευξη ευέλικτης και τακτικής επικοινωνίας μεταξύ επίγειων, εναέριων και κινητών κόμβων.

Τα MANETs με SDRs υποστηρίζουν επίσης εξελιγμένους μηχανισμούς κρυπτογράφησης και προσαρμοστική δρομολόγηση(adaptive routing). Η δρομολόγηση δεν βασίζεται μόνο στη γεωγραφική απόσταση, αλλά λαμβάνει υπόψη την ποιότητα σήματος, το επίπεδο παρεμβολών και τη διαθεσιμότητα κόμβων. Αυτό είναι κρίσιμο σε περιβάλλοντα ηλεκτρονικού πολέμου, όπου το φάσμα μπορεί να αλλάζει συνεχώς λόγω jamming ή spoofing. Ο δυναμικός αυτός χαρακτήρας κάνει τα MANETs όχι μόνο ευέλικτα αλλά και ιδιαίτερα ανθεκτικά απέναντι σε επιθέσεις [52].

Η τεχνολογία αυτή βρίσκει εφαρμογές τόσο σε καθαρά στρατιωτικά σενάρια όσο και σε ανθρωπιστικές επιχειρήσεις. Σε αποστολές διάσωσης μετά από φυσικές καταστροφές, UAVs και φορητοί ασύρματοι με SDRs μπορούν να σχηματίσουν μέσα σε λίγα λεπτά ένα προσωρινό δίκτυο, επιτρέποντας την επικοινωνία σωστικών συνεργείων σε περιοχές χωρίς καμία υποδομή. Στο πεδίο μάχης, μικρές μονάδες που κινούνται ανεξάρτητα μπορούν να παραμείνουν συνδεδεμένες σε πραγματικό χρόνο, χωρίς να χρειάζονται κεντρικό σταθμό ή υποστήριξη από εμπορικά δίκτυα.



Σχήμα 15-Ενσωμάτωση SDR σε MANET για τακτική επικοινωνία

Παρά τα πλεονεκτήματά τους, τα MANETs αντιμετωπίζουν και σημαντικούς περιορισμούς. Το routing παραμένει μια πρόκληση, καθώς η συνεχής κινητικότητα των κόμβων δημιουργεί συνεχείς αλλαγές στη τοπολογία του δικτύου. Επίσης, η κατανάλωση ενέργειας είναι ιδιαίτερα κρίσιμη, αφού οι φορητοί κόμβοι έχουν περιορισμένη αυτονομία και η συνεχής αναμετάδοση δεδομένων μπορεί να

εξαντλήσει γρήγορα τις μπαταρίες. Τέλος, η πολυπλοκότητα στη διαχείριση και η ανάγκη για ισχυρό λογισμικό αυξάνουν το κόστος και τις τεχνικές απαιτήσεις [53].

Συνοψίζοντας, τα MANETs σε συνδυασμό με SDRs προσφέρουν ένα ευέλικτο, ανθεκτικό και διαλειτουργικό σύστημα επικοινωνιών που ανταποκρίνεται στις ανάγκες του σύγχρονου πεδίου μάχης. Η δυνατότητα αυτό-οργάνωσης, η ανθεκτικότητα σε απώλειες κόμβων, η χρήση UAVs ως ενδιάμεσων κόμβων και η δυναμική προσαρμογή στο φάσμα καθιστούν τα δίκτυα αυτά κρίσιμα για μελλοντικές στρατιωτικές επιχειρήσεις. Παράλληλα, η εξέλιξή τους ανοίγει τον δρόμο για την επόμενη γενιά συστημάτων τα Cognitive MANETs, όπου η τεχνητή νοημοσύνη προσθέτει γνωστικές δυνατότητες στην ήδη δυναμική φύση των MANETs.

3.2.3 Cognitive Radios και Cognitive MANETs

Η εξέλιξη από τα SDRs προς τα Cognitive Radios αποτελεί ένα από τα πιο σημαντικά βήματα στη σύγχρονη στρατιωτική επικοινωνιακή τεχνολογία. Ενώ τα SDRs προσφέρουν ευελιξία και προσαρμοστικότητα μέσω αλλαγών λογισμικού, τα Cognitive Radios ενσωματώνουν τεχνικές τεχνητής νοημοσύνης(AI) και αυτόνομης λήψης αποφάσεων, επιτρέποντας στο σύστημα να καταλαβαίνει το ραδιοφάσμα, να μαθαίνει από το περιβάλλον του και να προσαρμόζει αυτόματα τις λειτουργίες του[58]. Ο όρος εισήχθη από τον Mitola το 1999 και από τότε αποτελεί σημείο αναφοράς για την έρευνα γύρω από τα “έξυπνα” ασύρματα συστήματα [44]

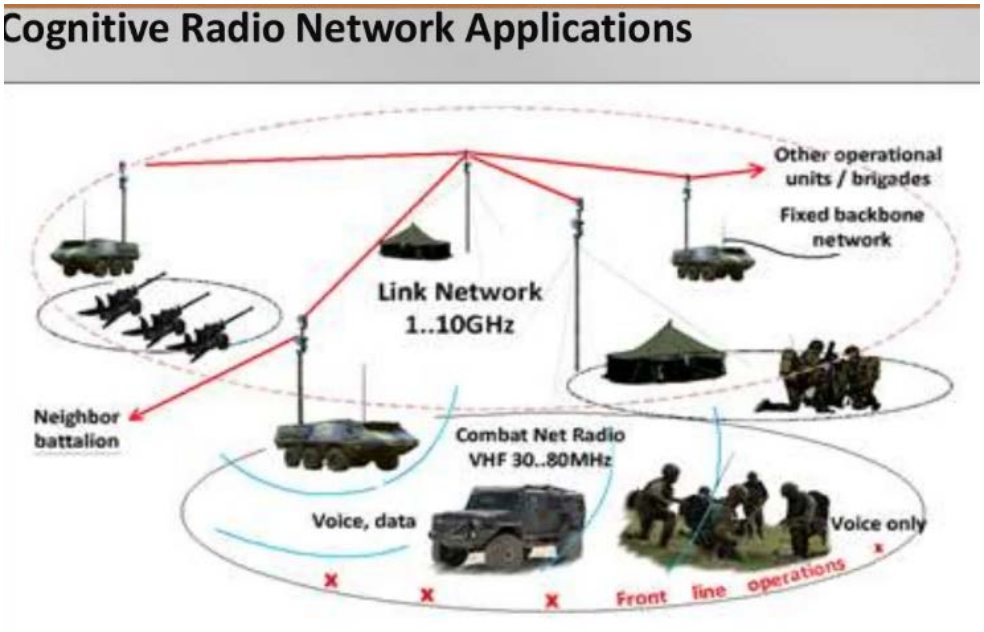
Κεντρική λειτουργία ενός Cognitive Radio είναι το spectrum sensing, δηλαδή η συνεχής παρακολούθηση του φάσματος για την ανίχνευση κενών καναλιών (spectrum holes) και την αποφυγή παρεμβολών. Σε στρατιωτικό περιβάλλον, αυτό μεταφράζεται αυξημένη ανθεκτικότητα απέναντι σε jamming και spoofing επιθέσεις, καθώς το ραδιοσύστημα μπορεί να αλλάξει συχνότητα ή ακόμη και waveform σε πραγματικό χρόνο χωρίς την παρέμβαση του χειριστή [54]. Παράλληλα, τα Cognitive Radios υποστηρίζουν dynamic spectrum access(DSA), που επιτρέπει την κατανομή πόρων ανάλογα με την κρισιμότητα της επικοινωνίας. Για παράδειγμα, ένα slice του δικτύου μπορεί να αφιερωθεί αποκλειστικά σε επικοινωνίες C2(Command and Control), ενώ το λιγότερο κρίσιμα δεδομένα να δρομολογούνται σε δεύτερα κανάλια [55].

Η ικανότητα αυτή αποκτά ιδιαίτερη σημασία σε πολυεθνικές επιχειρήσεις, όπου συχνά οι διαφορετικοί στρατοί χρησιμοποιούν ετερογενείς τεχνολογίες και φάσματα. Τα Cognitive Radios επιτρέπουν την αυτόματη γεφύρωση μεταξύ διαφορετικών συστημάτων, διευκολύνοντας τη συνεργασία χωρίς να απαιτείται κοινός εξοπλισμός εκ των προτέρων. Επίσης, περιβάλλοντα με περιορισμένο φάσμα, τα Cognitive Radios μπορούν να διαμοιράζουν δυναμικά το διαθέσιμο εύρος ζώνης, ελαχιστοποιώντας τον κίνδυνο συμφόρησης.

Μία ακόμη καινοτομία είναι η ενσωμάτωση μηχανισμών adaptive modulation and coding(AMC), που επιτρέπουν στο δίκτυο να προσαρμόζει τον τρόπο μετάδοσης ανάλογα με την

ποιότητα καναλιού. Έτσι, σε συνθήκες υψηλού θορύβου ή παρεμβολών, το Cognitive Radio μειώνει το ρυθμό μετάδοσης για να διατηρήσει την αξιοπιστία, ενώ σε καθαρό φάσμα αυξάνει το throughput [56]. Η δυνατότητα αυτή είναι κρίσιμη για τα στρατιωτικά δίκτυα, όπου η ποιότητα του καναλιού μεταβάλλεται συνεχώς λόγω κινητικότητας, γεωγραφικών εμποδίων ή εχθρικών επιθέσεων.

Η έννοια των Cognitive MANETs συνδυάζει τα παραπάνω χαρακτηριστικά των Mobile Ad Hoc Networks. Σε ένα Cognitive MANET, κάθε κόμβος δεν λειτουργεί μόνο ως πομπός/αναμεταδότης αλλά και ως «έξυπνος πράκτορας» που λαμβάνει αποφάσεις για το φάσμα και την δρομολόγηση. Η δικτυακή τοπολογία δεν είναι μόνο αυτό-οργανωμένη αλλά και αυτό-βελτιούμενη, με δυνατότητα self-healing σε περίπτωση βλάβης ή αποκοπής κόμβων [57]. Για παράδειγμα, αν μια ομάδα στρατιωτών χάσει την άμεση σύνδεση με το κέντρο, τα Cognitive Radio- enabled MANETs μπορούν να αναπροσαρμόσουν τις διαδρομές δεδομένων, αξιοποιώντας UAVs ή αισθητήρες ως ενδιάμεσους κόμβους χωρίς ανθρώπινη παρέμβαση. Η πρακτική εφαρμογή της αρχιτεκτονικής αυτής φαίνεται παρακάτω στο Σχήμα 16, το οποίο απεικονίζει ένα παράδειγμα δικτύου πεδίου μάχης βασισμένου σε Cognitive Radios, όπου οι κόμβοι λειτουργούν αυτόνομα ως Cognitive MANET, προσαρμόζοντας δυναμικά τη συχνότητα και τις διαδρομές μετάδοσης.



Σχήμα 16 - Δίκτυο πεδίου μάχης με nodes που λειτουργούν ως κόμβοι Cognitive MANETs[58]

Στην πράξη, τα Cognitive MANETs υπόσχονται ανθεκτικότητα σε ηλεκτρονικό πόλεμο και αυξημένη ασφάλεια. Χρησιμοποιώντας machine learning αλγόριθμους, μπορούν να αναγνωρίζουν πρότυπα παρεμβολών και να αντιδρούν προληπτικά, αλλάζοντας συχνότητα ή πρωτόκολλο πριν επηρεαστεί η επικοινωνία. Παράλληλα, η αποκεντρωμένη φύση τους τα καθιστά λιγότερο ευάλωτα σε single-point failures, σε αντίθεση με τα παραδοσιακά κεντρικά δίκτυα [59].

Παρότι οι δυνατότητές τους είναι εντυπωσιακές, οι προκλήσεις παραμένουν σημαντικές. Η συνεχής ανάλυση του φάσματος και η εκτέλεση αλγορίθμων μηχανικής μάθησης απαιτούν μεγάλη υπολογιστική ισχύ και κατανάλωση ενέργειας, κάτι που μπορεί να περιορίσει τη χρήση τους σε μικρές φορητές συσκευές. Επιπλέον, τα Cognitive Radios εισάγουν νέα σημεία ευπάθειας, καθώς οι αλγόριθμοι που βασίζονται σε δεδομένα μπορεί να γίνουν στόχος κακόβουλων επιθέσεων(π.χ. adversarial machine learning) [60].

Συμπερασματικά, τα Cognitive Radios και Cognitive MANETs συνιστούν το επόμενο βήμα στην εξέλιξη των στρατιωτικών επικοινωνιών, προσφέροντας ένα «έξυπνο» και αυτοπροσαρμοζόμενο δίκτυο που ανταποκρίνεται δυναμικά στις απαιτήσεις του πεδίου μάχης. Αν και η τεχνολογία βρίσκεται ακόμη σε πειραματικό στάδιο, οι διεθνείς στρατιωτικές οργανώσεις και η ερευνητική κοινότητα επενδύουν σημαντικά την ανάπτυξή της, καθώς θεωρείται ότι θα αποτελέσει κεντρικό πυλώνα των μελλοντικών τακτικών επικοινωνιακών συστημάτων.

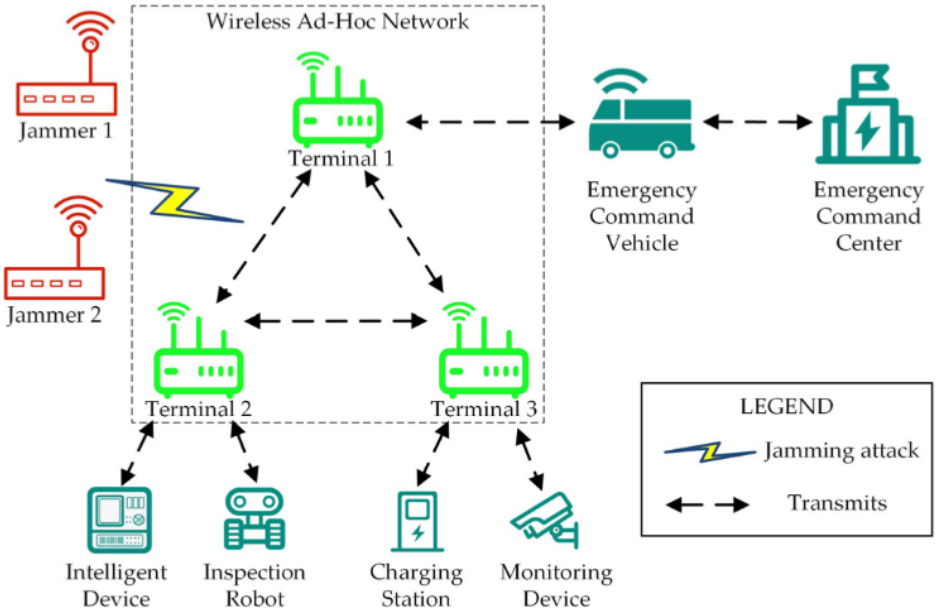
3.2.4 Προκλήσεις και περιορισμοί των SDR/Cognitive Radios

Παρά τα πλεονεκτήματα που παρουσιάζουν τα SDRs και τα Cognitive Radios για το στρατιωτικό πεδίο, η πρακτική τους εφαρμογή συνοδεύεται από μία σειρά προκλήσεων που αφορούν τόσο την τεχνολογική τους ωριμότητα όσο και τη στρατηγική τους αξιοποίηση. Οι περιορισμοί αυτοί πρέπει να αντιμετωπιστούν ώστε τα SDRs και τα Cognitive Radios να αποτελέσουν αξιόπιστο πυλώνα για τις επικοινωνίες επόμενης γενιάς. Παρά τα πλεονεκτήματα, οι πρακτικές εφαρμογές συνοδεύονται από σοβαρούς κινδύνους, για παράδειγμα, στο Σχήμα 17 παρουσιάζεται μια τυπική επίθεση jamming εναντίον στρατιωτικού ad-hoc δικτύου βασισμένου σε Cognitive Radios/SDRs, όπου η έλλειψη ανθεκτικής πολιτικής φάσματος και τ ανεπαρκή μέτρα ανίχνευσης οδηγούν σε απώλεια επικοινωνίας και διατάραξη της επιχειρησιακής συνέχειας.

Η πιο σημαντική πρόκληση αφορά την ασφάλεια. Η φύση των SDRs που βασίζονται σε λογισμικό, τα καθιστά ευάλωτα σε κυβερνοεπιθέσεις και παρεμβολές. Η δυνατότητα φόρτωσης νέων waveforms και λειτουργιών μέσω over-the-air updates δημιουργεί κενά ασφαλείας, δηλαδή εισαγωγή κακόβουλου κώδικα ή παραποίηση πρωτοκόλλων επικοινωνίας. Ειδικά τα Cognitive Radios, τα οποία λαμβάνουν αυτόνομες αποφάσεις για το φάσμα και τη δρομολόγηση, αποτελούν στόχο επιθέσεων adversarial machine learning, όπου εισάγονται ψευδή σήματα ώστε να παραπλανήσουν τον αλγόριθμο [60]. Για παράδειγμα, ένα δίκτυο μπορεί να νομίζει ότι ένα κανάλι είναι κατειλημμένο και να το εγκαταλείψει , δίνοντας στρατηγικό πλεονέκτημα στον αντίπαλο.

Η δεύτερη πρόκληση αφορά το υπολογιστικό και ενεργειακό κόστος. Τα SDRs και ακόμη περισσότερο τα Cognitive Radios απαιτούν ισχυρές μονάδες επεξεργασίας σήματος για να υποστηρίξουν συνεχές spectrum sensing, επεξεργασία δεδομένων και εκτέλεση αλγορίθμων μάθησης. Σε ένα φορητό τακτικό ραδιοσύστημα, η συνεχής αυτή λειτουργία μπορεί να εξαντλήσει γρήγορα την

μπαταρία, περιορίζοντας τον χρόνο επιχειρησιακής αυτονομίας [57]. Αυτό αποτελεί κρίσιμο εμπόδιο σε αποστολές ειδικών δυνάμεων ή UAVs, όπου η ενεργειακή αυτονομία είναι απαραίτητα για την επιβίωση.



Σχήμα 17-Παράδειγμα επίθεσης jamming σε στρατιωτικό ad-hoc δίκτυο Cognitive Radio/SDR [61]

Η υλοποίηση Cognitive Radios σε τακτικά δίκτυα απαιτεί προηγμένη διαχείριση πόρων και συντονισμό μεταξύ κόμβων. Η πολυπλοκότητα αυξάνεται δραματικά σε πολυεθνικές επιχειρήσεις, όπου πρέπει να εξασφαλιστεί η διαλειτουργικότητα μεταξύ συστημάτων διαφορετικών χωρών. Παρά το πλεονέκτημα της δυναμικής προσαρμογής, η παραμετροποίηση ενός Cognitive Radio παραμένει σταθερή, ενώ η ανάγκη για συνεχή ενημέρωση λογισμικού μπορεί να εισάγει νέα σφάλματα [59]. Αυτό δημιουργεί προβλήματα όχι μόνο σε επίπεδο τεχνολογίας αλλά και σε επίπεδο εκπαίδευσης προσωπικού, οι χειριστές πρέπει να διαθέτουν εξειδικευμένη γνώση για να αξιοποιούν πλήρως τις δυνατότητες του συστήματος.

Ένα ακόμη πρόβλημα αφορά το φάσμα συχνοτήτων. Αν και τα Cognitive Radios σχεδιάστηκαν για να εκμεταλλεύονται «κενά» στο φάσμα, η πραγματικότητα στο πεδίο μάχης είναι πιο περίπλοκη, οι συνεχείς παρεμβολές, το jamming και η χρήση εξοπλισμού διαφορετικών συμμάχων περιορίζουν την αποτελεσματικότητα του dynamic spectrum access. Επιπλέον, σε περιβάλλοντα όπου ο αντίπαλος χρησιμοποιεί ισχυρά μέσα ηλεκτρονικού πολέμου, οι αλγόριθμοι spectrum sensing μπορεί να καταστούν αναποτελεσματικοί.

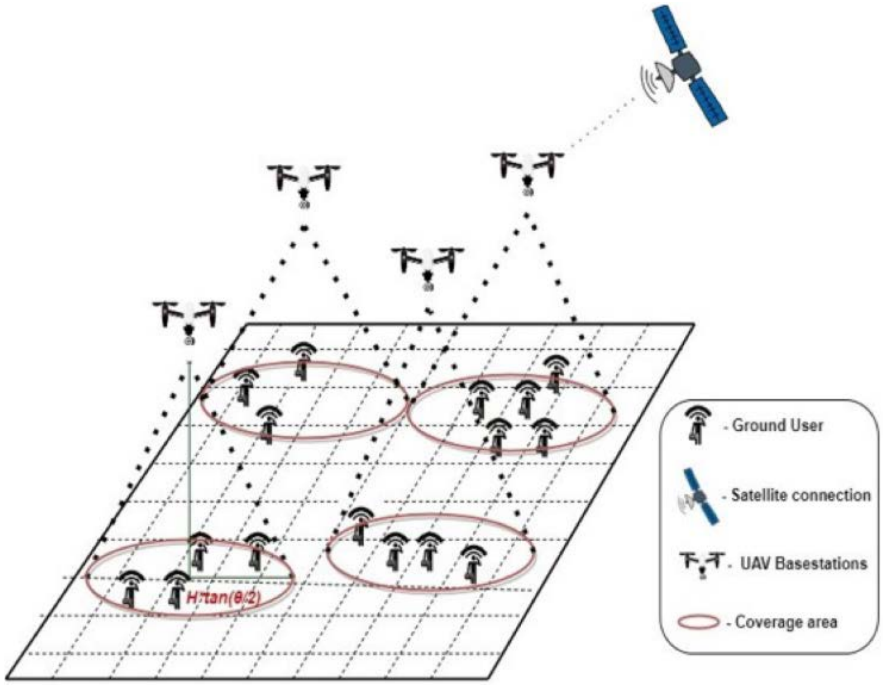
Τέλος, τα SDRs και Cognitive Radios υποφέρουν από την έλλειψη διεθνών προτύπων και πιστοποίησης. Αν και οργανισμοί όπως το IEEE και το ITU έχουν προτείνει τυποποιήσεις, δεν υπάρχει ενιαίο πλαίσιο για στρατιωτική χρήση. Αυτό σημαίνει ότι διαφορετικοί στρατοί αναπτύσσουν συστήματα με διαφορετικές προσεγγίσεις, κάτι που δυσχεραίνει την πολυεθνική συνεργασία.

Παράλληλα, πολλά συστήματα Cognitive Radio βρίσκονται ακόμη σε ερευνητικό στάδιο και δεν έχουν δοκιμαστεί εκτενώς σε πραγματικές συνθήκες μάχης.

3.3 UAVs/Drones και Tactical Mesh Networks

3.3.1 Ρόλος των UAVs στις στρατιωτικές επικοινωνίες

Τα Μη Επανδρωμένα Εναέρια Οχήματα (UAVs)έχουν εξελιχθεί σε μία από τις πιο κρίσιμες τεχνολογίες του σύγχρονου στρατιωτικού δόγματος, ξεπερνώντας κατά πολύ τον αρχικό τους ρόλο ως εργαλεία αναγνώρισης και επιτήρησης. Σήμερα αποτελούν βασικούς πυλώνες των στρατιωτικών επικοινωνιών, προσφέροντας δυνατότητες που δεν μπορούν να επιτευχθούν με παραδοσιακά επίγεια δίκτυα. Η ικανότητά τους να μετακινούνται γρήγορα, να επιχειρούν σε αντίξοες συνθήκες και να φέρουν προηγμένα φορτία επικοινωνιακού εξοπλισμού τα καθιστά πολύτιμους κόμβους για τη διατήρηση της συνδεσιμότητας σε πραγματικό χρόνο. Σε περιβάλλοντα όπου η γεωγραφία, οι εχθρικές ενέργειες ή οι φυσικές καταστροφές καθιστούν ανέφικτη τη χρήση σταθερής υποδομής, τα UAVs λειτουργούν ως κινητοί σταθμοί βάσης, επεκτείνοντας την κάλυψη και διασφαλίζοντας τη συνέχεια της επικοινωνίας. Η επικοινωνία των UAVs ως εναέριων σταθμών βάσης, που επιτρέπει την επέκταση της κάλυψης και τη διατήρηση της επικοινωνίας σε απομακρυσμένες περιοχές, παρουσιάζεται ενδεικτικά στο Σχήμα 18.



Σχήμα 18-UAV που λειτουργεί ως εναέριος σταθμός βάσης[62]

Η συμβολή τους στην τακτική επικοινωνία αποτυπώνεται κυρίως στη χρήση τους ως κινητοί αναμεταδότες. Ένα UAV, εξοπλισμένο με SDRs, μπορεί να συνδεθεί σε διαφορετικά πρότυπα επικοινωνίας και να λειτουργήσει ως ενδιάμεσος κόμβος μεταξύ επίγειων μονάδων που βρίσκονται

εκτός οπτικής επαφής. Με αυτόν τον τρόπο παρακάμπτονται γεωγραφικά εμπόδια, όπως βουνά ή αστικά κτίρια, ενώ διευρύνεται δραστικά η εμβέλεια των επιχειρησιακών δικτύων. Το υψόμετρο πτήσης προσφέρει σαφές πλεονέκτημα έναντι των παραδοσιακών επίγειων αναμεταδοτών, καθώς μειώνει τον κίνδυνο παρεμβολών και βελτιώνει την ποιότητα του σήματος. Ακόμη και ένα μικρό UAV μπορεί να εξασφαλίσει κάλυψη σε χιλιόμετρα ακτίνας, εφόσον τοποθετηθεί στρατηγικά στο επιχειρησιακό πεδίο [63].

Εξίσου καθοριστικός είναι ο ρόλος των UAVs ως φορείς αισθητήρων και «πυλώνων» του IoMT. Εξοπλισμένα με κάμερες, θερμικούς και χημικούς αισθητήρες ή ακόμη και με βιομετρικά συστήματα παρακολούθησης στρατιωτών, τα UAVs μπορούν να συλλέγουν και να μεταδίδουν δεδομένα κρίσιμης σημασίας σε πραγματικό χρόνο. Η ενσωμάτωσή τους σε δίκτυα διοίκησης και ελέγχου επιτρέπει την άμεση ανάλυση και αξιοποίηση των πληροφοριών αυτών, βελτιώνοντας την επίγνωση κατάστασης και επιταχύνοντας τον κύκλο λήψης αποφάσεων. Σε πολυεθνικές επιχειρήσεις, όπου οι πηγές δεδομένων είναι ετερογενείς, τα UAVs μπορούν να λειτουργήσουν ως «έξυπνες πύλες» που ενοποιούν και διαμοιράζουν πληροφορίες με τρόπο κατανεμημένο και ανθεκτικό.

Σε επιχειρήσεις Command and Control, η αξιοπιστία της επικοινωνίας είναι ζήτημα ζωής και θανάτου. Η παραδοσιακή εξάρτηση από δορυφορικά δίκτυα ή επίγειες υποδομές αποδείχθηκε ανεπαρκής σε περιβάλλοντα έντονου ηλεκτρονικού πολέμου ή μετά από επιθέσεις σε υποδομές. Τα UAVs μπορούν να γεφυρώσουν αυτά τα κενά, δημιουργώντας τοπικά δίκτυα που διασφαλίζουν τη συνέχεια της ροής πληροφοριών. Σε πρόσφατες ασκήσεις του NATO, UAVs χρησιμοποιήθηκαν για real-time μετάδοση εικόνας υψηλής ευκρίνειας από απομακρυσμένα πεδία μάχης, υποστηρίζοντας ταυτόχρονα επιχειρήσεις αναγνώρισης και τακτικής διοίκησης. Οι δυνατότητες αυτές αποδεικνύουν ότι τα UAVs δεν είναι απλώς επικουρικά μέσα, αλλά βασικό στοιχεία της τακτικής αρχιτεκτονικής επικοινωνιών [64].

Η ενσωμάτωσή τους σε δίκτυα ad hoc και mesh επεκτείνει ακόμη περισσότερο τις δυνατότητές τους. Ενώ τα παραδοσιακά MANETs περιορίζονται στην απόσταση και την ισχύ των επίγειων κόμβων, η χρήση UAVs ως εναέριων κόμβων δημιουργεί τρισδιάστατα δίκτυα που μπορούν να επεκταθούν γεωγραφικά με μοναδική ευκολία. Σενάρια με «σμήνη drones » επιδεικνύουν πώς πολλαπλά UAVs μπορούν να συνεργαστούν για να σχηματίσουν mesh δίκτυα υψηλής ανθεκτικότητας, τα οποία προσαρμόζονται δυναμικά σε απώλειες κόμβων ή σε εχθρικές παρεμβολές. Το πλεονέκτημα ενός τέτοιου συστήματος είναι ότι δεν υπάρχει κεντρικό σημείο αποτυχίας ακόμη και αν μερικά UAVs καταστραφούν, το δίκτυο συνεχίζει να λειτουργεί, ανακατευθύνοντας την κυκλοφορία μέσω εναλλακτικών διαδρομών.

Η πρακτική αξία των UAVs αποτυπώνεται σε ποικίλα επιχειρησιακά παραδείγματα. Σε πολεμικές επιχειρήσεις σε αστικά περιβάλλοντα, UAVs εξοπλισμένα με αισθητήρες έχουν

χρησιμοποιηθεί για την παροχή άμεσης εικόνας του πεδίου μάχης σε διοικητικά κέντρα, μειώνοντας δραστικά τον χρόνο απόκρισης. Σε αποστολές σε ερήμους ή ορεινές περιοχές, UAVs έχουν προσφέρει προσωρινή κάλυψη επικοινωνίας εκεί όπου καμία άλλη υποδομή δεν ήταν διαθέσιμη. Παράλληλα, σε ανθρωπιστικές αποστολές και επιχειρήσεις διάσωσης μετά από φυσικές καταστροφές, UAVs έδωσαν τη δυνατότητα δημιουργίας ad hoc δικτύων που επέτρεψαν τον συντονισμό σωστικών συνεργειών και την αποστολή κρίσιμων δεδομένων σε πραγματικό χρόνο [65].

Καθώς η τεχνολογία εξελίσσεται, οι δυνατότητες των UAVs εμπλουτίζονται με προηγμένα χαρακτηριστικά όπως edge computing, κρυπτογραφημένες ζεύξεις υψηλής ασφάλειας και αλγορίθμους μηχανικής μάθησης που βελτιώνουν την αποδοτικότητα πτήσης και τη διαχείριση πόρων. Το μέλλον τους διαγράφεται ακόμη πιο καθοριστικό, με έρευνες να εστιάζουν σε σμήνη UAVs που συνεργάζονται αυτόνομα, διαμορφώνοντας κατανεμημένα «έξυπνα» δίκτυα επικοινωνιών. Αυτές οι εξελίξεις δείχνουν ότι τα UAVs δεν θα είναι πλέον συμπληρωματικό εργαλείο, αλλά θεμελιώδης συνιστώσα των δικτύων μάχης επόμενης γενιάς, σε πλήρη συνέργεια με τα 5G/6G δίκτυα, τα γνωσιακά ραδιόφωνα και τις δορυφορικές επικοινωνίες [63].

Συνολικά, τα UAVs έχουν μετατραπεί σε κεντρικό στοιχείο των στρατιωτικών επικοινωνιών, με ρόλο που ξεπερνά την παραδοσιακή επιτήρηση. Αποτελούν «ιπτάμενους κόμβους» που εξασφαλίζουν την επιχειρησιακή συνέχεια, προσφέρουν κρίσιμα δεδομένα σε πραγματικό χρόνο και επεκτείνουν τη συνδεσιμότητα σε όλα τα επίπεδα της διοίκησης. Η στρατηγική τους αξία ενισχύεται συνεχώς, καθιστώντας τα αναπόσπαστο μέρος κάθε μελλοντικής αρχιτεκτονικής τακτικών επικοινωνιών.

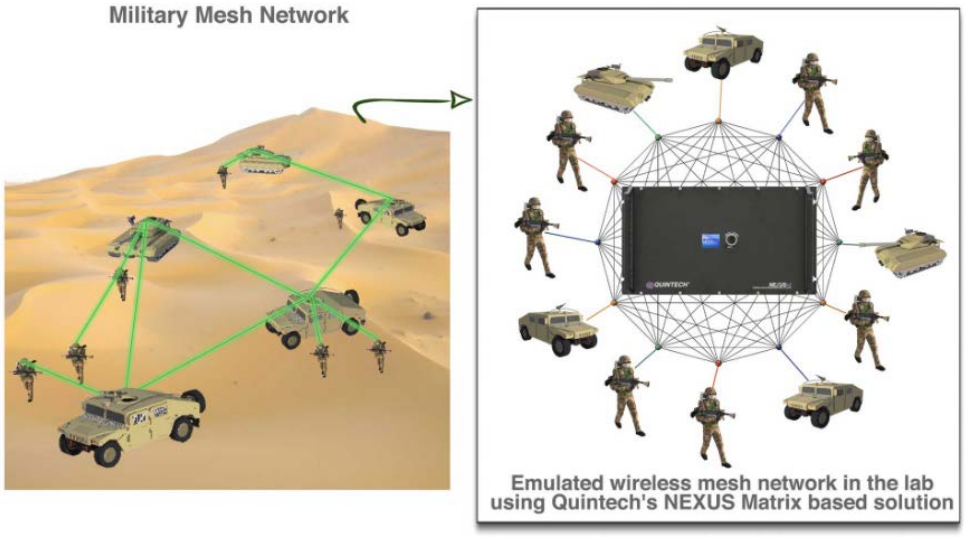
3.3.2 Tactical Mesh Networks

Τα Tactical Mesh Networks(TMNs) αποτελούν μια από τις πλέον κρίσιμες τεχνολογικές λύσεις για την υποστήριξη ευέλικτων, ανθεκτικών και αποκεντρωμένων στρατιωτικών επικοινωνιών. Σε αντίθεση με τα παραδοσιακά δίκτυα, τα οποία βασίζονται σε σταθερές υποδομές και κεντρικούς ελεγκτές, τα mesh δίκτυα οργανώνονται με κατανεμημένο τρόπο, όπου κάθε κόμβος λειτουργεί ταυτόχρονα ως πομπός, δέκτης και αναμεταδότης. Αυτό σημαίνει ότι η απώλεια ή αποκοπή ενός κόμβου δεν οδηγεί σε κατάρρευση του συστήματος, καθώς τα δεδομένα μπορούν να δρομολογηθούν μέσω εναλλακτικών διαδρομών. Η αρχιτεκτονική αυτή προσφέρει την απαραίτητη ανθεκτικότητα και αυτονομία που απαιτείται στο πεδίο μάχης, όπου οι συνθήκες αλλάζουν διαρκώς και οι επιθέσεις στον κυβερνοχώρο ή οι φυσικές καταστροφές μπορούν να θέσουν εκτός λειτουργίας κρίσιμες υποδομές [50].

Στο στρατιωτικό πλαίσιο, τα mesh δίκτυα θεωρούνται αναπόσπαστο τμήμα της φιλοσοφίας του network-centric warfare, όπου η πληροφορία πρέπει να διακινείται απρόσκοπτα ανάμεσα σε διαφορετικά επίπεδα διοίκησης και μάχης. Ένα Tactical Mesh Network μπορεί να υποστηρίξει την επικοινωνία σε πολλαπλές μορφές, από την φωνή και τα δεδομένα μέχρι βίντεο υψηλής ευκρίνειας και

τηλεμετρία UAVs. Το χαρακτηριστικό που τα ξεχωρίζει είναι η δυνατότητα αυτό-οργάνωσης(self-forming) και self-healing, ιδιότητες που καθιστούν τα δίκτυα ιδανικά για περιβάλλοντα όπου η σταθερή υποδομή είναι ανύπαρκτη ή έχει καταστραφεί [66].

Η βασική τεχνική αρχή των mesh δικτύων είναι ότι κάθε κόμβος επικοινωνεί με τους γειτονικούς του και σε περίπτωση που χαθεί ένας σύνδεσμος, το δίκτυο αυτόματα επαναδρομολογεί την κυκλοφορία μέσω άλλων κόμβων. Αυτή η πολλαπλότητα διαδρομών(multi-hop routing) ενισχύει δραστικά την ανθεκτικότητα. Παράλληλα, η κατανεμημένη φύση τους μειώνει τον κίνδυνο single point of failure, χαρακτηριστικό των παραδοσιακών κεντρικών αρχιτεκτονικών. Για τον λόγο αυτό, τα Tactical Mesh Networks θεωρούνται κατάλληλα για επιχειρήσεις ειδικών δυνάμεων, ανθρωπιστικές αποστολές αλλά και πολυεθνικές επιχειρήσεις όπου απαιτείται γρήγορη ανάπτυξη προσωρινών επικοινωνιακών δομών [67] Στο Σχήμα 19 παρουσιάζεται ένα παράδειγμα στρατιωτικού TMN, όπου οι στρατιώτες και τα οχήματα σχηματίζουν κατανεμημένο δίκτυο, καθώς και η αντίστοιχη εργαστηριακή προσομοίωσή του.



Σχήμα 19-Στρατιωτικό TMN και εργαστηριακή προσομοίωση[68]

Η πρακτική εφαρμογή των TMNs έχει αποδειχθεί σε πολλές στρατιωτικές ασκήσεις. Σε αστικά περιβάλλοντα, όπου τα κτίρια και οι παρεμβολές περιορίζουν δραστικά το σήμα, τα mesh δίκτυα επιτρέπουν τη δημιουργία ευέλικτων τοπικών υποδομών που εξασφαλίζουν επικοινωνία ακόμη και μεταξύ διασκορπισμένων ομάδων. Σε επιχειρήσεις σε μεγάλες αποστάσεις, mesh δίκτυα σε συνδυασμό με UAVs έχουν προσφέρει συνεχή κάλυψη, επιτρέποντας τη δικτύωση μονάδων που διαφορετικά θα ήταν αποκομμένες. Επιπλέον, η δυνατότητα ενσωμάτωσης SDRs και Cognitive Radios στα mesh δίκτυα επιτρέπει τη δυναμική προσαρμογή στο φάσμα, εξασφαλίζοντας ότι η επικοινωνία παραμένει αδιάλειπτη ακόμη και σε συνθήκες τεχνολογικού πολέμου [64].

Τα Tactical Mesh Networks ενσωματώνουν τεχνολογίες Quality of Service(QoS) για την ιεράρχηση της κυκλοφορίας δεδομένων. Ένα μήνυμα που αφορά μια κρίσιμη εμπλοκή στο πεδίο μάχης πρέπει να δρομολογηθεί με προτεραιότητα έναντι διοικητικών πληροφοριών ή δεδομένων χαμηλής σημασίας. Με μηχανισμούς traffic shaping και resource allocation,τα TMNs εξασφαλίζουν ότι οι επικοινωνίες Command and Control έχουν την υψηλότερη προτεραιότητα, μειώνοντας δραστικά την καθυστέρηση και βελτιώνοντας τη λήψη αποφάσεων σε πραγματικό χρόνο [69].

Παράλληλα, τα mesh δίκτυα υποστηρίζουν την ενσωμάτωση ετερογενών συστημάτων. Στρατιωτικές επιχειρήσεις συχνά φέρουν μαζί δυνάμεις από διαφορετικά έθνη, με διαφορετικό εξοπλισμό και πρωτόκολλα. Μέσω των SDRs, τα mesh δίκτυα μπορούν να προσαρμόζονται ώστε να υποστηρίζουν πολλαπλά πρότυπα επικοινωνίας, διευκολύνοντας τη συνεργασία σε πολυεθνικό επίπεδο. Αυτή η διαλειτουργικότητα είναι κρίσιμη για το ΝΑΤΟ, το οποίο επενδύει στην ανάπτυξη συστημάτων Federated Mission Networking(FMN), τα οποία βασίζονται σε κατανεμημένα μοντέλα δικτύωσης με στοιχεία mesh.

Ωστόσο, τα TMN αντιμετωπίζουν και σημαντικές προκλήσεις. Η ενεργειακή κατανάλωση παραμένει κρίσιμο ζήτημα, καθώς οι κόμβοι, ιδίως όταν πρόκειται για UAVs ή φορητούς ασυρμάτους, έχουν περιορισμένη αυτονομία. Η συνεχής αναμετάδοση δεδομένων σε multi-hop περιβάλλοντα μπορεί να εξαντλήσει γρήγορα τους διαθέσιμους πόρους. Επιπλέον, το routing σε ταχέως μεταβαλλόμενες τοπολογίες παραμένει περίπλοκο, αλγόριθμοι που λαμβάνουν υπόψη τη ποιότητα σήματος, την κινητικότητα και τον φόρτο κίνησης βρίσκονται ακόμη υπό ανάπτυξη. Εξίσου σημαντικό είναι το ζήτημα της ασφάλειας, καθώς τα mesh δίκτυα είναι ευάλωτα σε επιθέσεις jamming, spoofing ή ακόμη και σε επιθέσεις routing manipulation, όπου εισάγονται ψευδείς κόμβοι με στόχο τη διατάραξη της κυκλοφορίας [70].

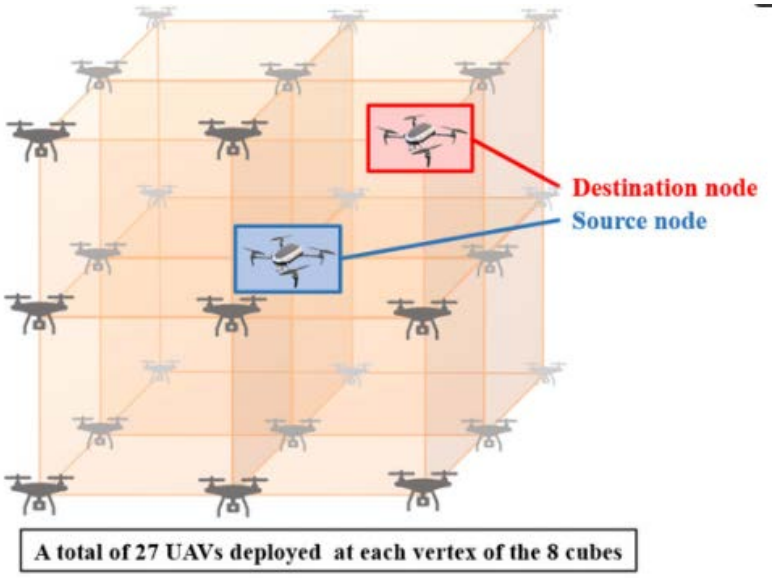
Συμπερασματικά, τα TMN αποτελούν μία από τις πιο υποσχόμενες τεχνολογίες για τις Ένοπλες Δυνάμεις, καθώς προσφέρουν έναν ευέλικτο, κατανεμημένο και ανθεκτικό μηχανισμό επικοινωνίας. Η δυνατότητα ταχείας ανάπτυξης χωρίς υποδομές, η αυτό-οργάνωση και η διαλειτουργικότητα με UAVs, SDRs και Cognitive Radios καθιστούν τα TMNs βασικό συστατικό της επόμενης γενιάς στρατιωτικών δικτύων. Παρά τις προκλήσεις, η συνεχής έρευνα και η ενσωμάτωση νέων τεχνολογιών(όπως AI-driven routing και 5G/6G integration) αναμένεται να ενισχύσουν ακόμη περισσότερο την αποτελεσματικότητά τους.

3.3.3 Ενσωμάτωση UAVs σε Mesh Networks

Η ενσωμάτωση των UAVs σε αρχιτεκτονικές Mesh δικτύων αποτελεί ένα από τα πιο καινοτόμα και υποσχόμενα πεδία στη σύγχρονη στρατιωτική επικοινωνία. Η δυνατότητα των UAVs να λειτουργούν ως κινητοί, εναέριοι κόμβοι μεταμορφώνει τα Mesh Networks από δίκτυα τοπικής εμβέλειας σε

τρισδιάστατες, πολυεπίπεδες υποδομές που μπορούν να καλύψουν τεράστιες γεωγραφικές περιοχές και να αντέξουν σε συνθήκες υψηλής απειλής.

Η βασική συνεισφορά των UAVs στα Mesh δίκτυα είναι ότι προσθέτουν την κάθετη διάσταση. Σε ένα παραδοσιακό Tactical Mesh Network, η κάλυψη περιορίζεται από την ισχύ των επίγειων κόμβων και από τα φυσικά εμπόδια. Με την εισαγωγή UAVs, το δίκτυο αποκτά εναέριους κόμβους που παρακάμπτουν τα εμπόδια αυτά, προσφέροντας «οπτική γραμμή» επικοινωνίας και διευρύνοντας σημαντικά την ακτίνα δράσης. Στην πράξη, αυτό σημαίνει ότι ακόμη και σε ένα πολύπλοκο αστικό περιβάλλον ή σε ορεινές περιοχές, η επικοινωνία μεταξύ μονάδων μπορεί να διατηρείται απρόσκοπτα μέσω UAV relays [71]. Ένα παράδειγμα τρισδιάστατου στρατιωτικού mesh δικτύου UAVs παρουσιάζεται στο Σχήμα 20.



Σχήμα 20-Τρισδιάστατο στρατιωτικό mesh δίκτυο UAVs[72]

Η ενσωμάτωση UAVs σε Mesh Networks έχει δοκιμαστεί εκτενώς σε ασκήσεις του NATO και σε πειραματικές πλατφόρμες των ΗΠΑ, όπου UAVs με ενσωματωμένα SDRs συνδέθηκαν με επίγειους κόμβους για την δημιουργία υβριδικών ad hoc δικτύων. Τα αποτελέσματα έδειξαν ότι ακόμη και με μικρό αριθμό UAVs, η κάλυψη και η σταθερότητα του δικτύου αυξήθηκαν σημαντικά. Ιδιαίτερα σημαντική είναι η δυνατότητα των UAVs να λειτουργούν ως ενδιάμεσοι κόμβοι πολλαπλών hops, δημιουργώντας μια αρχιτεκτονική όπου τα δεδομένα μεταφέρονται σε μεγάλες αποστάσεις με ελάχιστη απώλεια ποιότητας.

Εκτός από την αύξηση της εμβέλειας, τα UAVs ενισχύουν την ανθεκτικότητα των Mesh δικτύων. Σε περίπτωση που ένας επίγειος κόμβος τεθεί εκτός λειτουργίας, το UAV μπορεί να αναπροσαρμόσει τη θέση του ώστε να καλύψει το κενό, ενισχύοντας έτσι τις self-healing ιδιότητες του δικτύου. Αυτό είναι ιδιαίτερα κρίσιμο σε επιχειρήσεις ειδικών δυνάμεων, όπου η απώλεια ακόμη και ενός κόμβου

μπορεί να οδηγήσει σε επιχειρησιακή αποτυχία. Σε αποστολές διάσωσης, UAVs έχουν χρησιμοποιηθεί για να διατηρήσουν τη δικτύωση μεταξύ αποκομμένων ομάδων μέχρι να αποκατασταθούν οι υποδομές [65].

Η συμβολή των UAVs δεν περιορίζεται μόνο στην επικοινωνία, αλλά και στη διαχείριση φάσματος και δεδομένων. Με την υποστήριξη γνωστικών λειτουργιών, τα UAVs μπορούν να ανιχνεύουν παρεμβολές και να ανακατανέμουν δυναμικά το φάσμα, εξασφαλίζοντας ότι οι κρίσιμες επικοινωνίες έχουν πάντα την απαραίτητη ποιότητα υπηρεσίας. Παράλληλα, με την ενσωμάτωση τεχνολογιών edge computing, τα UAVs μπορούν να επεξεργάζονται τοπικά δεδομένα, όπως εικόνες από αισθητήρες ή βιομετρικές μετρήσεις στρατιωτών, μειώνοντας την ανάγκη για μετάδοση μεγάλων όγκων πληροφορίας και βελτιώνοντας τον χρόνο απόκρισης.

Η χρήση UAVs σε Mesh Networks έχει βρει εφαρμογή τόσο σε πολεμικές όσο και σε ανθρωπιστικές επιχειρήσεις. Σε πεδία μάχης, UAVs χρησιμοποιήθηκαν για real-time streaming εικόνας από απομακρυσμένες περιοχές, υποστηρίζοντας την άμεση λήψη αποφάσεων από τα διοικητικά κέντρα. Σε επιχειρήσεις μετά από φυσικές καταστροφές, UAVs σε mesh αρχιτεκτονική επέτρεψαν τη δικτύωση σωστικών συνεργειών που επιχειρούσαν σε περιοχές χωρίς τηλεπικοινωνιακή κάλυψη, όπως συνέβη σε σεισμούς και πλημμύρες [63].

Συνολικά, η ενσωμάτωση UAVs σε Mesh Networks μετασχηματίζει τον τρόπο με τον οποίο αντιλαμβανόμαστε τις τακτικές επικοινωνίες. Η δυνατότητα δημιουργίας κινητών, τρισδιάστατων, αυτό-οργανωμένων δικτύων με υψηλή ανθεκτικότητα και ευελιξία καθιστά τα συστήματα αυτά θεμέλιο λίθο του μελλοντικού network-centric warfare. Παρά τις προκλήσεις που σχετίζονται με την κατανάλωση ενέργειας, την ασφάλεια και την πολυπλοκότητα διαχείρισης, τα UAV-enabled Mesh Networks αναμένεται να αποτελέσουν βασικό εργαλείο στις στρατιωτικές επιχειρήσεις των επόμενων δεκαετιών.

3.3.4 Προκλήσεις και περιορισμοί

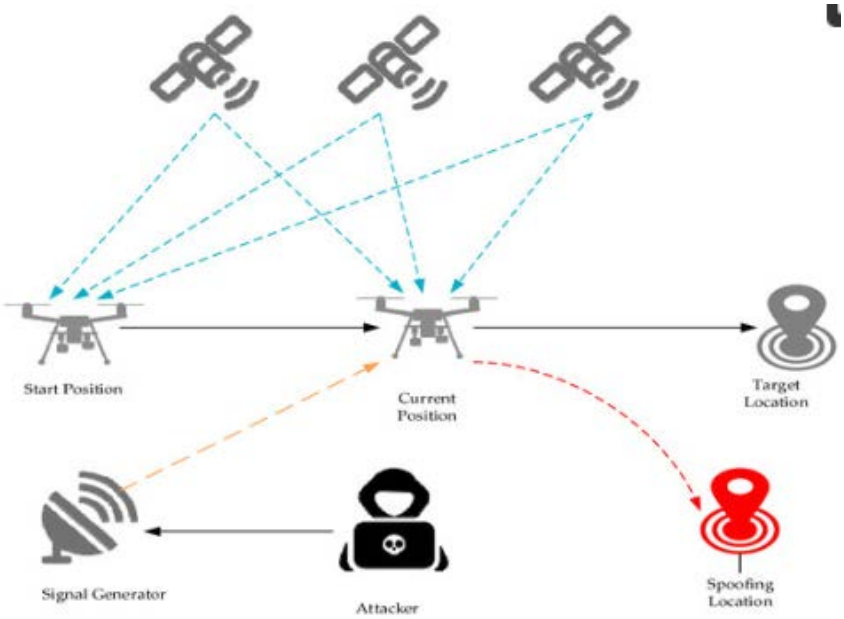
Παρά τα σημαντικά πλεονεκτήματα που προσφέρει η ενσωμάτωση UAVs σε Tactical Mesh Networks, η πρακτική εφαρμογή τους δεν είναι χωρίς δυσκολίες. Οι προκλήσεις που ανακύπτουν είναι πολυδιάστατες, περιλαμβάνοντας τεχνικούς, επιχειρησιακούς και στρατηγικούς περιορισμούς, οι οποίοι πρέπει να ξεπεραστούν ώστε τα δίκτυα αυτά να καταστούν πραγματικά αξιόπιστα στο πεδίο των επιχειρήσεων.

Μια από τις μεγαλύτερες προκλήσεις είναι η ενεργειακή αυτονομία των UAVs. Τα περισσότερα drones έχουν περιορισμένη διάρκεια πτήσης, που σπάνια ξεπερνά τη μία ώρα για τακτικές πληροφορίες. Όταν τα UAVs χρησιμοποιούνται ως αναμεταδότες σε mesh δίκτυα, η συνεχής μετάδοση και αναμετάδοση δεδομένων αυξάνει την κατανάλωση ενέργειας. Αυτό μειώνει την επιχειρησιακή τους αυτονομία και απαιτεί συχνή αντικατάσταση ή επαναφόρτιση, γεγονός που μπορεί να είναι δύσκολο ή

επικίνδυνο στο πεδίο μάχης [73]. Έρευνες επικεντρώνονται στην ανάπτυξη ενεργειακά αποδοτικών πρωτοκόλλων routing και τεχνικών wireless power transfer, ωστόσο η επίλυση του προβλήματος παραμένει κρίσιμο ζητούμενο.

Ένα άλλο σημαντικό ζήτημα είναι η πολυπλοκότητα της δρομολόγησης σε δυναμικά περιβάλλοντα. Σε ένα UAV-Mesh δίκτυο, οι κόμβοι δεν είναι στατικοί αλλά κινούνται συνεχώς, αλλάζοντας την τοπολογία του δικτύου. Αυτό καθιστά το routing ιδιαίτερα περίπλοκο, απαιτούνται εξελιγμένοι αλγόριθμοι που λαμβάνουν υπόψη όχι μόνο την απόσταση, αλλά και παραμέτρους όπως η κατανάλωση ενέργειας, η ποιότητα καναλιού και η πιθανότητα απώλειας σύνδεσης [74]. Παρά τη σημαντική πρόοδο σε routing πρωτόκολλα όπως OLSR και AODV, η αποτελεσματικότητά τους περιορίζεται σε ταχέως μεταβαλλόμενες τοπολογίες, γεγονός που δημιουργεί προβλήματα αξιοπιστίας.

Η ασφάλεια αποτελεί ίσως την μεγαλύτερη πρόκληση. Τα UAVs ως εναέριοι κόμβοι, είναι ιδιαίτερα εκτεθειμένα σε επιθέσεις jamming,spoofing και hijacking. Έχουν καταγραφεί περιστατικά όπου UAVs παραπλανήθηκαν μέσω GPS spoofing, με αποτέλεσμα να χαθούν ή να πέσουν σε εχθρικά χέρια [75]. Επιπλέον, τα mesh δίκτυα είναι ευάλωτα σε επιθέσεις τύπου Sybil και blockhole, όπου κακόβουλοι κόμβοι εισάγονται στο δίκτυο για να εκτρέψουν ή να καταστρέψουν την κυκλοφορία. Η ανάπτυξη ισχυρών μηχανισμών κρυπτογράφησης, ελέγχου ποιότητας και ανίχνευσης εισβολών είναι απαραίτητη για την ασφαλή λειτουργία των UAV-Mesh δικτύων. Η απειλή του GPS spoofing αποτυπώνεται στο Σχήμα 21, όπου φαίνεται η παραπλάνηση ενός UAV μέσω ψευδούς σήματος θέσης.



Σχήμα 21- Επίθεση GPS spoofing[76]

Πέρα από τα τεχνικά ζητήματα, υπάρχουν και κανονιστικοί και επιχειρησιακοί περιορισμοί. Η χρήση UAVs σε στρατιωτικές επιχειρήσεις απαιτεί αυστηρό συντονισμό για την αποφυγή συγκρούσεων

στον εναέριο χώρο και την εναρμόνιση με διεθνείς κανονισμούς. Σε πολυεθνικές επιχειρήσεις, όπου UAVs διαφορετικών χωρών επιχειρούν ταυτόχρονα, η απουσία ενοποιημένων προτύπων για την επικοινωνία και τον έλεγχο τους περιπλέκει περαιτέρω την κατάσταση.

Τέλος, πρέπει να ληφθεί υπόψη η υπολογιστική πολυπλοκότητα. Η ενσωμάτωση λειτουργιών όπως Cognitive Radios και edge computing στα UAVs ενισχύει τις δυνατότητες τους, αλλά απαιτεί ισχυρό υλικό και αυξάνει το βάρος και την κατανάλωση ενέργειας. Παράλληλα, οι αλγόριθμοι μηχανικής μάθησης που χρησιμοποιούνται για την αυτόνομη λήψη αποφάσεων δημιουργούν νέα σημεία ευπάθειας, καθώς μπορεί να γίνουν στόχος adversarial attacks που αλλοιώνουν τα δεδομένα εκπαίδευσης.

Συμπερασματικά, οι προκλήσεις των UAV-Mesh δικτύων καταδεικνύουν ότι η τεχνολογία, αν και ώριμη σε πειραματικό επίπεδο, δεν έχει ακόμη φτάσει στο σημείο πλήρους επιχειρησιακής αξιοποίησης. Η επίλυση των ζητημάτων που αφορούν την ενέργεια, το routing, την ασφάλεια και την τυποποίηση θα καθορίσει το κατά πόσο τα δίκτυα αυτά θα καταστούν θεμέλιο της μελλοντικής αρχιτεκτονικής στρατιωτικών επικοινωνιών. Παράλληλα, οι επενδύσεις σε έρευνα και ανάπτυξη από στρατιωτικούς οργανισμούς και ακαδημαϊκά ιδρύματα δείχνουν ότι η διεθνής κοινότητα αναγνωρίζει τις δυνατότητες αυτής της τεχνολογίας, ενισχύοντας την προοπτική να εξελιχθεί σε κρίσιμο συστατικό του network-centric warfare.

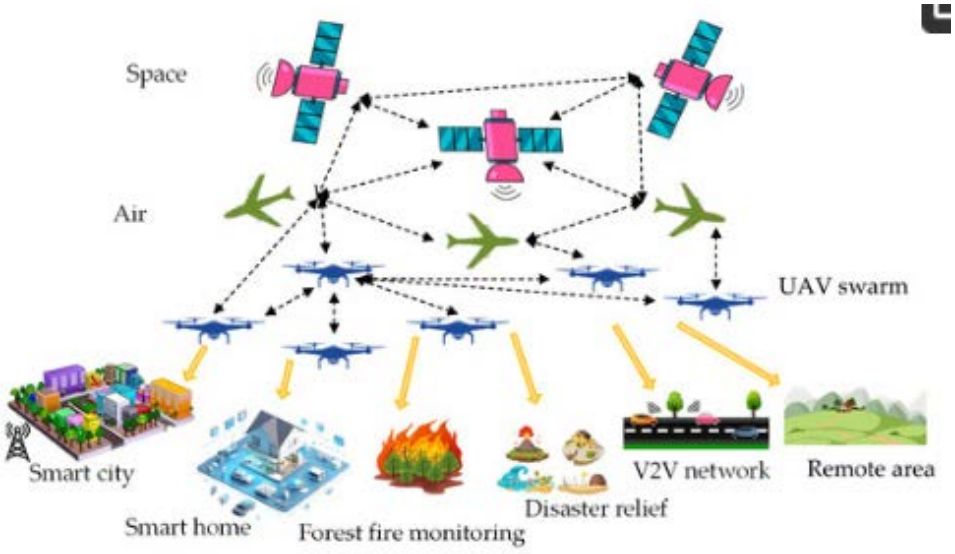
3.3.5 Μελλοντικές κατευθύνσεις

Η ταχεία εξέλιξη της τεχνολογίας UAVs και των Tactical Mesh Networks υποδεικνύει ότι οι δυνατότητες που αξιοποιούνται σήμερα αντιπροσωπεύουν μόνο την αρχή. Οι μελλοντικές κατευθύνσεις εστιάζουν στην συνδυαστική αξιοποίηση τεχνητής νοημοσύνης, νέων προτύπων επικοινωνίας και συνεργατικών αρχιτεκτονικών, με στόχο τη δημιουργία ευφυών, ανθεκτικών και αυτόνομων δικτύων μάχης.

Μία από τις υποσχόμενες εξελίξεις είναι η ανάπτυξη σμηνών UAVs(UAV swarms) όπου δεκάδες ή εκατοντάδες drones συνεργάζονται αυτόνομα με βάση αποκεντρωμένους αλγορίθμους. Τα σμήνη αυτά μπορούν να σχηματίζουν δυναμικά mesh δίκτυα, να καλύπτουν τεράστιες γεωγραφικές περιοχές και να αναπροσαρμόζονται σε πραγματικό χρόνο σε απώλειας ή παρεμβολές. Η ενσωμάτωση τεχνητής νοημοσύνης επιτρέπει στα UAVs να λαμβάνουν συλλογικές αποφάσεις, βελτιστοποιώντας τη δρομολόγηση δεδομένων και τον καταμερισμό πόρων. Η προοπτική αυτή μετατρέπει τα UAV-Mesh δίκτυα σε «ζωντανά οικοσυστήματα», όπου η ανθεκτικότητα και η προσαρμοστικότητα προκύπτουν από τη συνεργασία πολλών αυτόνομων οντοτήτων [77]. Ορισμένες τυπικές εφαρμογές και διατάξεις σμηνών UAV παρουσιάζονται στο Σχήμα 22.

Παράλληλα, η ενοποίηση με τα δίκτυα 5G και μελλοντικά 6G αναμένεται να προσδώσει νέα δυναμική. Οι χαμηλές καθυστερήσεις(sub-millisecond latency), η μαζική διασύνδεση(massive MIMO)

και οι δυνατότητες slicing καθιστούν το 5G/6G ιδανικό υπόβαθρο για τη διαχείριση UAV-Mesh δικτύων. Η υιοθέτηση Non-Terrestrial Networks(NTNs) θα επιτρέψει τη συνεργασία UAVs με δορυφορικές επικοινωνίες και High Altitude Platforms(HAPs), δημιουργώντας πολυεπίπεδα υβριδικά δίκτυα που θα καλύπτουν από το έδαφος μέχρι την ανώτερη στρατόσφαιρα [64].



Σχήμα 22-Ορισμένες τυπικές εφαρμογές σμηνών UAV [78]

Εξίσου σημαντική κατεύθυνση είναι η ενσωμάτωση γνωστικών λειτουργιών και τεχνητής νοημοσύνης στα UAVs. Τα Cognitive Radios που φέρουν μπορούν να εκτελούν spectrum sensing και να προσαρμόζονται αυτόματα σε παρεμβολές, ενώ η χρήση machine learning αλγορίθμων θα επιτρέπει την πρόβλεψη μελλοντικών αναγκών επικοινωνίας και την προληπτική αναδιάταξη του δικτύου. Με αυτόν τον τρόπο, οι επικοινωνίες θα αποκτήσουν χαρακτηριστικά αυτό-βελτίωσης και πρόβλεψης, μειώνοντας τον χρόνο απόκρισης και αυξάνοντας την επιχειρησιακή αποτελεσματικότητα [56].

Μία ακόμη προοπτική αφορά την ανάπτυξη υβριδικών αρχιτεκτονικών Mesh-MANET-SATCOM. Τα UAVs θα μπορούν να συνδέονται ταυτόχρονα σε mesh δίκτυα με άλλους UAVs και MANETs με επίγειες μονάδες, ενώ παράλληλα θα λειτουργούν ως γέφυρες με δορυφορικά δίκτυα. Αυτό δημιουργεί ένα πολυεπίπεδο πλέγμα επικοινωνιών, όπου κάθε τεχνολογία ενισχύει τις υπόλοιπες, μειώνοντας τον κίνδυνο συνολικής κατάρρευσης [79].

Τέλος, οι μελλοντικές κατευθύνσεις δεν περιορίζονται μόνο στο στρατιωτικό πεδίο αλλά επεκτείνονται και σε ανθρωπιστικές και πολιτικές εφαρμογές. Τα UAV-Mesh δίκτυα μπορούν να χρησιμοποιηθούν σε αποστολές διάσωσης, στην πολιτική προστασία ή στην υποστήριξη κρίσιμων υποδομών μετά από φυσικές καταστροφές. Η διπλή τους χρήση ενισχύει την αποδοχή τους και επιταχύνει την ανάπτυξη, καθώς οι επενδύσεις στον πολιτικό τομέα συχνά δημιουργούν τεχνολογίες που επαναχρησιμοποιούνται στο στρατιωτικό [80].

Συνοψίζοντας, οι μελλοντικές κατευθύνσεις για τα UAV-Mesh δίκτυα κινούνται σε τέσσερις βασικούς άξονες. Οι εξελίξεις αυτές αναμένεται να καθορίσουν την επόμενη γενιά στρατιωτικών επικοινωνιών, καθιστώντας τα UAV-Mesh δίκτυα όχι απλώς υποστηρικτικά εργαλεία αλλά τον πυρήνα της μελλοντικής επιχειρησιακής δικτύωσης.

3.4 Δορυφορικές επικοινωνίες και tactical SATCOM

Οι δορυφορικές επικοινωνίες αποτελούν διαχρονικά έναν από τους βασικότερους πυλώνες των στρατιωτικών τηλεπικοινωνιών, προσφέροντας δυνατότητα κάλυψης σε παγκόσμιο επίπεδο και εξασφαλίζοντας τη συνδεσιμότητα από τους περιορισμούς του γεωγραφικού περιβάλλοντος. Σε αντίθεση με τα επίγεια ή εναέρια δίκτυα, τα οποία συχνά εξαρτώνται από την εγγύτητα και την τοπική υποδομή, τα δορυφορικά συστήματα παρέχουν συνεχή επικοινωνία σε στρατηγικό, επιχειρησιακό και τακτικό επίπεδο. Η συμβολή τους είναι καθοριστική τόσο σε συμβατικές πολεμικές επιχειρήσεις όσο και σε αποστολές διατήρησης της ειρήνης, ανθρωπιστικής βοήθειας ή αντιμετώπισης φυσικών καταστροφών.

Το Tactical SATCOM, δηλαδή οι τακτικές εφαρμογές των δορυφορικών επικοινωνιών, εστιάζουν στην υποστήριξη μονάδων που επιχειρούν σε απομακρυσμένα ή εχθρικά περιβάλλοντα, εκεί που οι παραδοσιακές υποδομές είναι ανύπαρκτες ή έχουν καταστραφεί. Η εξέλιξη των δορυφορικών συστημάτων, από τους γεωστατικούς δορυφόρους έως τις σύγχρονες χαμηλής τροχιάς(LEO) συστοιχίες, έχει διευρύνει δραστικά τις δυνατότητες του στρατεύματος, προσφέροντας χαμηλότερη καθυστέρηση, μεγαλύτερη χωρητικότητα και αυξημένη ανθεκτικότητα έναντι παρεμβολών.

Η σημασία των δορυφορικών επικοινωνιών στηρίζεται στην ικανότητά τους να λειτουργούν ως «συνδετικός ιστός» μεταξύ διαφορετικών επιπέδων δικτύωσης, από τα στρατηγεία μέχρι τους μεμονωμένους στρατιώτες στο πεδίο μάχης. Το παρόν κεφάλαιο εξετάζει το ρόλο και τις τεχνολογίες των στρατιωτικών SATCOM, αναλύει τα πλεονεκτήματα και τις επιχειρησιακές δυνατότητές τους, παρουσιάζει τους περιορισμούς και τις ευπάθειές τους και τέλος αναφέρεται στις μελλοντικές τάσεις που διαμορφώνουν την εξέλιξη του συγκεκριμένου τομέα.

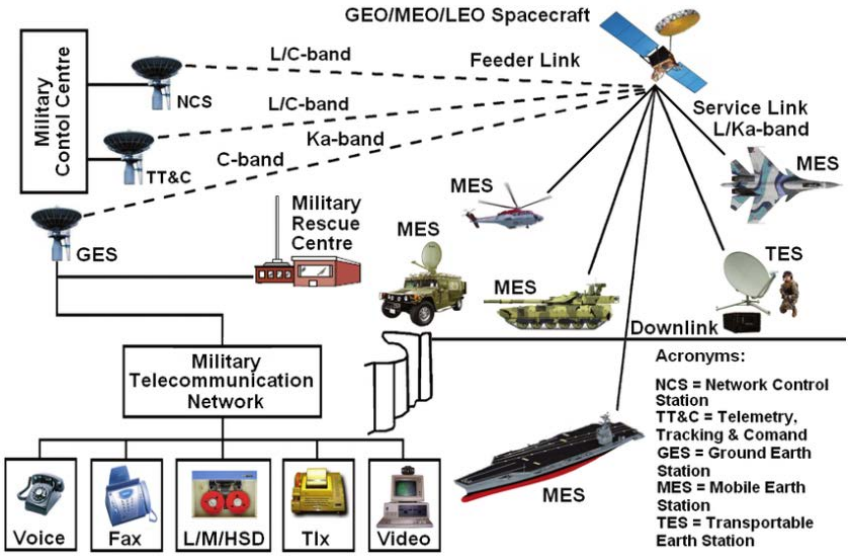
3.4.1 Ο ρόλος των δορυφορικών επικοινωνιών στις στρατιωτικές επιχειρήσεις

Οι δορυφορικές επικοινωνίες αποτελούν θεμέλιο λίθο των στρατιωτικών τηλεπικοινωνιακών υποδομών, καθώς εξασφαλίζουν παγκόσμια κάλυψη και συνεχή διαθεσιμότητα ανεξάρτητα από το γεωγραφικό ή επιχειρησιακό περιβάλλον. Σε αντίθεση με τα επίγεια και εναέρια δίκτυα, τα οποία περιορίζονται από φυσικά εμπόδια και απαιτούν τοπική υποδομή, τα δορυφορικά συστήματα προσφέρουν τη δυνατότητα επικοινωνίας πέρα από τη γραμμή του ορίζοντα, γεγονός που τα καθιστά ζωτικής σημασίας σε κάθε στρατιωτική επιχείρηση μεγάλης κλίμακας [80]. Η δομή και η λειτουργία ενός στρατιωτικού δικτύου SATCOM που παρέχει συνδεσιμότητα σε ξηρά, θάλασσα και αέρα μέσω

GEO/MEO/LEO δορυφόρων απεικονίζονται στο Σχήμα 23, επιδεικνύοντας πως τα δορυφορικά στοιχεία γεφυρώνουν διαφορετικά θέατρα επιχειρήσεων.

Η σημασία τους αναδεικνύεται ιδιαίτερα στο πεδίο της διοίκησης και ελέγχου. Η λήψη αποφάσεων σε στρατιωτικό περιβάλλον προϋποθέτει αδιάλειπτη ροή αξιόπιστων πληροφοριών, ώστε οι εντολές να μεταφέρονται έγκαιρα στις απομακρυσμένες μονάδες και τα δεδομένα από αισθητήρες,UAVs ή επίγειους σταθμούς να επιστρέφουν άμεσα στο στρατηγείο. Μέσω των δορυφορικών δικτύων διαμορφώνεται μια ενιαία εικόνα της επιχειρησιακής κατάστασης, η οποία ενισχύει την ταχύτητα και την ακρίβεια της διαδικασίας λήψης αποφάσεων και μειώνει τον κίνδυνο καθυστερήσεων που θα μπορούσαν να αποβούν μοιραίες σε συνθήκες υψηλής έντασης.

Η στρατηγική τους αξία εκτείνεται και στη δυνατότητα γεφύρωσης διαφορετικών θεάτρων επιχειρήσεων. Οι χερσαίες, ναυτικές και αεροπορικές δυνάμεις μπορούν να επιχειρούν διασκορπισμένες σε μεγάλες αποστάσεις, αλλά παραμένουν διασυνδεδεμένες μέσω των δορυφόρων. Αυτή η δυνατότητα «διασποράς με δικτύωση» επιτρέπει στις ένοπλες δυνάμεις να διατηρούν υψηλά επίπεδα ευελιξίας και επιχειρησιακής αυτονομίας, χωρίς να θυσιάζουν τον συντονισμό και την κεντρική εποπτεία.



Σχήμα 23-Στρατιωτικό δίκτυο SATCOM με συνδεσιμότητα ξηράς, θάλασσας και αέρα μέσω GEO/MEO/LEO δορυφόρων[81]

Η συνεισφορά των δορυφορικών επικοινωνιών είναι εξίσου καθοριστική σε τακτικό επίπεδο. Ειδικές δυνάμεις που επιχειρούν σε εχθρικό έδαφος, αποστολές επιτήρησης σε θαλάσσια περιβάλλοντα ή ανθρωπιστικές επιχειρήσεις σε περιοχές όπου οι υποδομές έχουν καταστραφεί βασίζονται στην ύπαρξη SATCOM για να διατηρούν επικοινωνία σε πραγματικό χρόνο. Η δυνατότητα παροχής ευρυζωνικών υπηρεσιών, όπως μετάδοση βίντεο υψηλής ευκρίνειας και δεδομένων

αναγνώρισης, ενισχύει την επιχειρησιακή εικόνα και καθιστά τα δορυφορικά συστήματα αναντικατάστατα σε σύγχρονα σενάρια μάχης.

Παράλληλα, τα δορυφορικά δίκτυα αποτελούν αναπόσπαστο κρίκο στην ανάπτυξη του IoMT. Η ολοένα αυξανόμενη διασύνδεση αισθητήρων, στρατιωτών, οχημάτων και UAVs απαιτεί μια υποδομή ικανή να μεταφέρει τεράστιους όγκους δεδομένων σε πραγματικό χρόνο. Τα SATCOM λειτουργούν ως γέφυρα που συνδέει τα τοπικά ad hoc δίκτυα με τις κεντρικές δομές διοίκησης, επιτρέποντας τη συνεχή ροή πληροφοριών και ενισχύοντας την επιχειρησιακή αποτελεσματικότητα.

Η αξία των δορυφορικών επικοινωνιών δεν περιορίζεται στο καθαρά στρατιωτικό πλαίσιο. Σε αποστολές πολιτικής προστασίας, ειρηνευτικές επιχειρήσεις ή διαχείριση φυσικών καταστροφών, το SATCOM παρέχει τον αναγκαίο συντονισμό ανάμεσα σε διεθνείς οργανισμούς, στρατιωτικές δυνάμεις και ανθρωπιστικές αποστολές. Ο διττός χαρακτήρας αυτής της τεχνολογίας, ως εργαλείου στρατιωτικής ισχύος αλλά και μέσου υποστήριξης κρίσιμων πολιτικών λειτουργιών, επιβεβαιώνει τη στρατηγική της σημασία.

Συνολικά, οι δορυφορικές επικοινωνίες αποτελούν αναπόσπαστο στοιχείο του δόγματος του δικτυοκεντρικού πολέμου. Η ικανότητά τους να εξασφαλίζουν στρατηγική συνδεσιμότητα, να υποστηρίζουν την αποτελεσματική διοίκηση και έλεγχο και να παρέχουν επιχειρησιακή συνέχεια σε αντίξοες συνθήκες καταδεικνύει ότι η παρουσία τους δεν είναι απλώς χρήσιμη, αλλά απολύτως απαραίτητα για τις σύγχρονες και μελλοντικές ένοπλες συγκρούσεις.

3.4.2 Τεχνολογίες και αρχιτεκτονικές Tactical SATCOM

Η τεχνολογική αρχιτεκτονική των δορυφορικών επικοινωνιών έχει εξελιχθεί ραγδαία τις τελευταίες δεκαετίες, προσαρμοζόμενη στις αυξανόμενες απαιτήσεις των στρατιωτικών επιχειρήσεων. Οι παραδοσιακές γεωστατικές πλατφόρμες(GEO) εξακολουθούν να αποτελούν τη βάση της στρατιωτικής υποδομής, ωστόσο νέες προσεγγίσεις όπως οι μεσαίες(MEO) και χαμηλές τροχιές(LEO) εμπλουτίζουν το επιχειρησιακό φάσμα, προσφέροντας μικρότερη καθυστέρηση και μεγαλύτερη ανθεκτικότητα σε παρεμβολές.

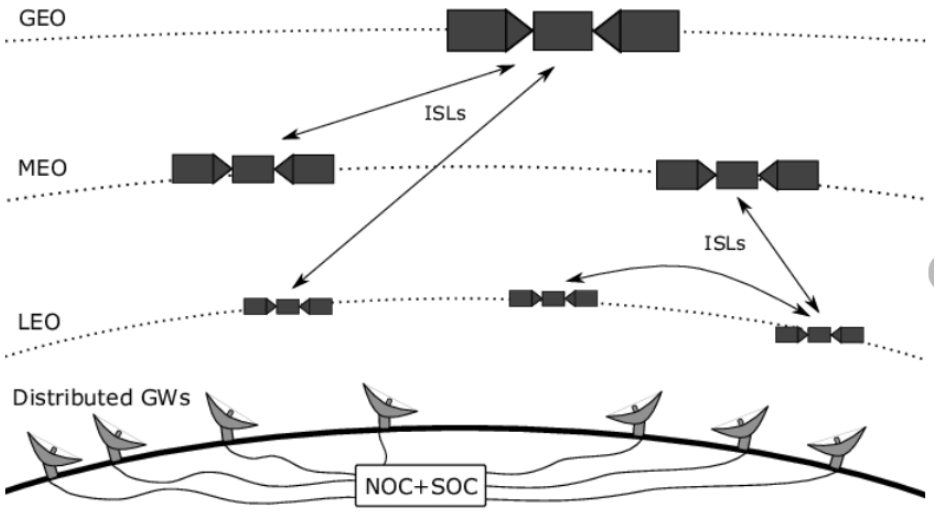
Οι γεωστατικοί δορυφόροι(GEO), τοποθετημένοι σε ύψος περίπου 36.000 χιλιομέτρων, παρέχουν συνεχή κάλυψη κλίμακας, καλύπτοντας γεωγραφικές περιοχές ίσες με ολόκληρες ηπείρους. Το πλεονέκτημά τους είναι η σταθερότητα και η δυνατότητα συνεχούς επικοινωνίας με επίγειους σταθμούς χωρίς την ανάγκη συνεχούς παρακολούθησης τροχιάς. Ωστόσο, η μεγάλη απόσταση συνεπάγεται υψηλή καθυστέρηση , γεγονός που αποτελεί σοβαρό μειονέκτημα σε εφαρμογές που απαιτούν πραγματικό χρόνο, όπως ο τηλεχειρισμός UAVs ή η δικτυοκεντρική μάχη.

Οι δορυφόροι μεσαίας τροχιάς(MEO) επιχειρούν σε υψόμετρα 5.000-20.000 χιλιομέτρων και αντιπροσωπεύουν έναν συμβιβασμό ανάμεσα στην κάλυψη και την καθυστέρηση. Παρότι απαιτούν

μεγαλύτερο αριθμό δορυφόρων για πλήρη γεωγραφική κάλυψη, προσφέρουν σαφώς χαμηλότερο latency και μπορούν να υποστηρίξουν επικοινωνίες υψηλής χωρητικότητας σε κρίσιμες περιοχές ενδιαφέροντος [82].

Οι δορυφόροι χαμηλής τροχιάς(LEO) βρίσκονται σε υψόμετρα 500-2.000 χιλιομέτρων και αποτελούν την πλέον δυναμική εξέλιξη του τομέα. Με πολύ μικρότερη καθυστέρηση, υψηλή ευελιξία και δυνατότητα σχηματισμούς mega-constellations, οι LEO δορυφόροι προσφέρουν επιχειρησιακά πλεονεκτήματα που δύσκολα μπορούν να αγνοηθούν. Παράδειγμα αποτελούν τα εμπορικά προγράμματα όπως το Starlink και το OneWeb, τα οποία ήδη εξετάζονται για στρατιωτικές εφαρμογές. Η χρήση LEO δορυφόρων επιτρέπει την υποστήριξη εφαρμογών υψηλής ευαισθησίας στον χρόνο, όπως η real-time μετάδοση δεδομένων από αισθητήρες πεδίου ή ο συντονισμός πυρών [83].

Η αρχιτεκτονική των Tactical SATCOM δεν περιορίζεται μόνο στο διαστημικό σκέλος αλλά επεκτείνεται και στα επίγεια τερματικά και φορητά συστήματα. Από μεγάλα σταθερά κέντρα επικοινωνιών έως μικρά, φορητά τερματικά που μπορούν να μεταφερθούν από στρατιώτες στο πεδίο, η τεχνολογία έχει εξελιχθεί ώστε να καλύπτει όλο το εύρος επιχειρησιακών αναγκών. Τα σύγχρονα φορητά SATCOM terminal μπορούν να στηθούν σε λίγα λεπτά, να συνδεθούν αυτόματα με το δορυφορικό δίκτυο και να προσφέρουν κρυπτογραφημένη επικοινωνία υψηλής ασφάλειας, ακόμη και σε συνθήκες ηλεκτρονικού πολέμου. Η συνολική αρχιτεκτονική ενός στρατιωτικού δικτύου SATCOM παρουσιάζεται στο Σχήμα 24.



Σχήμα 24-Πολυεπίπεδη αρχιτεκτονική στρατιωτικών SATCOM[84]

Ιδιαίτερο ενδιαφέρον παρουσιάζει η ενοποίηση των SATCOM με άλλες υποδομές επικοινωνίας, όπως τα επίγεια δίκτυα MANET και Mesh, τα SDRs και τα UAV-based communication nodes. Η διαλειτουργικότητα αυτή επιτρέπει τη δημιουργία υβριδικών δικτύων πολλαπλών επιπέδων, όπου οι δορυφόροι παρέχουν στρατηγική κάλυψη μεγάλης κλίμακας, ενώ τα επίγεια και εναέρια δίκτυα

εξασφαλίζουν ευελιξία σε τακτικό επίπεδο. Στην πράξη, αυτό σημαίνει ότι μια μονάδα ειδικών δυνάμεων μπορεί να επικοινωνεί απευθείας με το στρατηγείο μέσω SATCOM, ενώ παράλληλα να παραμένει διασυνδεδεμένη με γειτονικές ομάδες μέσω τοπικών MANETs.

Συμπερασματικά, οι τεχνολογίες και οι αρχιτεκτονικές του Tactical SATCOM εξελίσσονται προς ένα πολυεπίπεδο και υβριδικό οικοσύστημα επικοινωνιών, όπου οι διαφορετικοί τύποι δορυφορικών τροχιών και τερματικών συνεργάζονται με επίγειες και εναέριες υποδομές. Η μετάβαση αυτή αντανακλά τη στρατηγική ανάγκη για δίκτυα που να είναι ταυτόχρονα ανθεκτικά, ευέλικτα και ικανά να προσαρμόζονται στις ακραίες απαιτήσεις του σύγχρονου πεδίου μάχης.

3.4.3 Πλεονεκτήματα και επιχειρησιακές δυνατότητες

Οι δορυφορικές επικοινωνίες και ειδικότερα το Tactical SATCOM προσφέρουν ένα σύνολο πλεονεκτημάτων που τα καθιστούν αναπόσπαστο στοιχείο των σύγχρονων στρατιωτικών επιχειρήσεων. Το κυριότερο πλεονέκτημα είναι η παγκόσμια κάλυψη. Οι γεωστατικοί, μεσαίας και χαμηλής τροχιάς δορυφόροι συνεργάζονται για να εξασφαλίσουν συνεχή επικοινωνία σε οποιοδήποτε σημείο του πλανήτη, από τις πιο απομακρυσμένες ερήμους μέχρι τον Αρκτικό κύκλο. Αυτή η δυνατότητα είναι κρίσιμη σε επιχειρήσεις όπου οι επίγειες υποδομές είναι ανύπαρκτες ή κατεστραμμένες, όπως σε περιοχές πολέμου ή σε αποστολές αντιμετώπισης φυσικών καταστροφών.

Η δεύτερη σημαντική επιχειρησιακή δυνατότητα είναι η αξιοπιστία και η ανθεκτικότητα. Τα δορυφορικά συστήματα είναι λιγότερο ευάλωτα σε φυσικές καταστροφές, όπως σεισμοί ή πλημμύρες, σε σχέση με τις επίγειες υποδομές, ενώ μπορούν να συνεχίσουν να λειτουργούν ακόμη και σε περιπτώσεις μαζικών επιθέσεων στις τηλεπικοινωνιακές υποδομές μιας χώρας. Επιπλέον, με τη χρήση τεχνικών όπως spread spectrum, frequency hopping και ισχυρή κρυπτογράφηση, τα SATCOM συστήματα προσφέρουν αυξημένη ανθεκτικότητα σε παρεμβολές και ηλεκτρονικές επιθέσεις.

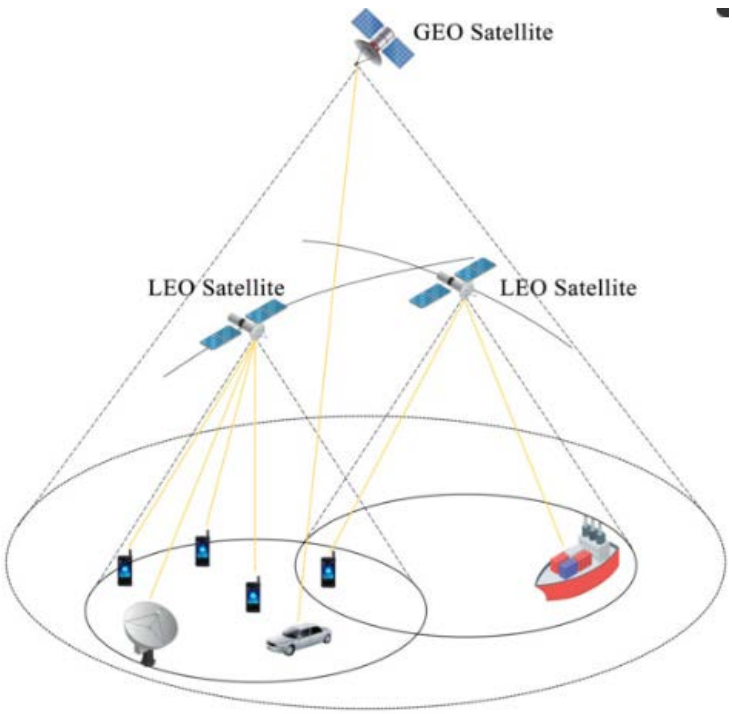
Ένα ακόμη πλεονέκτημα είναι η δυνατότητα διασύνδεσης πολλαπλών επιπέδων και πλατφορμών. Μέσω του SATCOM, στρατηγεία, επίγειες μονάδες, πλοία και αεροσκάφη μπορούν να μοιράζονται σε πραγματικό χρόνο δεδομένα που αφορούν την επιχειρησιακή εικόνα. Αυτή η ικανότητα διαλειτουργικότητας καθιστά το SATCOM βασικό πυλώνα της φιλοσοφίας του δικτυοκεντρικού πολέμου(network-centric warfare), όπου η πληροφορία θεωρείται ισχυρό πολλαπλασιαστικό στοιχείο ισχύος.

Τα σύγχρονα δορυφορικά συστήματα υποστηρίζουν επίσης υψηλής χωρητικότητας επικοινωνίες. Οι εξελίξεις στα LEO δίκτυα και οι τεχνικές πολλαπλών δεσμών(multi-beam) επιτρέπουν τη μετάδοση δεδομένων υψηλού όγκου με μειωμένη καθυστέρηση. Έτσι καθίσταται δυνατή η μετάδοση βίντεο σε πραγματικό χρόνο από UAVs, η άμεση ανταλλαγή δεδομένων αναγνώρισης ή ακόμη και η υποστήριξη εφαρμογών επαυξημένης πραγματικότητας (AR) και εικονικής πραγματικότητας(VR) στην εκπαίδευση και στο πεδίο μάχης.

Επιπλέον, το SATCOM ενισχύει την επιχειρησιακή ευελιξία. Σε περιβάλλοντα όπου οι δυνάμεις μετακινούνται συνεχώς, η χρήση φορητών τερματικών SATCOM προσφέρει στις μικρές μονάδες τη δυνατότητα να παραμένουν συνδεδεμένες με το κέντρο επιχειρήσεων. Ακόμη και σε απομονωμένες ομάδες ειδικών δυνάμεων, η πρόσβαση σε δορυφορικά δίκτυα παρέχει κρίσιμη επιχειρησιακή συνέχεια, αποτρέποντας την αποκοπή από το κύριο δίκτυο επικοινωνιών.

Τέλος, οι δορυφορικές επικοινωνίες συμβάλλουν σημαντικά στη διασύνδεση με τα εμπορικά δίκτυα. Σε ορισμένες περιπτώσεις, τα στρατιωτικά SATCOM μπορούν να λειτουργήσουν σε συνέργεια με εμπορικές δορυφορικές υπηρεσίες, επεκτείνοντας ακόμη περισσότερο τις δυνατότητες κάλυψης και ενισχύοντας την ανθεκτικότητα του συνολικού δικτύου. Αυτή η πρακτική αποκτά όλο και μεγαλύτερη σημασία καθώς οι σύγχρονες επιχειρήσεις βασίζονται σε υβριδικές αρχιτεκτονικές, οι οποίες συνδυάζουν στρατιωτικές και εμπορικές τεχνολογίες.

Συνολικά, τα πλεονεκτήματα των δορυφορικών επικοινωνιών αποτυπώνονται σε τέσσερις βασικές επιχειρησιακές δυνατότητες : παγκόσμια κάλυψη, αξιοπιστία και ανθεκτικότητα, υψηλή χωρητικότητα και ευελιξία στη διασύνδεση διαφορετικών πλατφορμών. Αυτά τα χαρακτηριστικά καθιστούν το SATCOM αναντικατάστατο εργαλείο στο σύγχρονο και μελλοντικό επιχειρησιακό περιβάλλον, ενισχύοντας την αποτελεσματικότητα των Ένοπλων Δυνάμεων και τη στρατηγική τους υπεροχή. Ένα παράδειγμα συνδεδεμένης λειτουργίας GEO και LEO δορυφόρων παρουσιάζεται στο Σχήμα 25.

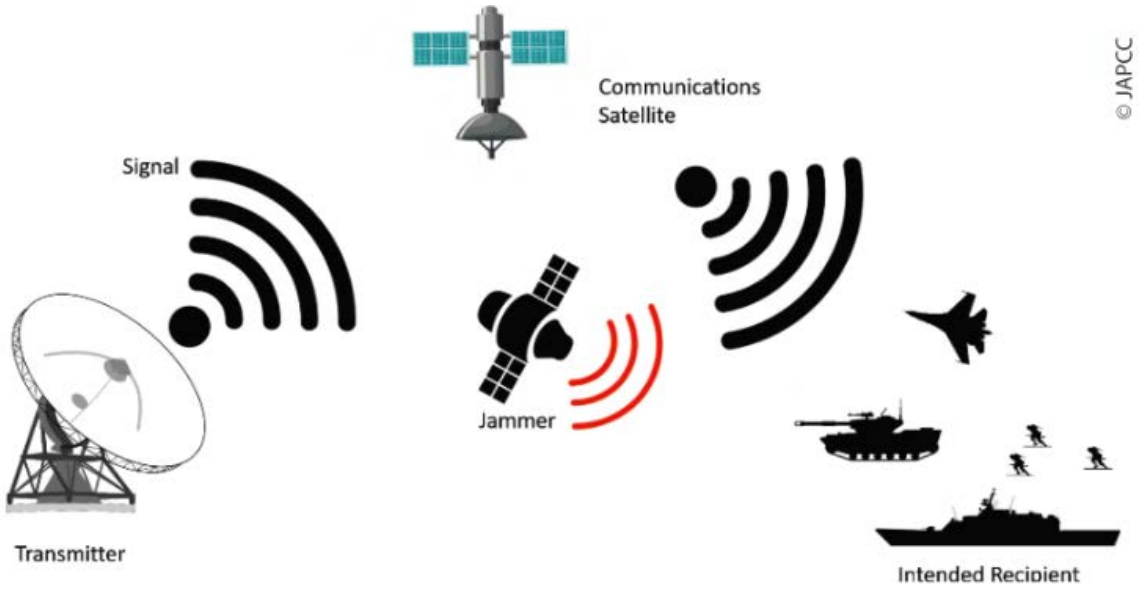


Σχήμα 25-Συνύπαρξη GEO και LEO δορυφόρων για υποστήριξη real-time και υψηλής χωρητικότητας υπηρεσιών σε επίγειους, ναυτικούς και UAV χρήστες[85]

3.4.4 Περιορισμοί και ευπάθειες των SATCOM

Παρά τη στρατηγική τους σημασία, τα δορυφορικά συστήματα επικοινωνιών παρουσιάζουν συγκεκριμένους περιορισμούς και ευπάθειες, οι οποίοι επηρεάζουν άμεσα την επιχειρησιακή τους αξιοπιστία. Ένα από τα πλέον χαρακτηριστικά προβλήματα είναι η καθυστέρηση μετάδοσης, ιδιαίτερα στις γεωστατικές πλατφόρμες(GEO). Το σήμα χρειάζεται να διανύσει απόσταση περίπου 72.000 χιλιομέτρων(πήγαινε-έλα), γεγονός που οδηγεί σε καθυστερήσεις της τάξης των 500-600ms. Σε εφαρμογές όπως ο τηλεχειρισμός UAVs ή η τακτική δικτυοκεντρική μάχη, η καθυστέρηση αυτή μπορεί να αποδειχθεί κρίσιμη.

Ένα δεύτερο σημαντικό ζήτημα είναι η ευπάθεια σε ηλεκτρονικό πόλεμο και εχθρικές παρεμβολές. Οι δορυφορικές επικοινωνίες μπορούν να στοχοποιηθούν από jamming, spoofing και παρεμβολές στο φάσμα. Ιδιαίτερα σε περιβάλλοντα με προηγμένους αντιπάλους, η ικανότητα του εχθρού να «τυφλώσει» ή να αποκόψει δορυφορικά κανάλια αποτελεί σοβαρή απειλή. Επιπλέον, η ίδια η υποδομή των δορυφόρων παραμένει εκτεθειμένη σε φυσικές και τεχνητές απειλές. Τα anti-satellite(ASAT) όπλα, που έχουν δοκιμαστεί από διάφορες χώρες, αποδεικνύουν ότι ακόμη και προηγμένα δίκτυα SATCOM μπορούν να τεθούν εκτός λειτουργίας με στοχευμένες επιθέσεις. Στο Σχήμα 26 φαίνεται η διακοπή σύνδεσης ενός δορυφόρου λόγω ισχυρών σημάτων jamming που εκπέμπονται από εχθρικό σταθμό.



Σχήμα 26-Παράδειγμα επίθεσης jamming σε δορυφορικές επικοινωνίες, όπου ο δορυφόρος διακόπτεται από σήματα παρεμβολής[86]

Η διαθεσιμότητα του φάσματος αποτελεί επίσης πρόκληση. Με την αυξανόμενη εξάρτηση από εμπορικά και στρατιωτικά δίκτυα, το φάσμα στις ζώνες Ku, Ka και X παρεμβολών. Αν και οι τεχνικές frequency hopping και beamforming προσφέρουν μερικές λύσεις, η διαχείριση του φάσματος

παραμένει κρίσιμο ζήτημα, ιδίως σε πολυεθνικές επιχειρήσεις όπου συνυπάρχουν διαφορετικά πρότυπα και τεχνολογίες [83].

Σημαντικός περιορισμός είναι επίσης το κόστος ανάπτυξης και συντήρησης. Η εκτόξευση, η λειτουργία και η αντικατάσταση δορυφόρων απαιτούν τεράστιους οικονομικούς πόρους, ενώ η τεχνολογία εξελίσσεται ταχύτερα από τον κύκλο ζωής ενός δορυφόρου(συχνά 15-20 έτη). Αυτό σημαίνει ότι οι στρατιωτικές δυνάμεις μπορεί να αναγκάζονται να χρησιμοποιούν παλαιότερες πλατφόρμες, λιγότερο ανθεκτικές σε σύγχρονες απειλές.

Πέρα από τα τεχνικά ζητήματα, υπάρχουν και κανονιστικοί και επιχειρησιακοί περιορισμοί. Η χρήση εμπορικών δορυφορικών υπηρεσιών για στρατιωτικούς σκοπούς δημιουργεί εξάρτηση από τρίτους παρόχους, με ζητήματα ασφάλειας και αξιοπιστίας. Σε πολυεθνικές αποστολές, η διαλειτουργικότητα δεν είναι πάντα διασφαλισμένη, καθώς διαφορετικές χώρες μπορεί να χρησιμοποιούν μη συμβατά δορυφορικά πρότυπα ή να επιβάλλουν περιορισμούς στη χρήση του φάσματος.

Τέλος, δεν πρέπει να παραβλέπεται η φυσική ευπάθεια των δορυφορικών επικοινωνιών. Η κοσμική ακτινοβολία, οι γεωμαγνητικές καταιγίδες και οι αλλαγές στην ατμόσφαιρα μπορούν να επηρεάσουν σημαντικά την ποιότητα του σήματος, ιδιαίτερα στις υψηλές συχνότητες(Ka και V bands). Αυτές οι φυσικές επιδράσεις είναι δύσκολο να προβλεφθούν και περιορίζουν τη διαθεσιμότητα των συστημάτων, ειδικά σε περιοχές υψηλών γεωγραφικών πλατών.

Συνοψίζοντας, αν και δορυφορικά συστήματα αποτελούν αναντικατάστατο στοιχείο των στρατιωτικών επικοινωνιών, η αξιοπιστία τους εξαρτάται από την αντιμετώπιση συγκεκριμένων αδυναμιών. Η υψηλή καθυστέρηση, η ευπάθεια σε επιθέσεις και παρεμβολές, η συμφόρηση του φάσματος και το υψηλό κόστος καθιστούν αναγκαία τη συνεχή έρευνα και ανάπτυξη νέων τεχνολογιών, ώστε τα SATCOM να παραμείνουν αποτελεσματικά και ασφαλή σε ένα περιβάλλον ολοένα και πιο απαιτητικό.

3.4.5 Μελλοντικές Τάσεις

Η ανάπτυξη των δορυφορικών επικοινωνιών βρίσκεται σε καμπή, καθώς οι τεχνολογικές και επιχειρησιακές απαιτήσεις οδηγούν σε νέες προσεγγίσεις και υβριδικές αρχιτεκτονικές. Οι παραδοσιακές πλατφόρμες GEO παραμένουν σημαντικές, αλλά το μέλλον φαίνεται να ανήκει σε πολυεπίπεδες υποδομές που συνδυάζουν δορυφόρους χαμηλής και μεσαίας τροχιάς με προηγμένα επίγεια και εναέρια δίκτυα.

Μια από τις σημαντικότερες εξελίξεις είναι η ανάπτυξη μεγάλων συστοιχιών LEO δορυφόρων(mega-constellations). Προγράμματα όπως το Starlink και το OneWeb έχουν ήδη αρχίσει να παρέχουν παγκόσμια κάλυψη με χαμηλή καθυστέρηση και οι στρατιωτικοί οργανισμοί μελετούν την

επιχειρησιακή αξιοποίησή τους. Η χρήση LEO δορυφόρων μειώνει δραστικά το latency, γεγονός που επιτρέπει εφαρμογές σε πραγματικό χρόνο όπως ο τηλεχειρισμός οπλικών συστημάτων ή η άμεση μετάδοση δεδομένων μάχης. Παράλληλα, η διασπορά μεγάλου αριθμού δορυφόρων ενισχύει την ανθεκτικότητα, καθώς η απώλεια μεμονωμένων πλατφορμών δεν επηρεάζει σοβαρά το συνολικό δίκτυο.

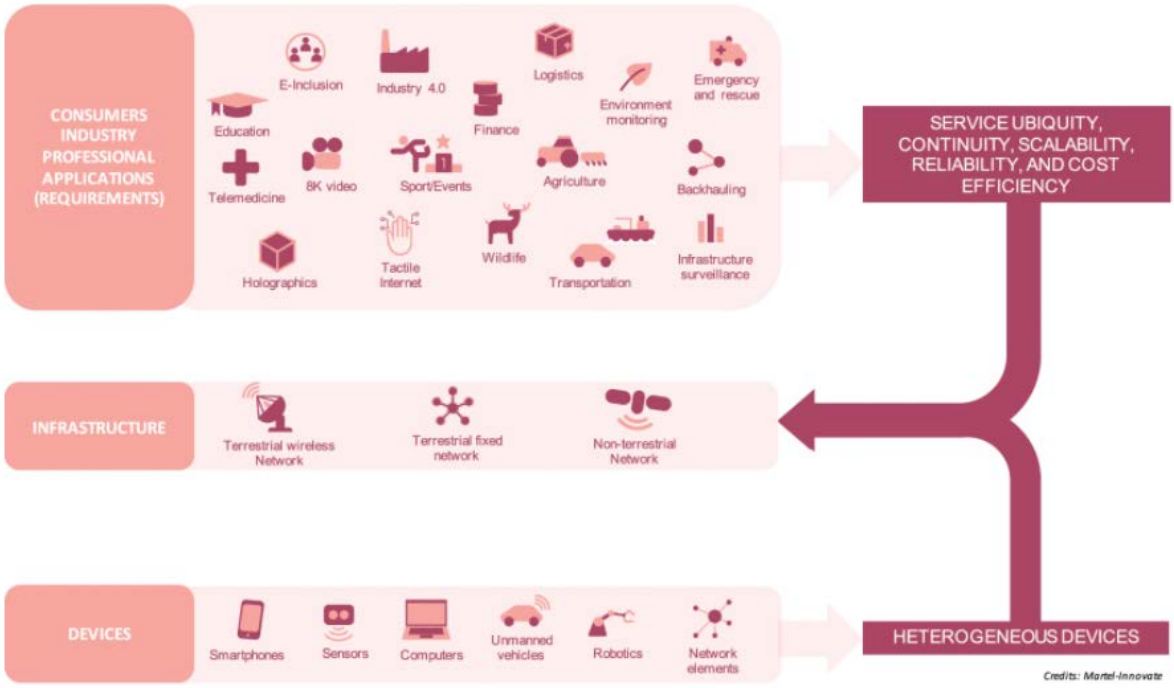
Εξίσου σημαντική κατεύθυνση είναι η ενοποίηση με τα δίκτυα 5G και τα μελλοντικά 6G.Η σύγκλιση δορυφορικών και επίγειων τεχνολογιών στο πλαίσιο των Non-Terrestrial Networks(NTNs) επιτρέπει την ανάπτυξη υβριδικών συστημάτων, όπου οι δορυφόροι συνεργάζονται με UAVs, HAPs(High Altitude Platforms) και επίγεια MANETs. Αυτό το πολυεπίπεδο οικοσύστημα υπόσχεται μεγαλύτερη χωρητικότητα, ευελιξία και βελτιωμένη αξιοποίηση του φάσματος.

Η εισαγωγή τεχνητής νοημοσύνης και μηχανικής μάθησης στα δορυφορικά δίκτυα αποτελεί επίσης μελλοντική τάση μεγάλης σημασίας. Η χρήση αλγορίθμων AI για τη διαχείριση φάσματος, τη δρομολόγηση δεδομένων και την πρόβλεψη παρεμβολών υπόσχεται να βελτιώσει δραστικά την αποδοτικότητα και την ανθεκτικότητα των SATCOM. Επιπλέον, οι τεχνολογίες αυτές μπορούν να αυτοματοποιήσουν διαδικασίες όπως το dynamic spectrum sharing ή η ανακατανομή πόρων σε περιβάλλοντα υψηλής κινητικότητας.

Επίσης, παρατηρείται αυξανόμενο ενδιαφέρον για την ανάπτυξη ασφαλών και ανθεκτικών SATCOM που μπορούν να αντέξουν σε κυβερνοεπιθέσεις και σε απειλές ηλεκτρονικού πολέμου. Οι μελλοντικές δορυφορικές υποδομές θα ενσωματώνουν ενισχυμένα πρωτόκολλα κρυπτογράφησης, μηχανισμούς ανίχνευσης ανωμαλιών και τεχνολογίες προστασίας από spoofing και jamming, ώστε να διασφαλίζεται η αδιάλειπτη λειτουργία ακόμη και σε περιβάλλοντα υψηλής απειλής.

Τέλος, μια ακόμη κατεύθυνση είναι η διπλή χρήση (dual-use) εμπορικών και στρατιωτικών δορυφορικών συστημάτων. Η συνεργασία με εμπορικούς παρόχους δορυφορικών υπηρεσιών μειώνει το κόστος και επιταχύνει την ανάπτυξη νέων δυνατοτήτων. Παράλληλα, οι στρατιωτικές εφαρμογές συμβάλλουν στη σκλήρυνση(hardening) των εμπορικών τεχνολογιών, καθιστώντας τις πιο ανθεκτικές σε αντίξοες συνθήκες. Η ενοποίηση δορυφορικών και επίγειων δικτύων για την υποστήριξη μελλοντικών εφαρμογών στο Σχήμα 27.

Εν κατακλείδι, οι μελλοντικές τάσεις δείχνουν προς ένα υβριδικό, ευφυές και ανθεκτικό οικοσύστημα SATCOM, όπου οι LEO mega-constellations, η σύγκλιση με 5G/6G, η ενσωμάτωση AI και η συνεργασία με τον εμπορικό τομέα θα καθορίσουν την επόμενη γενιά στρατιωτικών επικοινωνιών. Η εξέλιξη αυτή θα ενισχύσει την επιχειρησιακή αυτονομία των Ένοπλων Δυνάμεων και θα συμβάλει καθοριστικά στη διαμόρφωση του μελλοντικού δικτυοκεντρικού πεδίου μάχης.



Σχήμα 27-Ενσωμάτωση δορυφορικών και επίγειων δικτύων για μελλοντικές εφαρμογές [87]

ΚΕΦΑΛΑΙΟ 4

4 Πρωτόκολλα και Δομές Στρατιωτικών Δικτυών

4.1 Τροποποιήσεις TCP/IP για τα τακτικά δίκτυα

Το μοντέλο TCP/IP(Transmission Control Protocol / Internet Protocol) αποτελεί το θεμέλιο του σύγχρονου διαδικτύου και των περισσότερων εμπορικών επικοινωνιών, καθώς σχεδιάστηκε για περιβάλλοντα με σταθερή συνδεσιμότητα, επαρκές εύρος ζώνης και περιορισμένη κινητικότητα. Ωστόσο, σε στρατιωτικά τακτικά δίκτυα –όπου οι συνθήκες είναι μεταβαλλόμενες, δυναμικές και πολλές φορές εχθρικές- η χρήση των παραδοσιακών μηχανισμών του TCP/IP παρουσιάζει σοβαρούς περιορισμούς. Για να καταστεί δυνατή η αξιόπιστη και αποτελεσματική επικοινωνία στο πεδίο της μάχης, απαιτούνται προσαρμογές τόσο στην αρχιτεκτονική όσο και στη συμπεριφορά του πρωτοκόλλου [88], [89].

Τα τακτικά στρατιωτικά δίκτυα υποστηρίζουν τη διασύνδεση δυνάμεων στο πεδίο μάχης, συνδέοντας κινητά τερματικά, φορητούς σταθμούς, οχήματα, drones και άλλες μονάδες που κινούνται σε ρευστά περιβάλλοντα. Τα χαρακτηριστικά τους περιλαμβάνουν:

- ψηλή κινητικότητα: Οι κόμβοι -είτε πρόκειται για ομάδες πεζικού, θωρακισμένα οχήματα ή UAVs- που αλλάζουν συνεχώς θέση, προκαλώντας διαρκείς μεταβολές στην τοπολογία του δικτύου και απαιτώντας από τα πρωτόκολλα να ανταποκρίνονται άμεσα σε νέες συνθήκες σύνδεσης [90], [91].
- Χαμηλό bandwidth και αυξημένες παρεμβολές: Η επικοινωνία βασίζεται συχνά σε ασύρματα κανάλια περιορισμένης χωρητικότητας, όπως τα UHF(Ultra High Frequency), VHF(Very High Frequency),HF(High Frequency) ή tactical radios, τα οποία είναι ευάλωτα σε θόρυβο, φυσικά εμπόδια και σκόπιμες παρεμβολές (jamming) [92], [93].
- Αποσπασματική και μη προβλέψιμη συνδεσιμότητα: Οι συνδέσεις μπορεί να διακόπτονται ξαφνικά λόγω γεωγραφικών εμποδίων, παρεμβολών ή απώλειας ενέργειας στους κόμβους, καθιστώντας αδύνατη τη συνεχή ροή δεδομένων χωρίς ειδικά μέτρα αντοχής σε καθυστερήσεις [94], [95], [96].
- Υψηλές απαιτήσεις ασφάλειας και real-time απόκρισης: Η καθυστέρηση ή απώλεια κρίσιμων πληροφοριών, όπως εντολές διοίκησης ή πληροφορίες αναγνώρισης, μπορεί να έχει άμεσες επιπτώσεις στην επιτυχία της αποστολής και στην ασφάλεια του προσωπικού [89], [97].

Το πρωτόκολλο TCP, που έχει ενσωματωμένο μηχανισμό ελέγχου συμφόρησης (congestion control), θεωρεί κάθε απώλεια πακέτου ως ένδειξη υπερφόρτωσης και μειώνει το ρυθμό μετάδοσης. Σε ένα τακτικό ασύρματο δίκτυο, όμως, οι απώλειες δεν προκαλούνται κατ' ανάγκη από συμφόρηση, αλλά και παρεμβολές, αποσύνδεση ή θόρυβο. Συνεπώς, η λανθασμένη απόκριση του TCP έχει ως αποτέλεσμα τη μειωμένη απόδοση και αναξιόπιστη μετάδοση [98], [99].

Επιπλέον, ο μηχανισμός slow-start, ο οποίος εφαρμόζει σταδιακή αύξηση του ρυθμού μετάδοσης για την αποφυγή συμφόρησης στην έναρξη μιας σύνδεσης, οδηγεί σε υποεκμετάλλευση του διαθέσιμου εύρους ζώνης σε συνδέσεις μικρής διάρκειας ή μεταβλητής ποιότητας – όπως συμβαίνει συχνά στα τακτικά δίκτυα MANETs (Mobile Ad-hoc Networks) [100], [101]. Τέλος, η έλλειψη συνεργασίας του TCP με κατώτερα επίπεδα του OSI (Open Systems Interconnection) –όπως το φυσικό επίπεδο ή το επίπεδο πρόσβασης στο μέσο (MAC- Medium Access Control)- περιορίζει την ικανότητα του να προσαρμόζεται σε αλλαγές της ποιότητας σύνδεσης, αυξάνοντας τον κίνδυνο αναποτελεσματικής χρήσης του καναλιού [102], [103].

4.1.1 Βελτιωμένες εκδόσεις TCP για τα τακτικά δίκτυα

Για να καλυφθούν οι αυστηρές επιχειρησιακές απαιτήσεις των τακτικών στρατιωτικών δικτύων, έχουν σχεδιαστεί πολλαπλές παραλλαγές και τεχνικές επέκτασης του κλασικού TCP, ειδικά προσαρμοσμένες σε ασύρματα περιβάλλοντα με υψηλή κινητικότητα, περιορισμένο εύρος ζώνης και αυξημένη πιθανότητα παρεμβολών [98].

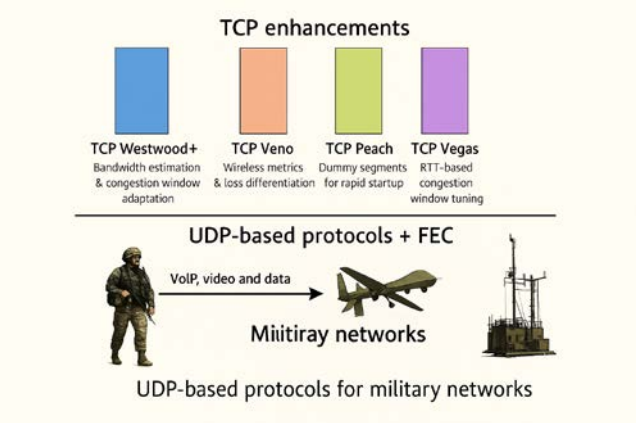
Μία από τις πλέον διαδεδομένες τροποποιήσεις είναι το TCP Westwood+, το χρησιμοποιεί προηγμένες τεχνικές εκτίμησης του διαθέσιμου bandwidth βασιζόμενο στην παρακολούθηση των πακέτων επιβεβαίωσης (ACKs). Έτσι, προσαρμόζει δυναμικά το congestion window αποφεύγοντας αδικαιολόγητες μειώσεις ρυθμού σε περιβάλλοντα με συχνές απώλειες λόγω παρεμβολών και όχι συμφόρησης, όπως συμβαίνει στα tactical radios [98], [95].

Αντίστοιχα, το TCP Veno συνδυάζει στοιχεία του TCP Reno με μετρήσεις χαρακτηριστικών ασύρματης σύνδεσης (wireless metrics), όπως το ρυθμό απωλειών και τη διακύμανση καθυστερήσεων. Αυτή η υβριδική προσέγγιση επιτρέπει στο πρωτόκολλο να διαχωρίζει καλύτερα μεταξύ πραγματικής συμφόρησης και τυχαίων απωλειών, προσφέροντας σταθερότερη απόδοση σε δίκτυα MANET(Mobile Ad-hoc Networks) [96].

Μία ακόμη καινοτόμος προσέγγιση είναι το TCP Peach, το οποίο εισάγει την χρήση dummy segments (τεχνητών πακέτων ελέγχου) κατά τη φάση επανασύνδεσης, ώστε να επιταχύνει την αποκατάσταση του ρυθμού μετάδοσης. Αυτή η τεχνική είναι ιδανική για δίκτυα υψηλής κινητικότητας και συνεχών αποσυνδέσεων , όπως οι κινητοί κόμβοι σε MANETs [104].

Τέλος, το TCP Vegas διαφοροποιείται από τα υπόλοιπα, εφαρμόζοντας μια προληπτική προσέγγιση ελέγχου συμφόρησης. Αντί να περιμένει απώλειες πακέτων, το Vegas παρακολουθεί το round-trip time(RTT) και ρυθμίζει εγκαίρως το μέγεθος του congestion window, αποτρέποντας καθυστερήσεις ή απώλειες πριν εμφανιστούν [99].

Αυτές οι εκδόσεις αποτελούν παραδείγματα στοχευμένων προσπαθειών προσαρμογής του TCP ώστε να λειτουργεί αποδοτικά σε στρατιωτικά ασύρματα δίκτυα, με γνώμονα τη βελτιστοποίηση της ροής δεδομένων, την ανοχή σε λάθη και την ταχεία ανάκαμψη από απώλειες. Η σύγκριση και οι βασικές αρχές λειτουργίας των παραλλαγών αυτών αποτυπώνονται συνοπτικά στο Σχήμα 28, το οποίο παρουσιάζει γραφικά τις κύριες βελτιώσεις του TCP για ασύρματα και τακτικά δίκτυα, καθώς και τη σύνδεσή τους με πρωτόκολλα UDP που χρησιμοποιούνται σε στρατιωτικά περιβάλλοντα.



Σχήμα 28-Γραφική απεικόνιση επιλεγμένων TCP τροποποιήσεων για ασύρματα και τακτικά δίκτυα

4.1.2 Cross-layer βελτιστοποίηση και ECN

Πέρα από τις παραλλαγές TCP, σημαντικό ρόλο στη βελτίωση της απόδοσης των τακτικών στρατιωτικών δικτύων διαδραματίζουν και οι αρχιτεκτονικές τεχνικές προσαρμογής, οι οποίες επεκτείνουν τις δυνατότητες των πρωτοκόλλων μεταφοράς αξιοποιώντας πληροφορίες από άλλα επίπεδα του OSI μοντέλου [102], [103].

Η προσέγγιση της Cross-layer βελτιστοποίησης επιτρέπει την αμφίδρομη αλληλεπίδραση πληροφοριών ανάμεσα σε επίπεδα όπως το transport (TCP), το network (IP), το MAC και το physical layer. Για παράδειγμα, το TCP μπορεί να προσαρμόσει δυναμικά παραμέτρους όπως το congestion window ή το retransmission timeout (RTO), λαμβάνοντας υπόψη δείκτες όπως η ισχύς σήματος, ο ρυθμός απώλειας πακέτων ή η σχετική κίνηση των κόμβων. Αυτή η στρατηγική μειώνει την πιθανότητα λανθασμένου εντοπισμού συμφόρησης, καθώς τα σφάλματα ασύρματης μετάδοσης δε συγχέονται πλέον με συμφόρηση δικτύου [102], [103].

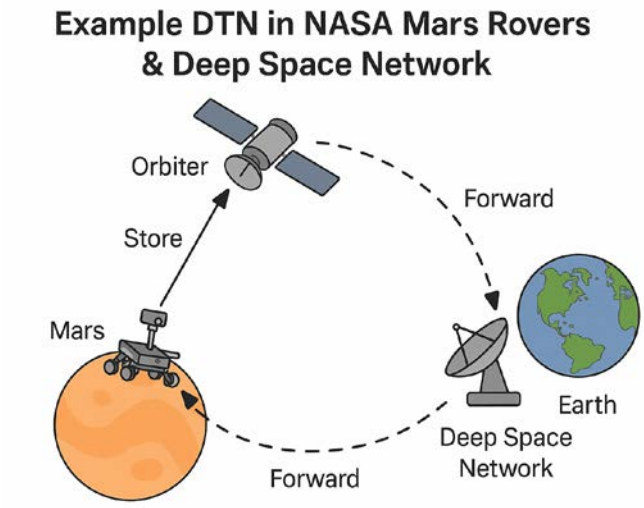
Μια άλλη τεχνική που ενισχύει την αντίδραση του δικτύου χωρίς να στηρίζεται σε packet loss είναι η Explicit Congestion Notification(ECN). Το ECN επιτρέπει στους δρομολογητές να επισημαίνουν

την πιθανή συμφόρηση σε IP πακέτα, ενημερώνοντας τους αποστολείς ώστε να προσαρμόσουν τους ρυθμούς μετάδοσης χωρίς την ανάγκη απόρριψης πακέτων [105]. Η τεχνική αυτή είναι ιδιαίτερα σημαντική για τα ad-hoc δίκτυα, όπου οι απώλειες οφείλονται συχνά σε θόρυβο ή μεταβολή τοπολογίας και όχι σε πραγματική υπερφόρτωση του καναλιού.

Τέλος, το Delay-Tolerant Networking(DTN) αποτελεί μια επαναστατική αρχιτεκτονική προσέγγιση που βασίζεται στην τεχνική store-and-forward. Σε περιβάλλοντα με ασυνεχή ή ασταθή συνδεσιμότητα, όπως επιχειρήσεις UAVs, απομακρυσμένες βάσεις ή ακόμα και σε διαστημικές αποστολές, οι κόμβοι μπορούν να αποθηκεύουν προσωρινά πακέτα και να τα προωθούν όταν επανέλθει η δυνατότητα σύνδεσης. Το DTN λειτουργεί ανεξάρτητα από TCP/IP και εισάγει ένα νέο layer γνωστό ως Bundle Layer, το οποίο διαχειρίζεται buffer, timeout και πολιτικές επανεκπομπής σε κόμβους που δρουν ως ενδιάμεσοι σταθμοί [94], [106]. Έτσι, τα δεδομένα μπορούν να παραμείνουν ασφαλή και να μεταδοθούν όταν επανέλθει η συνδεσιμότητα, κάτι ιδιαίτερα χρήσιμο σε δίκτυα UAVs, πλοίων ή απομακρυσμένες περιοχές με χαμηλή πυκνότητα κόμβων.

Παράδειγμα εφαρμογής: NASA Mars Rovers

Στις αποστολές της NASA προς τον Άρη, όπως οι Opportunity, Curiosity και Perseverance, εφαρμόζεται DTN για την αποστολή δεδομένων από τους ρομποτικούς rovers στη Γη. Η επικοινωνία δεν είναι συνεχής και βασίζεται στην παρουσία δορυφόρων σε τροχιά (Mars Orbiters), οι οποίοι λειτουργούν ως ενδιάμεσοι σταθμοί αποθήκευσης και προώθησης (store-and-forward). Ο rover μεταδίδει τα δεδομένα στον orbiter όταν υπάρχει οπτική επαφή. Στη συνέχεια, ο orbiter αποθηκεύει τα δεδομένα τοπικά και τα προωθεί στη Γη όταν έρθει σε ευθυγράμμιση με το Deep Space Network (DSN) [96], [106].



Σχήμα 29-Εφαρμογή του Delay-Tolerant Networking(DTN) σε διαστημικές αποστολές

Το Σχήμα 29 απεικονίζει την αρχή λειτουργίας του DTN σε περιβάλλον μεγάλης καθυστέρησης, όπως μεταξύ γήινων σταθμών, δορυφόρων και διαστημόπλοιων, με την τεχνική “store-and-forward” να επιτρέπει τη μετάδοση δεδομένων ακόμα και όταν δεν υπάρχει συνεχής σύνδεση.

4.1.3 Εναλλακτικά πρωτόκολλα

Πέρα από τις βελτιώσεις στο TCP, αρκετά σύγχρονα στρατιωτικά συστήματα επιλέγουν και εναλλακτικά πρωτόκολλα, ειδικά για εφαρμογές που απαιτούν real-time μετάδοση με χαμηλή καθυστέρηση και αυξημένη ανθεκτικότητα σε παρεμβολές.

Ένα τυπικό παράδειγμα είναι ο συνδυασμός UDP(User Datagram Protocol) με κωδικούς διόρθωσης σφαλμάτων (FEC- Forward Error Correction). Παρότι το UPD δεν εγγυάται αξιόπιστη μετάδοση, προσφέρει εξαιρετικά χαμηλό latency και απλότητα υλοποίησης, καθιστώντας το ιδανικό για φωνητικές επικοινωνίες (VoIP), streaming βίντεο και χρονικά ευαίσθητα δεδομένα σε τακτικά δίκτυα. Η προσθήκη FEC επιτρέπει στα πακέτα να αναδομηθούν ακόμη και αν μερικά χαθούν κατά τη μετάδοση, ενισχύοντας τη συνολική αξιοπιστία χωρίς καθυστέρηση λόγω επαναμετάδοσης [104], [101].

Ένα νεότερο και πολλά υποσχόμενο πρωτόκολλα είναι το QUIC (Quick UPD Internet Connections), το οποίο αναπτύχθηκε αρχικά από την Google και πλέον αποτελεί ανοιχτό πρότυπο. Το QUIC βασίζεται στο UPD αλλά ενσωματώνει κρυπτογράφηση TLS 1.3, βελτιωμένο μηχανισμό επαναμετάδοσης, και πολλαπλά streams σε μία σύνδεση, ελαχιστοποιώντας το latency και αποφεύγοντας προβλήματα head-of-line blocking [99]. Για στρατιωτικά δίκτυα, το QUIC είναι ιδιαίτερα χρήσιμο σε mobile και ασταθή περιβάλλοντα, όπου η συχνή μεταβολή της τοπολογίας μπορεί να διακόψει συνδέσεις TCP.

Το SCPS (Space Communications Protocol Standards), που αναπτύχθηκε από τη NASA και το Υπουργείο Άμυνας των ΗΠΑ, αποτελεί μια ειδική επέκταση του TCP για διαστημικά και δορυφορικά δίκτυα μεγάλης καθυστέρησης. Περιλαμβάνει λειτουργίες όπως επιλεκτικές επιβεβαιώσεις (SACK), συμπίεση κεφαλίδων TCP/IP και ενσωματωμένη διόρθωση σφαλμάτων, καθιστώντας το κατάλληλο για στρατιωτικά δίκτυα μεγάλων αποστάσεων, όπως τα SATCOM (Satellite Communications) [107].

4.1.4 Split TCP : Αρχή λειτουργίας και πραγματικές εφαρμογές

Μια ιδιαίτερα αποτελεσματική προσέγγιση για τη βελτίωση της απόδοσης σε τέτοια δυναμικά δίκτυα είναι η αρχιτεκτονική Split TCP. Σε αυτήν, η end-to-end σύνδεση TCP διαχωρίζεται σε επιμέρους τμήματα με τη βοήθεια ενδιάμεσων κόμβων (gateway nodes).

Πιο συγκεκριμένα, η συνολική σύνδεση διαιρείται σε δύο ανεξάρτητες συνδέσεις:

- η πρώτη εκτείνεται από τον αποστολέα (π.χ. στρατιώτη ή μονάδα πεδίου) μέχρι τον ενδιάμεσο κόμβο (gateway).

- η δεύτερη ξεκινά από τον gateway και καταλήγει προς τον τελικό παραλήπτη (π.χ. κέντρο επιχειρήσεων ή cloud).

Ο gateway λειτουργεί ως ενδιάμεσος διαμεσολαβητής (proxy), αναλαμβάνοντας την επιβεβαίωση λήψης πακέτων (ACKs), την προσωρινή αποθήκευση(buffering), και την τοπική διαχείριση σφαλμάτων. Έτσι, η απώλεια πακέτων στο δεύτερο τμήμα (π.χ. στο MANET ή στο SATCOM link) δεν μεταδίδεται άμεσα στον αποστολέα, αποτρέποντας αδικαιολόγητη μείωση του ρυθμού μετάδοσης [108]. Το αποτέλεσμα είναι η μικρότερη καθυστέρηση (RTT) και πιο αποδοτικός χειρισμός σφαλμάτων.

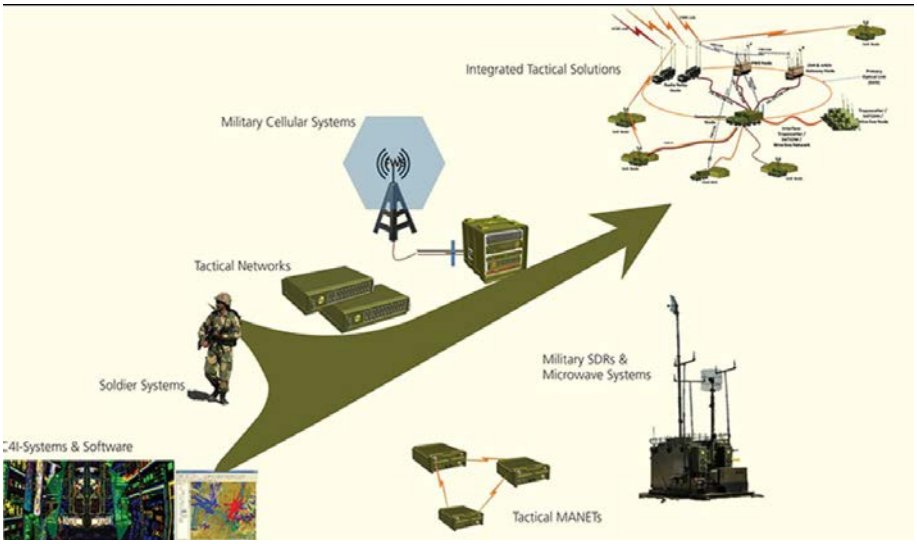
Ωστόσο, η προσέγγιση Split TCP απαιτεί επιπλέον υπολογιστικούς πόρους στον κόμβο gateway και συνεπάγεται προκλήσεις ασφαλείας, ειδικά σε διαβαθμισμένα περιβάλλοντα όπου απαιτείται διαχείριση κρυπτογράφησης και πολιτικές πιστοποίησης [109].

Πραγματικά Παραδείγματα σε Εφαρμογή

Η πρακτική αξιοποίηση των πρωτοκόλλων TCP, και ειδικότερα της αρχιτεκτονικής Split TCP, έχει αποδειχθεί μέσα από μια σειρά επιχειρησιακών υλοποιήσεων σε τακτικά στρατιωτικά δίκτυα. Ένα από τα χαρακτηριστικότερα παραδείγματα αποτελεί το WIN-T(Warfighter Information Network-Tactical) του Αμερικανικού Στρατού, το οποίο εφαρμόζει Split TCP για την εξασφάλιση αξιόπιστης και χαμηλής καθυστέρησης επικοινωνίας σε πραγματικό χρόνο, ακόμη και σε απομακρυσμένα ή ταχέως μεταβαλλόμενα πεδία επιχειρήσεων. [110]. Η αρχιτεκτονική διαιρεί τη σύνδεση σε δύο τμήματα : ένα τοπικό MANET (Mobile Ad-hoc Network) και ένα δεύτερο σκέλος προς δίκτυα SATCOM ή LOS (Line-of-Sight). Αυτό επιτρέπει μικρότερη καθυστέρηση στο τοπικό τμήμα και μεγαλύτερη σταθερότητα μετάδοσης υπό δύσκολες συνθήκες.

Αντίστοιχες τεχνικές έχουν υλοποιηθεί και από τη NATO Communications and Information Agency (NCIA), η οποία έχει εφαρμόσει προηγμένες τεχνικές Split TCP και SCPS σε πολυεθνικά δίκτυα μεγάλης καθυστέρησης, όπως οι δορυφορικές ζεύξεις (SATCOM). Η τεχνολογία SCPS περιλαμβάνει συμπίεση TCP headers, επιλεκτικές επιβεβαιώσεις (SACK) και διορθώσεις σφαλμάτων, επιτρέποντας προσαρμοστικότητα σε περιορισμένο bandwidth και κακές καιρικές συνθήκες. Επιπλέον, διασφαλίζεται διαλειτουργικότητα μεταξύ κρατών-μελών με βάση τα STANAGs(Standardization Agreements) του NATO [107], [111], [55].

Η εφαρμογή του Split TCP επεκτείνεται και σε δίκτυα που αξιοποιούν UAVs(Unmanned Aerial Vehicles) ως εναέριους κόμβους (gateways) που συλλέγουν δεδομένα πεδίου (εικόνα λήψης ευκρίνειας, τηλεμετρία) και τα προωθούν μέσω δορυφορικής ή LOS ζεύξης. Το Split TCP επιτρέπει στο UAV να χειρίζεται ξεχωριστά τη σύνδεση με τον αισθητήρα στο τακτικό περιβάλλον και τη σύνδεση προς το command post. Αυτό αυξάνει την ανθεκτικότητα στη διακοπή, ακόμη και όταν το UAV κινείται ή αλλάζει ρότα συχνά [110], [112].



Σχήμα 30-Απλή αναπαράσταση του Split-TCP σε τακτικό δίκτυο [113]

Στο Σχήμα 30 ο αποστολέας (τάγμα ή στρατιώτης) στέλνει TCP Segment 1στο Getaway (όχημα/UAV), το οποίο αναμεταδίδει το TCP Segment 2 προς τον τελικό παραλήπτη (κέντρο διοίκησης), βελτιώνοντας την απόδοση σε περιβάλλοντα με μεταβαλλόμενη συνδεσιμότητα.

4.1.5 Μελλοντικές τάσεις στα πρωτόκολλα στρατιωτικών τακτικών δικτύων

Η συνεχιζόμενη εξέλιξη των στρατιωτικών τακτικών δικτύων απαιτεί πρωτόκολλα μεταφοράς όλο και πιο ευφυή και προσαρμόσιμα. Η πρόσφατη έρευνα στρέφεται στην ανάπτυξη στοιβών πρωτοκόλλων TCP με γνωστικές δυνατότητες (Cognitive TCP stacks), οι οποίες ενσωματώνουν τεχνικές τεχνητής νοημοσύνης (AI) για την ανάλυση της ποιότητας σύνδεσης σε πραγματικό χρόνο. Μέσω αλγορίθμων μάθησης, τα συστήματα αυτά μπορούν να προβλέπουν και να ρυθμίζουν δυναμικά παραμέτρους όπως το congestion window ή οι στρατηγικές επαναμετάδοσης (retransmission), χωρίς ανθρώπινη παρέμβαση [105], [114].

Παράλληλα, η ενσωμάτωση του Multipath TCP (MPTCP) προσφέρει σημαντικές δυνατότητες για στρατιωτικά δίκτυα που βασίζονται σε πολλαπλές και ετερογενείς ζεύξεις. Το MPTCP επιτρέπει τη διάχυση της κυκλοφορίας ταυτόχρονα σε περισσότερα από ένα διαθέσιμα links – για παράδειγμα μπορεί να χρησιμοποιεί ταυτόχρονα ένα MANET, μια δορυφορική ζεύξη SATCOM και LOS συνδέσεις, αυξάνοντας την αξιοπιστία και την ανθεκτικότητα απέναντι σε παρεμβολές (jamming), φυσικά εμπόδια ή αποσυνδέσεις [115].

Η cross-layer αρχιτεκτονικής συνεχίζει επίσης να αποτελεί σημαντική ερευνητική κατεύθυνση. Μέσω της αλληλεπίδρασης πληροφοριών ανάμεσα σε επίπεδα του OSI μοντέλου, όπως το MAC και το transport layer, καθίσταται δυνατή η ολιστική εκτίμηση της κατάστασης του δικτύου. Αυτό επιτρέπει ταχύτερη προσαρμογή, βελτιστοποίηση πόρων, και μείωση καθυστερήσεων ή σφαλμάτων, ακόμη και σε ιδιαίτερα ευμετάβλητα περιβάλλοντα [102], [103].

Συνοψίζοντας, η χρήση του κλασικού TCP/IP, χωρίς στοχευμένες προσαρμογές, περιορίζει την επιχειρησιακή αποτελεσματικότητα. Το μέλλον ανήκει σε πιο «έξυπνα», ελαφριά και αυτόνομα πρωτόκολλα μεταφοράς, σχεδιασμένα να ανταπεξέρχονται σε παρεμβολές, καθυστερήσεις και αστάθειες σύνδεσης με ελάχιστη ανθρώπινη παρέμβαση [105], [114].

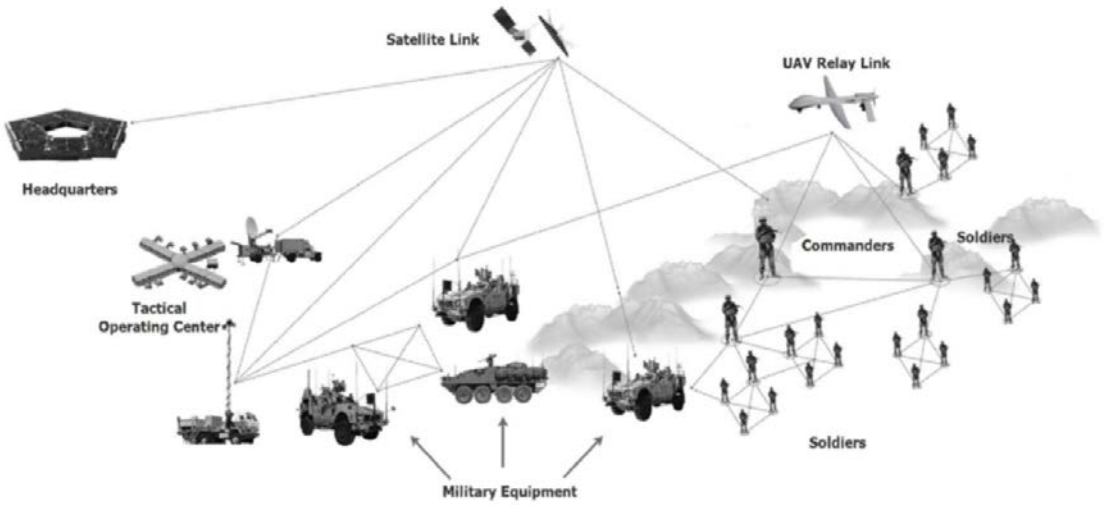
4.2 MANETs & Ad-Hoc Αρχιτεκτονικές

Στις σύγχρονες στρατιωτικές επιχειρήσεις, η ανάγκη για ευέλικτες, ανθεκτικές και ασφαλείς επικοινωνίες χωρίς εξάρτηση από σταθερή υποδομή θεωρείται καθοριστικής σημασίας για την επιτυχία κάθε αποστολής. Οι στρατιωτικές δυνάμεις συχνά καλούνται να επιχειρήσουν σε απομακρυσμένα, εχθρικά ή κατεστραμμένα περιβάλλοντα όπου δεν είναι εφικτή η ανάπτυξη συμβατικών τηλεπικοινωνιακών γραμμών ή σταθερών σταθμών βάσης. Σε αυτό το πλαίσιο, τα κινητά ad-hoc δίκτυα (Mobile Ad hoc Networks - MANETs) παρέχουν μια αποτελεσματική και πρακτική λύση, καθώς επιτρέπουν τη δημιουργία ενός ευέλικτου, αυτοοργανωμένου και δυναμικού δικτύου επικοινωνίας που μπορεί να αναπτυχθεί άμεσα, προσαρμοζόμενο στις συνεχώς μεταβαλλόμενες συνθήκες του πεδίου της μάχης [116], [117].

Ένα MANET αποτελείται από πολλούς κινητούς κόμβους, όπως στρατιώτες που φέρουν φορητά τερματικά επικοινωνίας, οχήματα μάχης που δρουν ως αναμεταδότες και μη επανδρωμένα αεροσκάφη (UAVs) που επεκτείνουν την εμβέλεια του δικτύου από αέρος. Οι κόμβοι αυτοί επικοινωνούν μεταξύ τους είτε άμεσα είτε μέσω ενδιάμεσων κόμβων που δρουν ως δρομολογητές, δημιουργώντας ένα πλέγμα (mesh) δυναμικών συνδέσεων. Η τοπολογία του δικτύου μεταβάλλεται συνεχώς ανάλογα με την κίνηση των χρηστών, τις επιχειρησιακές ανάγκες και τις αλλαγές στο πεδίο. Το routing επιτυγχάνεται με δυναμικά πρωτόκολλα, όπως AODV(Ad-hoc On-Demand Distance Vector) και OLSR(Optimized Link State Routing) [118], [100], [119].

Τα MANETs διακρίνονται για ορισμένα βασικά χαρακτηριστικά που τα καθιστούν ιδανικά για τακτικές στρατιωτικές επιχειρήσεις. Πρώτον, διαθέτουν αυτοσυγκρότηση (self-forming), καθώς δεν απαιτείται κεντρικός διαχειριστής ή προκαθορισμένη υποδομή, το δίκτυο δημιουργείται αυτόματα από τους κόμβους που συμμετέχουν. Δεύτερον, χαρακτηρίζονται από αυτοθεραπεία (self-healing) δηλαδή την ικανότητα να ανακατευθύνουν αυτόματα την κυκλοφορία των δεδομένων όταν ένας κόμβος αποσυνδεθεί ή τεθεί εκτός λειτουργίας. Επιπλέον, παρουσιάζουν υψηλό βαθμό προσαρμοστικότητας καθώς η αρχιτεκτονική τους επιτρέπει συνεχή αναδιάρθρωση ανάλογα με τις μεταβολές θέσης, την επιχειρησιακή κατάσταση ή τις παρεμβολές στο περιβάλλον. Τέλος, χαρακτηρίζονται από ετερογένεια κόμβων, αφού μπορούν να περιλαμβάνουν ποικιλία συσκευών από φορητά τερματικά στρατιωτών έως οχήματα μάχης και UAVs με διαφορετικές δυνατότητες μετάδοσης,

ισχύος και ενεργειακής αυτονομίας. Η λειτουργία και τα πλεονεκτήματα των MANETs σε πραγματικές επιχειρησιακές συνθήκες αποτυπώνονται στο Σχήμα 31.



Σχήμα 31-Εφαρμογή MANET σε στρατιωτική αποστολή [108]

4.2.1 Πλεονεκτήματα στα τακτικά δίκτυα

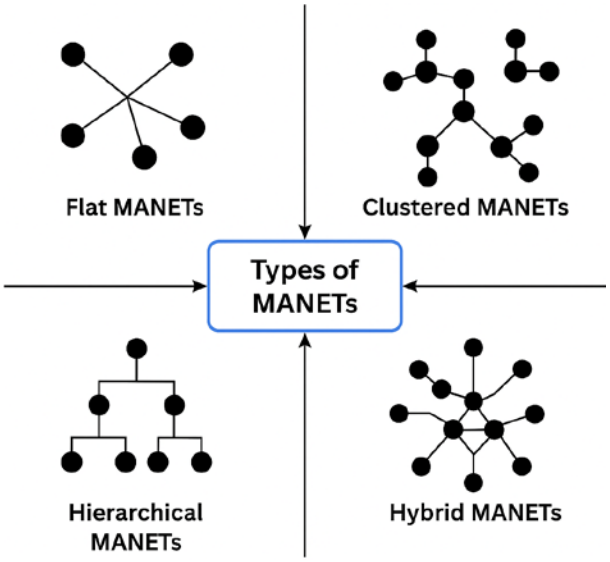
Η αρχιτεκτονική των MANETs παρέχει σημαντικά επιχειρησιακά πλεονεκτήματα που τα καθιστούν εξαιρετικά χρήσιμα σε αποστολές άμεσης ανάπτυξης, σε απομονωμένες περιοχές ή σε περιβάλλοντα που έχουν υποστεί καταστροφή λόγω πολέμου ή φυσικών φαινομένων. Χάρη στη μη εξάρτηση από σταθερή υποδομή ή κεντρικούς κόμβους ελέγχου, εξαλείφεται ο κίνδυνος «ενιαίου σημείου αποτυχίας» (single point of failure), γεγονός που βελτιώνει τη συνολική ανθεκτικότητα του συστήματος [101].

Η δυνατότητα αυτό-οργάνωσης και αυτοθεραπείας επιτρέπει στο δίκτυο να συνεχίζει να λειτουργεί απρόσκοπτα ακόμη και αν κάποιοι κόμβοι αποσυνδεθούν, υποστούν βλάβη (π.χ. λόγω καταστροφής, ηλεκτρομαγνητικής παρεμβολής ή γεωγραφικών εμποδίων). Αυτή η δυναμική προσαρμοστικότητα είναι ιδιαίτερα κρίσιμη σε σενάρια υψηλής επικινδυνότητας, όπως στρατιωτικές επεμβάσεις ή φυσικές καταστροφές, όπου η απώλεια επικοινωνίας μπορεί να οδηγήσει σε επιχειρησιακή αποτυχία ή κίνδυνο ζωής [108], [97].

Επιπλέον, τα MANETs επιτρέπουν τη γρήγορη ανάπτυξη του δικτύου χωρίς χρονοβόρα εγκατάσταση υποδομών, προσφέροντας ευελιξία σε ασύμμετρα πεδία μάχης και σύνδεση μεταξύ ανομοιογενών πλατφορμών. Με την υποστήριξη τεχνικών για routing πολλαπλών αλμάτων (multi-hop routing) και διαφορετικές μορφές ζεύξεων (π.χ. LOS, SATCOM, relay UAVs), μπορούν να διασφαλίσουν συνεχή ροή δεδομένων και εντολών ακόμα και σε δύσκολες γεωγραφικές ή περιβαλλοντικές συνθήκες [120], [110].

4.2.2 Δομή και τύποι MANETs

Η αρχιτεκτονική ενός MANET δεν είναι ενιαία, αλλά προσαρμόζεται ανάλογα με τις επιχειρησιακές ανάγκες, το μέγεθος του δικτύου και τον ρόλο των εμπλεκόμενων μονάδων. Αυτή η ευελιξία καθιστά τα MANETs κατάλληλα για εφαρμογές από μικρές ομάδες αναγνώρισης έως στρατηγικά δίκτυα που συνδυάζουν επίγειες και εναέριες μονάδες. Η διαφοροποίηση στη δομή τους έχει οδηγήσει στην ανάπτυξη διαφόρων αρχιτεκτονικών προσεγγίσεων, οι οποίες διακρίνονται κυρίως σε flat, clustered, hierarchical και hybrid MANETs, όπως συνοψίζονται και στο Σχήμα 32.



Σχήμα 32-Τυπολογία MANETs

Στα flat MANETs, όλοι οι κόμβοι είναι ισότιμοι, χωρίς ιεραρχία. Διαχειρίζονται μόνοι τους τη δρομολόγηση και την αναμετάδοση πακέτων. Αυτή η απλή αρχιτεκτονική είναι ιδανική για ομάδες πεζικού ή ταχείας επέμβασης, προσφέροντας ευελιξία και ελαχιστοποίηση καθυστερήσεων, αλλά περιορισμένη απόδοση σε μεγάλης κλίμακας δίκτυα [117], [100].

Μια πιο οργανωμένη μορφή αποτελούν τα clustered MANETs: Οι κόμβοι οργανώνονται σε ομάδες (clusters) με κεντρικό συντονιστή (cluster head), ο οποίος χειρίζεται την επικοινωνία εντός και μεταξύ ομάδων. Μειώνει τον φόρτο στους απλούς κόμβους και επιτρέπει αποδοτικό routing σε εκτεταμένες επιχειρησιακές ζώνες, καθιστώντας το ιδανικό για ταξιαρχίες ή πολυεθνικές ασκήσεις NATO [120].

Ακόμη πιο εξελιγμένη προσέγγιση αποτελούν τα hierarchical MANETs, τα οποία προσθέτουν πολυεπίπεδη ιεραρχία στους clustered τύπους. Συντονιστές ανώτερου επιπέδου (super cluster heads) οργανώνουν clusters χαμηλότερου επιπέδου. Ιδανικό για UAV-UAV-επίγειες συνδυασμένες επιχειρήσεις, όπου απαιτείται κλιμακωτός έλεγχος και κατανομή ευθυνών [119], [110].

Τέλος, στα hybrid MANETs: Τα περισσότερα στρατιωτικά δίκτυα υλοποιούν υβριδικές αρχιτεκτονικές, συνδυάζοντας προδραστική δρομολόγηση (π.χ. OLSR) και αντιδραστική δρομολόγηση(π.χ. AODV) για βελτιστοποίηση πόρων και real-time απόκριση, ανάλογα με το φορτίο, την τοπολογία και την προτεραιότητα του δεδομένου [121], [122].

Η σωστή επιλογή αρχιτεκτονικού μοντέλου είναι κρίσιμη για την επιτυχία της αποστολής, καθώς επηρεάζει τη δυναμική ανταπόκριση, την κατανάλωση ενέργειας, την ανθεκτικότητα σε παρεμβολές και τη συμβατότητα με υβριδικά περιβάλλοντα μάχης. Η στρατηγική χρήση MANET μπορεί να εξασφαλίσει τη συνέχεια διοίκησης και ελέγχου (C2) ακόμα και υπό εχθρικές ή καταστροφικές συνθήκες.

4.2.3 Σύγκριση MANET με παραδοσιακά δίκτυα

Για την ανάδειξη της λειτουργικής και στρατηγικής υπεροχής των MANETs έναντι των παραδοσιακών τηλεπικοινωνιακών υποδομών, κρίνεται απαραίτητη μια συγκριτική θεώρηση βασικών χαρακτηριστικών. Τα παραδοσιακά δίκτυα (όπως τα ενσύρματα LAN ή τα κλασικά κυψελοειδή δίκτυα) βασίζονται σε σταθερή υποδομή, προκαθορισμένη τοπολογία και κεντρικό έλεγχο, καθιστώντας τα ακατάλληλα για επιχειρήσεις σε μεταβαλλόμενα ή απομακρυσμένα πεδία. Αντίθετα, τα MANETs προσφέρουν υψηλή ευελιξία, δυναμική τοπολογία, και ιδιότητες αυτοθεραπείας, καθιστώντας τα ιδανικά για στρατιωτικά περιβάλλοντα με υψηλή κινητικότητα και έλλειψη υποδομής [101], [55]. Ο Πίνακας 3 συνοψίζει τα συγκριτικά στοιχεία.

Πίνακας 3-Σύγκριση MANETs και παραδοσιακών δικτύων

Χαρακτηριστικό	MANETs	Παραδοσιακά Δίκτυα
Υποδομή	Δεν απαιτείται	Απαραίτητη(σταθμοί βάσης, routers)
Κεντρικός έλεγχος	Όχι -πλήρως αποκεντρωμένα	Ναι -με κεντρικούς ελεγκτές
Κινητικότητα κόμβων	Υψηλή(στρατιώτες, UAVs, οχήματα)	Χαμηλή ή ανύπαρκτη
Ευελιξία	Πολύ υψηλή - δυναμική επανασύνδεση	Περιορισμένη με στατική τοπολογία
Ανθεκτικότητα	Υψηλή(self-healing, fault tolerance)	Μέτρια -ευάλωτα σε κόμβους κρίσιμης σημασίας

Εφαρμογές	Τακτικές αποστολές, UAVs, IoMT, C4ISR	Εμπορικές, διοικητικές, στατικές εφαρμογές

Ο Πίνακας 3 καταδεικνύει ξεκάθαρα τη στρατηγική καταλληλότητα των MANETs για αποστολές πεδίου όπου η ευκινησία, η αντοχή σε παρεμβολές, και η απουσία υποδομής είναι κρίσιμες παράμετροι. Ειδικά σε περιβάλλοντα με UAV relay, κατεστραμμένες υποδομές ή ασύμμετρο πόλεμο, η χρήση παραδοσιακών δικτύων δεν είναι βιώσιμη. Τα MANETs, μέσα από τον αποκεντρωμένο, προσαρμοστικό και modular σχεδιασμό τους, υποστηρίζουν την επιβιωσιμότητα της δικτυακής πληροφορίας και την αποδοτική λήψη αποφάσεων σε συνθήκες έντασης ή απρόβλεπτης απώλειας κόμβων.

4.2.4 Πρωτόκολλα δρομολόγησης σε MANETs

Η αποτελεσματική λειτουργία ενός MANET βασίζεται σε μεγάλο βαθμό στην ικανότητα του δικτύου να εντοπίζει και να διατηρεί βέλτιστες διαδρομές επικοινωνίας μεταξύ κινητών κόμβων, παρά τις συνεχείς αλλαγές τοπολογίας. Για τον σκοπό αυτό, έχουν αναπτυχθεί εξειδικευμένα πρωτόκολλα δρομολόγησης, τα οποία χωρίζονται γενικά σε δύο μεγάλες κατηγορίες : τα αντιδραστικά (reactive) και τα προδραστικά (proactive).

Ένα χαρακτηριστικό παράδειγμα αντιδραστικού πρωτοκόλλου αποτελεί το AODV. Λειτουργεί με αρχή «κατόπιν απαίτησης» - δηλαδή, δημιουργεί διαδρομές μόνο όταν ένας κόμβος χρειάζεται να στείλει δεδομένα σε άλλον κόμβο για τον οποίο δεν έχει ήδη πληροφορία διαδρομής. Αυτό μειώνει σημαντικά το overhead του δικτύου, καθώς αποφεύγεται η συνεχής ανταλλαγή ενημερωτικών πακέτων. Όταν χαθεί μια σύνδεση, το AODV εκκινεί διαδικασία εύρεσης νέας διαδρομής, εξασφαλίζοντας έτσι ευελιξία σε δυναμικά σενάρια.

Αντίστοιχα το DSR είναι επίσης αντιδραστικό, αλλά λειτουργεί με διαφορετική λογική: η διαδρομή από τον αποστολέα προς τον παραλήπτη ενσωματώνεται μέσα σε κάθε πακέτο δεδομένων (source routing). Αυτό σημαίνει ότι κάθε πακέτο «γνωρίζει» όλη την ακολουθία των κόμβων που πρέπει να περάσει, μειώνοντας την ανάγκη για πίνακες δρομολόγησης σε κάθε κόμβο. Αν και είναι πολύ αποδοτικό σε μικρά δίκτυα με λίγους κόμβους, σε μεγάλα δίκτυα μπορεί να αυξήσει το μέγεθος των πακέτων και την καθυστέρηση.

Από την άλλη πλευρά, το OLSR ανήκει στην κατηγορία των προδραστικών πρωτοκόλλων. Κάθε κόμβος διατηρεί συνεχώς πληροφορίες για την τοπολογία του δικτύου, ανανεώνοντας τις πληροφορίες περιοδικά μέσω μηνυμάτων ελέγχου. Αυτό επιτρέπει την άμεση διαθεσιμότητα διαδρομών χωρίς καθυστερήσεις αναζήτησης, κάτι που είναι σημαντικό σε εφαρμογές real-time (π.χ. live video feed από

UAV). Το OLSR είναι ιδιαίτερα κατάλληλο για μεγάλα MANETs με υψηλό traffic, αλλά αυξάνει το overhead λόγω της συνεχούς ενημέρωσης.

Τα σύγχρονα πρωτόκολλα συνδυάζουν στοιχεία και από τα δύο μοντέλα: για παράδειγμα, πολλά υβριδικά πρωτόκολλα χρησιμοποιούν proactive μηχανισμούς για συχνές ή κρίσιμες διαδρομές και αντιδραστικούς μηχανισμούς για πιο σπάνιες συνδέσεις. Παράλληλα, υποστηρίζουν μηχανισμούς Quality of Service (QoS) ώστε να δίνεται προτεραιότητα σε δεδομένα υψηλής σημασίας (π.χ. φωνή, βίντεο αναγνώρισης) σε πραγματικό χρόνο.

Η σωστή επιλογή και παραμετροποίηση του πρωτοκόλλου δρομολόγησης αποτελεί καθοριστικό παράγοντα για τη διατήρηση της σταθερότητας και της απόδοσης ενός MANET σε σενάρια αυξημένης κινητικότητας και αστάθειας συνδεσιμότητας.

4.2.5 Εφαρμογές σε στρατιωτικά συστήματα

Τα MANETs έχουν ήδη καθιερωθεί ως βασικό δομικό στοιχείο σε διάφορα προηγμένα στρατιωτικά συστήματα επικοινωνιών, υποστηρίζοντας την απαίτηση για ταχεία, αξιόπιστη και ασφαλή διασύνδεση όλων των επιπέδων διοίκησης και μονάδων πεδίου.

Ένα χαρακτηριστικό παράδειγμα αποτελούν τα Tactical Radio Networks, μέσω των οποίων στρατιώτες, οχήματα και φορητοί σταθμοί επικοινωνίας ανταλλάσσουν φωνητικές εντολές και δεδομένα σε πραγματικό χρόνο, ακόμα και σε εχθρικό ή απρόσιτο περιβάλλον. Οι ασύρματοι πομποδέκτες που φέρουν οι μονάδες λειτουργούν ως κόμβοι του MANET, εξασφαλίζοντας διαρκή συνδεσιμότητα ακόμη και μετά από απώλεια ενδιάμεσων κόμβων [97].

Τα MANETs αποτελούν κρίσιμη τεχνολογική βάση για τα σύγχρονα συστήματα C4ISR και C5ISR (Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance). Μέσω αυτών των συστημάτων, οι διοικητές μπορούν να λαμβάνουν πληροφορίες πεδίου σε πραγματικό χρόνο, να συντονίζουν μονάδες σε διαφορετικά σημεία και να εκτελούν αποστολές με καλύτερη επίγνωση της κατάστασης (situational awareness) [109].

Επιπλέον, οι δικτυώσεις μεταξύ UAVs, αισθητήρων και μαχητικών οχημάτων βασίζονται στην αρχιτεκτονική των MANETs για τη συνεχή ροή δεδομένων όπως βίντεο, εικόνες και τηλεμετρία. Τα UAVs, ιδίως, λειτουργούν συχνά ως εναέριοι αναμεταδότες (relays) που επεκτείνουν το εύρος κάλυψης του δικτύου σε ορεινές ή απομονωμένες περιοχές [110].

Τέλος, η ταχεία άνοδος του Internet of Military Things(IoMT) ενσωματώνει τα MANETs ως την υποδομή που συνδέει αισθητήρες, οπλικά συστήματα, drones και άλλες πλατφόρμες σε ένα διανεμημένο δίκτυο υψηλής προσαρμοστικότητας. Κάθε κόμβος λειτουργεί ως έξυπνη μονάδα που μπορεί να συλλέγει, να αναλύει και να διαβιβάζει πληροφορίες με στόχο τη βελτιστοποίηση της επιχειρησιακής απόδοσης [111], [122].

Ο τελικός στόχος της χρήσης των MANETs σε αυτά τα συστήματα είναι η δημιουργία ενός ανθεκτικού, ευέλικτου και πλήρως διασυνδεδεμένου πεδίου πληροφορίας, το οποίο να μπορεί να προσαρμόζεται άμεσα στις ανάγκες της αποστολής, μεγιστοποιώντας την επιχειρησιακή αποτελεσματικότητα και την ασφάλεια του προσωπικού.

4.2.6 Προκλήσεις και τεχνολογικές κατευθύνσεις

Παρά τα πολλαπλά πλεονεκτήματα που προσφέρουν τα MANETs, η υλοποίηση τους σε στρατιωτικά περιβάλλοντα συνοδεύεται από αρκετές τεχνικές προκλήσεις που παραμένουν αντικείμενο έντονης έρευνας και τεχνολογικής καινοτομίας.

Μία από τις σημαντικότερες προκλήσεις είναι η διασφάλιση της ασφάλειας των επικοινωνιών. Η αποκεντρωμένη και δυναμική φύση ενός MANET καθιστά ιδιαίτερα περίπλοκη τη διατήρηση της αυθεντικότητας, της ακεραιότητας και της εμπιστευτικότητας των δεδομένων. Οι κόμβοι μπορούν να προστίθενται ή να αφαιρούνται συνεχώς, κάτι που αυξάνει την πιθανότητα κακόβουλων παρεμβολών και επιθέσεων τύπου spoofing ή man-in-the-middle [90], [123].

Ένα άλλο τεχνικό ζήτημα είναι η καθυστέρηση (latency). Η συχνή αλλαγή τοπολογίας και οι συνεχείς επαναδιαπραγματεύσεις διαδρομών ενδέχεται να προκαλέσουν καθυστερήσεις στην προώθηση πακέτων, γεγονός που επηρεάζει την απόδοση εφαρμογών που απαιτούν επικοινωνία σε πραγματικό χρόνο, όπως η ζωντανή μετάδοση βίντεο από UAVs ή η αποστολή εντολών σε μονάδες μάχης. Ο συνεχής επαναϋπολογισμός των διαδρομών αυξάνει τον υπολογιστικό φόρτο και επηρεάζει την ποιότητα υπηρεσίας(QoS) [117], [121].

Εξίσου σημαντική είναι η κατανάλωση ενέργειας. Οι φορητοί κόμβοι, όπως οι στρατιώτες ή τα drones, διαθέτουν περιορισμένες ενεργειακές δυνατότητες, και η συνεχής δρομολόγηση πακέτων ή η χρήση ισχυρών πομπών αυξάνει την κατανάλωση, μειώνοντας τον χρόνο λειτουργίας τους χωρίς επαναφόρτιση ή αντικατάσταση μπαταριών [108], [110].

Για την αντιμετώπιση αυτών των ζητημάτων, η σύγχρονη έρευνα επικεντρώνεται σε αρκετές καινοτόμες τεχνολογικές κατευθύνσεις. Τα Cognitive Radios θεωρούνται μια πολλά υποσχόμενη λύση, καθώς επιτρέπουν στους κόμβους να διαχειρίζονται αυτόματα το φάσμα συχνοτήτων, αποφεύγοντας παρεμβολές και βελτιστοποιώντας την εκπομπή σήματος ανάλογα με τις συνθήκες [55].

Παράλληλα, η υιοθέτηση αλγορίθμων δρομολόγησης που βασίζονται στην τεχνητή νοημοσύνη (AI-driven Routing) προσφέρει νέες δυνατότητες προσαρμογής σε μεταβαλλόμενες τοπολογίες και συνθήκες παρεμβολής, διασφαλίζοντας βέλτιστη απόδοση δικτύου με μειωμένη ανθρώπινη παρέμβαση.

Τέλος, η συνεργασία των MANETs με δίκτυα πέμπτης γενιάς (5G) και την αρχιτεκτονική Internet of Military Things (IoMT) αναμένεται να ανοίξει νέους δρόμους για την ανάπτυξη πλήρως

διασυνδεδεμένων, υψηλής χωρητικότητας και χαμηλής καθυστέρησης στρατιωτικών δικτύων. Ο συνδυασμός των MANETs με IoMT υπόσχεται την πλήρη δικτύωση αισθητήρων, φορητών συσκευών και έξυπνων όπλων σε ένα κοινό πληροφοριακό πεδίο, μεγιστοποιώντας την επίγνωση κατάστασης και την επιχειρησιακή ευελιξία [111], [122].

Συνοψίζοντας, τα MANETs αποτελούν βασικό εργαλείο για την εξασφάλιση ευέλικτης και ανθεκτικής επικοινωνίας σε δυναμικά στρατιωτικά περιβάλλοντα. Η συνεχής εξέλιξη των τεχνολογιών routing, η ενσωμάτωση τεχνητής νοημοσύνης και η σύζευξη με νέες υποδομές όπως το IoMT και το 5G αναμένεται να ενισχύσουν περαιτέρω τις δυνατότητες των MANETs. Ως εκ τούτου, παραμένουν στο επίκεντρο της έρευνας και ανάπτυξης για προηγμένα τακτικά δίκτυα επόμενης γενιάς.

4.3 Πρωτόκολλα Ασφαλούς Επικοινωνίας(IPsec,HAIPE,TACLANE)

Η ασφάλεια στις στρατιωτικές τηλεπικοινωνίες αποτελεί έναν από τους πλέον κρίσιμους παράγοντες για την επιτυχία και την προστασία των επιχειρήσεων στο πεδίο μάχης. Σε αντίθεση με τα εμπορικά δίκτυα, όπου η παραβίαση ή απώλεια δεδομένων μπορεί να έχει κυρίως οικονομικές συνέπειες, στα στρατιωτικά δίκτυα η απώλεια εμπιστευτικών πληροφοριών ή η παρεμβολή στην επικοινωνία μπορεί να οδηγήσει σε επιχειρησιακή αποτυχία ή ακόμη και σε απώλεια ανθρώπινων ζωών [124], [125].

Η προστασία των βασικών αρχών της κυβερνοασφαλείας -εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητας (CIA triad)- είναι ζωτικής σημασίας για την επιβίωση και την αποτελεσματικότητα των Ένοπλων Δυνάμεων. Τα στρατιωτικά δίκτυα καλούνται να λειτουργούν με αυξημένα επίπεδα αξιοπιστίας και ανθεκτικότητας, ακόμη και σε απομακρυσμένες, αποδιοργανωμένες ή εχθρικά ελεγχόμενες περιοχές. Οι επιχειρησιακές απαιτήσεις συχνά περιλαμβάνουν περιορισμένους πόρους, έντονη κινητικότητα και δυναμικές συνθήκες επικοινωνίας [124], [126].

Για την κάλυψη αυτών των αναγκών, έχουν αναπτυχθεί εξειδικευμένα πρωτόκολλα και τεχνολογίες ασφάλειας που ανταποκρίνονται στις προκλήσεις του τακτικού και στρατηγικού περιβάλλοντος.

Η παρούσα ενότητα επικεντρώνεται στην παρουσίαση και ανάλυση τριών βασικών πρωτοκόλλων ασφαλούς επικοινωνίας που εφαρμόζονται ευρέως σε στρατιωτικά δίκτυα:

- το IPsec (Internet Protocol Security),
- το HAIPE (High Assurance Internet Protocol Encryptor) και
- το TACLANE (Tactical Local Area Network Encryptor).

Κάθε τεχνολογία εξετάζεται ως προς την αρχιτεκτονική της, τον τρόπο λειτουργίας, τις δυνατότητες και τις εφαρμογές της σε σύγχρονες στρατιωτικές υποδομές.

4.3.1 IPsec-Το θεμέλιο της ασφάλειας σε επίπεδο IP

Το IPsec (Internet Protocol Security) αποτελεί ένα διεθνώς αναγνωρισμένο σύνολο πρωτοκόλλων ασφαλείας, σχεδιασμένο για την προστασία της επικοινωνίας σε επίπεδο δικτύου (Layer 3) του μοντέλου OSI. Στόχος του είναι η εξασφάλιση της εμπιστευτικότητας, της ακεραιότητας και την αυθεντικότητας των IP πακέτων, καθώς αυτά διακινούνται μέσα από μη ασφαλή δίκτυα, όπως το Διαδίκτυο ή ευαίσθητες στρατιωτικές υποδομές [123], [127], [128].

Σε αντίθεση με μηχανισμούς που εφαρμόζονται σε ανώτερα επίπεδα, όπως το SSL/TLS στο transport ή application layer, το IPsec λειτουργεί πιο «βαθιά» στη στοίβα πρωτοκόλλων, επιτρέποντας την προστασία κάθε τύπου εφαρμογών και δεδομένων ανεξάρτητα από το πρωτόκολλο μεταφοράς. Αυτή η προσέγγιση το καθιστά ιδανικό για συστηματική προστασία σε στρατιωτικά περιβάλλοντα, όπου η ασφάλεια πρέπει να εφαρμόζεται ενιαία σε όλες τις επικοινωνίες, από τα backhaul δίκτυα έως τα αισθητήρια πεδίου [123].

Η υιοθέτηση του από τον NATO και η ενσωμάτωση του σε πρότυπα STANAG διασφαλίζουν πλήρη διαλειτουργικότητα μεταξύ συμμαχικών δυνάμεων, επιτρέποντας ασφαλείς επικοινωνίες ακόμη και σε πολυεθνικές επιχειρήσεις. Η ευρεία χρήση του τόσο σε σταθερά στρατηγικά δίκτυα όσο και σε τακτικά περιβάλλοντα αναδεικνύει τη σημασία του ως θεμέλιο της σύγχρονης στρατιωτικής κυβερνοασφαλείας [129], [130].

Υποπρωτόκολλα του IPsec (AH & ESP) και Λειτουργίες τους

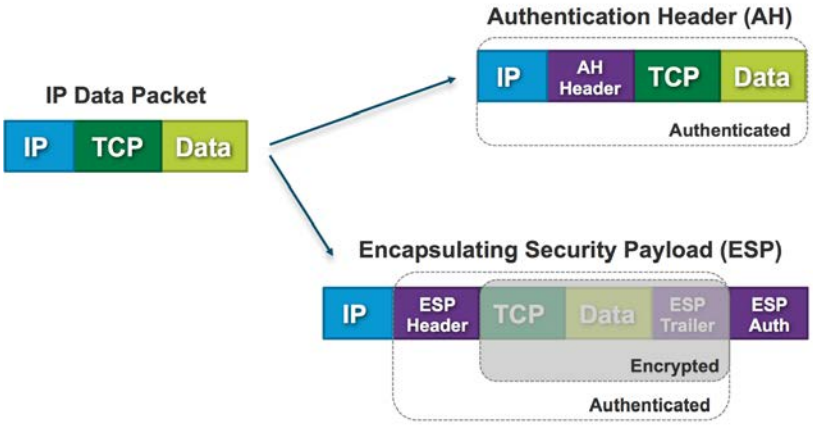
Το IPsec βασίζεται σε βασικά υροπρωτόκολλα για την υλοποίηση των λειτουργιών ασφαλείας: το **Authentication Header (AH)** και το **Encapsulating Security Payload (ESP).** Κάθε ένα από αυτά εξυπηρετεί διαφορετικές ανάγκες προστασίας και μπορεί να χρησιμοποιηθεί ανεξάρτητα ή σε συνδυασμό.Το AH παρέχει αυθεντικοποίηση προέλευσης (source authentication), ακεραιότητα δεδομένων (data integrity), προστασία από επιθέσεις αναπαραγωγής (anti-replay protection)

Ωστόσο, δεν προσφέρει κρυπτογράφηση – άρα δεν διατηρεί την εμπιστευτικότητα του περιεχομένου. Το AH καλύπτει τόσο το περιεχόμενο όσο και τα στατικά τμήματα της IP κεφαλίδας, διασφαλίζοντας ότι δεν έχει αλλοιωθεί κατά τη μεταφορά [128].

Το ESP είναι το πιο διαδεδομένο υποπρωτόκολλα του IPsec, καθώς προσφέρει κρυπτογράφηση του φορτίου δεδομένων, προαιρετική αυθεντικοποίηση, ακεραιότητα και anti-replay protection μέσω αλγορίθμων όπως AES και 3DES.

Στις περισσότερες στρατιωτικές υλοποιήσεις IPsec, το ESP αποτελεί την κύρια επιλογή, ιδιαίτερα σε συνδυασμό με ισχυρούς αλγορίθμους κρυπτογράφησης όπως το AES-256, ακριβώς λόγω

της ανάγκης προστασίας διαβαθμισμένων πληροφοριών. Επιπλέον, όταν απαιτείται επαλήθευση ταυτότητας χωρίς αποκάλυψη περιεχομένου, μπορεί να χρησιμοποιηθεί το AH ή να συνδυαστεί με ESP [126].



Σχήμα 33-Δομή πακέτων IPsec με AH και ESP(χωρίς modes)

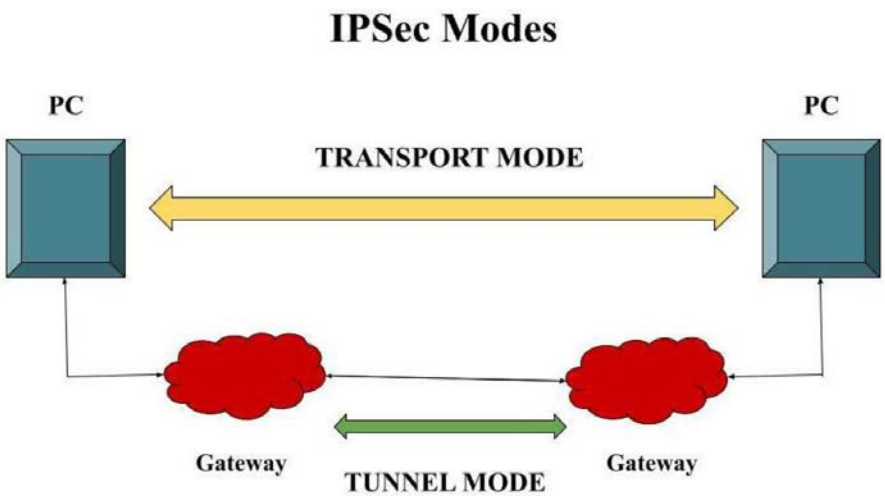
Το Σχήμα 33 αποτυπώνει τη βασική δομή των IP πακέτων όταν εφαρμόζεται το AH και το ESP. Στην περίπτωση του AH, προστίθεται ένας επί πλέον header μετά τον IP header που εξασφαλίζει την αυθεντικοποίηση και την ακεραιότητα, χωρίς όμως κρυπτογράφηση. Αντίθετα, το ESP εισάγεται με ένα header και trailer, κρυπτογραφεί το TCP/UDP payload και προσφέρει επιπλέον αυθεντικοποίηση και την προστασία from relay attacks. Αυτή η ξεκάθαρη απεικόνιση βοηθά στην κατανόηση των βασικών διαφορών ανάμεσα στα δύο πρωτόκολλα, χωρίς τη σύγχυση των λειτουργικών modes.

Λειτουργικές Στάσεις: Transport Mode και Tunnel Mode

Το IPsec μπορεί να λειτουργήσει σε διαφορετικές λειτουργικές στάσεις (modes), που καθορίζουν πως εφαρμόζεται η ασφάλεια στα IP πακέτα και για ποιες περιπτώσεις είναι κατάλληλη η κάθε προσέγγιση.

Στο transport mode, το IPsec προστατεύει μόνο το φορτίο (payload) του IP πακέτου, αφήνοντας την IP επικεφαλίδα (IP header) ανέπαφη. Η μορφή αυτή χρησιμοποιείται κυρίως σε επικοινωνίες μεταξύ δύο τερματικών με σχέση εμπιστοσύνης, όπως υπολογιστές ή servers εντός ασφαλών δικτύων, και είναι κατάλληλη για εφαρμογές όπου απαιτείται χαμηλό latency (π.χ. VoIP, SIP ή) [123].

Στο tunnel mode, το IPsec κρυπτογραφεί ολόκληρο το IP πακέτο, και προσθέτει μια νέα IP επικεφαλίδα για την ενθυλάκωση. Η μέθοδος αυτή χρησιμοποιείται ευρέως στη δημιουργία Virtual Private Networks(VPNs) και αποτελεί την τυπική επιλογή για στρατιωτικά δίκτυα και δορυφορικές ζεύξεις, όπου απαιτείται πλήρης προστασία των δεδομένων κατά τη μεταφορά [123], [130].

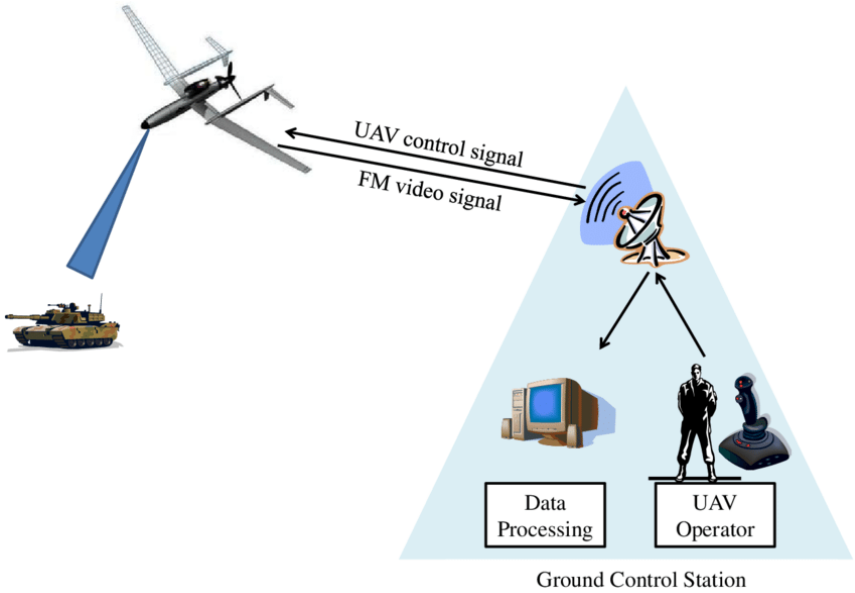


Σχήμα 34-Απεικόνιση των δύο λειτουργικών τάσεων(Transport & Tunnel Mode) του IPsec [123]

Το Σχήμα 34 δείχνει το Transport Mode, όπου η επικοινωνία είναι άμεση μεταξύ δύο τερματικών (PC-PC) και προστατεύεται μόνο το payload. Η κάτω απεικόνιση δείχνει το Tunnel Mode, όπου η επικοινωνία διέρχεται μέσω δύο πυλών (getaways), κρυπτογραφώντας ολόκληρο το IP πακέτο.

Πλεονεκτήματα και Τυπικές Χρήσεις του IPsec σε Στρατιωτικά Δίκτυα

Το IPsec παραμένει ένα από τα πιο αξιόπιστα και καθιερωμένα πρωτόκολλα ασφαλείας στο επίπεδο δικτύου, προσφέροντας κρίσιμα πλεονεκτήματα όπως εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση, προστασία από επιθέσεις αναπαραγωγής, διαλειτουργικότητα και ευελιξία εφαρμογής [123], [124], [127], [126].,[128], [129], [130].



Σχήμα 35-Απεικόνιση ασφαλούς μετάδοσης δεδομένων UAV μέσω IPsec σε πλατφόρμες ISR.

Οι τυπικές στρατιωτικές εφαρμογές του περιλαμβάνουν tactical VPNs για ασφαλή σύνδεση κέντρων διοίκησης με προκεχωρημένες βάσεις, δορυφορικά links(SATCOM) που εξασφαλίζουν την

εμπιστευτικότητα των δεδομένων σε μη ασφαλή δίκτυα και UAV/ISR πλατφόρμες όπου προστατεύονται βίντεο, τηλεμετρία και αισθητηριακά δεδομένα κατά τη μεταφορά [126], [131]. Επιπλέον, σε πολυεθνικές επιχειρήσεις, το IPsec διευκολύνει τη διαλειτουργικότητα μέσω κοινών κλειδιών και πιστοποιημένων αλγορίθμων όπως ορίζονται από τα NATO STANGs [129], [130].

Η λειτουργία ενός τέτοιου σεναρίου παρουσιάζεται στο Σχήμα35, όπου φαίνεται η ασφαλής μετάδοση δεδομένων μεταξύ UAV και επίγειου σταθμού ελέγχου(GCS). Το IPsec εξασφαλίζει την εμπιστευτικότητα, την ακεραιότητας και την αυθεντικοποίηση των ροών δεδομένων, προστατεύοντας κρίσιμες πληροφορίες από παρεμβολές ή παραποίηση.

Προκλήσεις & Περιορισμοί του IPsec σε MANETs & Ad hoc δίκτυα

Παρά τα πολλαπλά πλεονεκτήματα του, η εφαρμογή του IPsec σε δυναμικά και κινητικά περιβάλλοντα όπως τα MANETs αντιμετωπίζει σημαντικές δυσκολίες. Η κρυπτογράφηση και αυθεντικοποίηση προσθέτουν υπολογιστικό φόρτο και αύξηση μεγέθους πακέτων, επιβραδύνοντας την επικοινωνία – κρίσιμο σε real-time εφαρμογές όπως τηλεμετρία από UAVs [123], [126]. Η διαχείριση Κλειδιών (Key Management) γίνεται δυσχερής λόγω της συνεχούς αλλαγής τοπολογίας και της απουσίας κεντρικής υποδομής [107], [132], [133]. Επιπλέον, τα κινητά πρωτόκολλα δρομολόγησης (όπως AODV, DSR) δημιουργούν αστάθεια στις συνδέσεις, καθιστώντας δύσκολη τη διατήρηση έγκυρων Sas, καθώς και τη συνεχή εφαρμογή πολιτικών IPsec [118], [100]. Η υψηλή κατανάλωση ενέργειας λόγω της πρόσθετης επεξεργασίας μπορεί να περιορίσει τη διάρκεια λειτουργίας φορητών τερματικών και drones [108], [110], ενώ η Ενσωμάτωσή του σε υφιστάμενες πλατφόρμες χρησιμοποιούν παραλλαγές του IPsec ή άλλα πρωτόκολλα (π.χ. HAIPE). Η άμεση ενσωμάτωση του καθαρού IPsec μπορεί να απαιτεί μετατροπές σε υλικό ή firmware [131], [134].

4.3.2 HAIPE-Στρατιωτική επέκταση του IPsec

Το HAIPE (High Assurance Internet Protocol Encryptor) είναι μία στρατιωτική τεχνολογία κρυπτογράφησης δικτύου, η οποία έχει σχεδιαστεί και πιστοποιηθεί από την NSA(National Security Agency) για την προστασία διαβαθμισμένων πληροφοριών, συμπεριλαμβανομένων δεδομένων με σήμανση Top Secret/Sensitive Compartmented Information (TS/SCI), κατά τη μεταφορά τους μέσω IP δικτύων [131], [134].

Η βασική αρχή λειτουργίας του HAIPE βασίζεται στην προδιαγραφή IPsec και συγκεκριμένα στο IPsec ESP για την παροχή εμπιστευτικότητας, ακεραιότητας και αυθεντικοποίησης των πακέτων IP. Ωστόσο, το HAIPE δεν είναι απλώς μία υλοποίηση IPsec, αλλά μία υψηλής διασφάλισης (high-assurance) παραλλαγή που ενσωματώνει στρατιωτικού επιπέδου μηχανισμούς διαχείρισης κλειδιών, αυστηρό έλεγχο ταυτότητας και συμμόρφωση με πρότυπα ασφαλείας του Υπουργείου Άμυνας των ΗΠΑ και του ΝΑΤΟ [123], [131].

Σε αντίθεση με το εμπορικό IPsec, το οποίο μπορεί να λειτουργήσει σε ευρύ φάσμα εφαρμογών και περιβαλλόντων, το HAIPE έχει βελτιστοποιηθεί για ασφαλή διασύνδεση στρατιωτικών δικτύων σε τακτικό και στρατηγικό επίπεδο, για διαλειτουργικότητα μεταξύ συστημάτων διαφορετικών κλάδων και χωρών-μελών του ΝΑΤΟ μέσω πρότυπων NATO STANAG 5068/4677 και για αντοχή σε επιθέσεις και συμμόρφωση με απαιτήσεις NSA Type 1.

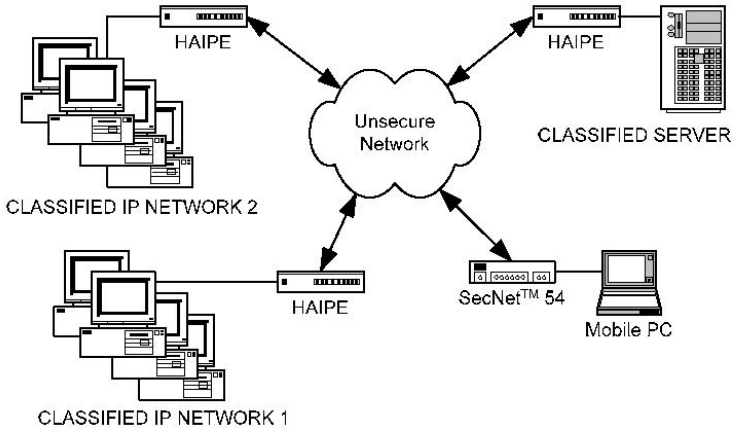
Το HAIPE μπορεί να θεωρηθεί ως η στρατηγικά πιστοποιημένη, ενισχυμένη και πλήρως διαλειτουργική μορφή του IPsec, σχεδιασμένη για να ανταποκρίνεται στις αυστηρότερες απαιτήσεις ασφαλείας που συναντώνται σε επιχειρησιακά περιβάλλοντα υψηλού κινδύνου [129], [135].

Κεντρική διαφοροποίηση του HAIPE είναι η πιστοποίηση NSA Type 1 encryption, δηλαδή η χρήση εγκεκριμένων αλγορίθμων για προστασία έως και Top Secret/SCI, με προδιαγραφές που δεν είναι δημόσια διαθέσιμες [131], [132]. Η διαχείριση κλειδιών υλοποιείται με στρατιωτικά πρότυπα EKMS (Electronic Key Management System) και KMI (Key Management Infrastructure) επιτρέποντας ασφαλή προμήθεια, ανανέωση και ανάκληση κλειδιών σε απομακρυσμένα περιβάλλοντα και σε συνθήκες μάχης [133], [136]. Η διαλειτουργικότητα διασφαλίζεται από τις HAIPE Interoperability Specifications και τα σχετικά STANAGs ώστε υλοποιήσεις διαφορετικών κατασκευαστών να συνεργάζονται σε πολυεθνικές επιχειρήσεις [129], [135], ενώ η ενισχυμένη ανθεκτικότητα περιλαμβάνει anti-tamper για φυσική ασφάλεια, καθώς και προστασία από επιθέσεις τύπου traffic analysis, jamming και spoofing, που στοχεύουν να παρακάμψουν ή να υποβαθμίσουν την κρυπτογράφηση [131], [134]. Επιπλέον οι συσκευές υποστηρίζουν δυναμική προσαρμογή σε αλλαγές τοπολογίας, χαμηλή καθυστέρηση για real-time εφαρμογές (π.χ. ISR feeds) και αντοχή σε διακοπές συνδεσιμότητας που χαρακτηρίζουν τα τακτικά δίκτυα πεδίου [126].

Αρχιτεκτονικά, ένα σύστημα HAIPE περιλαμβάνει κρυπτογραφική μονάδα Type 1 (π.χ. AES 256-bit Type 1 variants) [131], μονάδα διαχείρισης κλειδιών συμβατή με EKMS και KMI, επιτρέπει την ασφαλή φόρτωση, αποθήκευση, ανανέωση και διαγραφή κλειδιών [133], [136], διεπαφές δικτύου(Ethernet, οπτικές ίνες και δορυφορικές συνδέσεις (SATCOM)) [134] και το λογισμικό συμμόρφωσης με HAIPE IS, που εγγυάται διαλειτουργικότητα. Η λειτουργία μπορεί να περιγράφει σε τέσσερα βασικά στάδια: τα μη κρυπτογραφημένα (plain) IP πακέτα εισέρχονται στη συσκευή υποβάλλονται σε IPsec-like επεξεργασία με AH και ESP, αλλά με Type 1 αλγορίθμους και ενισχυμένες παραμέτρους ασφαλείας, τα κλειδιά δημιουργούνται ή ανανεώνονται μέσω ασφαλούς καναλιού EKMS/KMI και τα πακέτα εξέρχονται πλήρως κρυπτογραφημένα και έτοιμα για μετάδοση σε οποιοδήποτε δίκτυο, ακόμη και μη ασφαλές.

Το Σχήμα 36 παρουσιάζει δύο διαβαθμισμένα δίκτυα που συνδέονται μέσω ενός ανασφαλούς δικτύου, με τη χρήση HAIPE συσκευών οι οποίες λειτουργούν ως ασφαλείς «γέφυρες», κρυπτογραφώντας και αποκρυπτογραφώντας τη ροή δεδομένων.

Τα κύρια πλεονεκτήματα συνοψίζονται στην πολύ υψηλή διαβάθμιση ασφάλειας(NSA Type 1 για Top Secret/Sensitive Compartmented Information (SCI)) [131], [132], στην αυτόματη και ασφαλή διαχείριση κλειδιών με δυνατότητες Over-the-Air (OTAR) όπου μειώνει τον επιχειρησιακό κίνδυνο και το κόστος συντήρησης [133], [136], στη διαλειτουργικότητα βάσει HAIPE Interoperability Specification (HAIPE IS) [129], [131] και στην αποδεδειγμένη αξιοπιστία σε δύσκολα ηλεκτρομαγνητικά περιβάλλοντα [134]. Η ευελιξία εγκατάστασης σε επίγειες, ναυτικές εναέριες και ακόμη και διαστημικές πλατφόρμες, υποστηρίζοντας πολλαπλά επιχειρησιακά σενάρια [112].



Σχήμα 36-Αρχιτεκτονική δικτύου HAIPE [134]

Αντιστοίχως, οι τυπικές χρήσεις περιλαμβάνουν τη σύνδεση στρατιωτικών κέντρων διοίκησης πάνω από ανασφαλείς ή δημόσιες γραμμές [131], [134], την ασφαλή SATCOM μεταφορά δεδομένων ISR με αντοχή σε spoofing/anti-jamming [126], [134], τη διασύνδεση μονάδων μάχης με HQ μέσω κινητών σταθμών HAIPE, καθώς και την υποστήριξη πολυεθνικών επιχειρήσεων του NATO με κοινά πρότυπα κρυπτογράφησης και ανταλλαγής κλειδιών [129], [135].

Παρά τα σημαντικά πλεονεκτήματα του HAIPE στην προστασία στρατιωτικών επικοινωνιών, η εφαρμογή του σε διαφορετικά επιχειρησιακά σενάρια αντιμετωπίζει ορισμένες προκλήσεις. Η πολυπλοκότητα διαχείρισης κλειδιών αποτελεί κρίσιμο ζήτημα, καθώς το HAIPE χρησιμοποιεί αυστηρά πρωτόκολλα Key Management (π.χ. EKMS, KMI) τα οποία απαιτούν πιστοποιημένο προσωπικό και ασφαλείς υποδομές για την παραγωγή, διανομή και ανανέωση κλειδιών. Σε τακτικά περιβάλλοντα με κινητές μονάδες και υψηλή συχνότητα αλλαγών τοπολογίας, η διαδικασία αυτή μπορεί να καθυστερήσει την επιχειρησιακή ετοιμότητα [133], [136]. Οι υψηλές απαιτήσεις σε εξοπλισμό και πιστοποίηση, καθώς οι συσκευές πρέπει να είναι πιστοποιημένες από την NSA και να πληρούν αυστηρά πρότυπα ασφαλείας (π.χ. Suite A/Suite B algorithms). Αυτό περιορίζει τη διαθεσιμότητα εξοπλισμού και αυξάνει το κόστος προμήθειας και συντήρησης [131], [134]. Επιπλέον, η κατανάλωση ισχύος και το μέγεθος των HAIPE συσκευών μπορεί να αποτελέσει πρόβλημα σε πλατφόρμες με περιορισμένους ενεργειακούς πόρους ή φυσικούς περιορισμούς, όπως UAVs ή μικρά οχήματα μάχης [112]. Μία ακόμη πρόκληση αφορά τη διαλειτουργικότητα. Αν και το HAIPE βασίζεται στο IPsec, χρησιμοποιεί

εξειδικευμένες επεκτάσεις και ρυθμίσεις που μπορεί να μην είναι πλήρως συμβατές με εμπορικές υλοποιήσεις IPsec ή με μη πιστοποιημένες στρατιωτικές πλατφόρμες. Αυτό δημιουργεί ζητήματα σε μικτές επιχειρήσεις, ειδικά όταν συμμετέχουν δυνάμεις από διαφορετικές χώρες που δεν διαθέτουν ίδιες προδιαγραφές συσκευών [131]. Τέλος, η εκπαίδευση και πιστοποίηση του προσωπικού είναι απαραίτητη για την ασφαλή και αποδοτική χρήση του HAIPE. Η ελλιπής εκπαίδευση μπορεί να οδηγήσει σε κακή ρύθμιση, με αποτέλεσμα απώλεια ασφάλειας ή επικοινωνίας [132], [136].

Συνοπτικά, ενώ το HAIPE προσφέρει υψηλή ασφάλεια για κρίσιμες στρατιωτικές επικοινωνίας, η χρήση του απαιτεί σημαντική υποστήριξη σε επίπεδο υλικού, λογισμικού, διαδικασιών και ανθρώπινων πόρων.

4.3.3 TACLANE-Πρακτική εφαρμογή του HAIPE

Το TACLANE (Tactical Local Area Network Encryptor) αποτελεί οικογένεια συσκευών κρυπτογράφησης δικτύου που αναπτύχθηκε από την General Dynamics Mission Systems (GDMS) και χρησιμοποιείται ευρέως από τις Ένοπλες Δυνάμεις των Ηνωμένων Πολιτειών, του ΝΑΤΟ και συμμαχικών χωρών. Ανήκει στην κατηγορία των HAIPE συσκευών, καθώς υλοποιεί πλήρως το πρότυπο HAIPE IS, εξασφαλίζοντας διαλειτουργικότητα μεταξύ συσκευών διαφορετικών κατασκευαστών.

Η αρχιτεκτονική του TACLANE στηρίζεται στο IPsec, αλλά ενσωματώνει επιπλέον μηχανισμούς πιστοποίησης, διαχείρισης κλειδιών και προστασίας σύμφωνα με τις αυστηρές προδιαγραφές της NSA. Όλες οι συσκευές TACLANE διαθέτουν πιστοποίηση NAS Type 1 γεγονός που τις καθιστά κατάλληλες για τη διαχείριση πληροφοριών επιπέδου Top Secret/SCI.

Σε αντίθεση με το IPsec που είναι λογισμικό πρωτόκολλο, το TACLANE αποτελεί υλικό κρυπτογράφησης (hardware encryptor), εξασφαλίζοντας υψηλή απόδοση και προστασία έναντι φυσικών και κυβερνοεπιθέσεων. Αυτός ο συνδυασμός το καθιστά βασικό στοιχείο σε στρατιωτικά δίκτυα που απαιτούν ασφάλεια, αξιοπιστία και ανθεκτικότητα ακόμη και σε ιδιαίτερα απαιτητικά περιβάλλοντα μάχης [112].

Σε επίπεδο αρχιτεκτονικής, οι συσκευές TACLANE υποστηρίζουν αλγόριθμους υψηλής διαβάθμισης (π.χ. AES-256/GCM, NSA Type 1), ενσωματώνουν Over-the-Air Rekeying (OTAR) για δυναμική ανανέωση κλειδιών χωρίς φυσική παρέμβαση και συμμορφώνονται πλήρως με το HAIPE IS, διασφαλίζοντας επικοινωνία μεταξύ συμμαχικών δυνάμεων (π.χ. ΝΑΤΟ). Λειτουργούν ως «gateway» κρυπτογράφησης σε routers, tactical servers ή φορητές συσκευές, κρυπτογραφώντας επικοινωνία μεταξύ τοπικών και απομακρυσμένων δικτύων ενώ υποστηρίζουν IP4v, IP6v, multicast traffic [113], [112]. Από πλευράς επιδόσεων, καλύπτουν εύρος ρυθμών μετάδοσης από 200 Mbps (μικρότερα μοντέλα) έως και 20 Gbps (υψηλής απόδοσης TACLANE-20G) με ειδικές παραλλαγές φορητότητας όπως το TACLANE- Micro για UAVs, οχήματα ή φορητά τερματικά. Για διαχείριση, παρέχουν κεντρικοποιημένα εργαλεία διαχείρισης συμβατά με Key Management Infrastructure-KMI)[50].

Παρά την υψηλή αξιοπιστία και την τυποποίηση NSA Type 1, το TACLANE αντιμετωπίζει συγκεκριμένες προκλήσεις . Το κόστος απόκτησης και συντήρησης είναι υψηλό λόγω πιστοποίησης από την NSA και ανήκουν στην κατηγορία Type 1 cryptographic devices, κάτι που αυξάνει σημαντικά το κόστος προμήθειας, συντήρησης και αντικατάστασης, ειδικά για μικρότερες στρατιωτικές μονάδες [137]. Η διαχείριση απαιτεί εξειδικευμένη εκπαίδευση και ακριβή τήρηση διαδικασιών Key Management, αλλιώς αυξάνεται ο κίνδυνος σφαλμάτων [133], [136]. Επιπρόσθετα, παρά τις πιο πρόσφατες μικρότερες εκδόσεις (π.χ. TACLANE-Nano), πολλές συσκευές παραμένουν ενεργοβόρες και με περιορισμούς σε φορητές εφαρμογές. Αυτό μπορεί να είναι πρόβλημα για UAVs, στρατιωτικά οχήματα με περιορισμένο χώρο ή μονάδες που βασίζονται σε φορητές μπαταρίες [112]. Τέλος, η συνεχής εξάρτηση από πιστοποιήσεις της NSA(ανανεώσεις, αποχαρακτηρισμοί παλαιότερων μοντέλων) επηρεάζει τον κύκλο ζωής και την επιχειρησιακή διαθεσιμότητα [131].

Παρά τα παραπάνω, τα πλεονεκτήματα του TACLANE είναι καθοριστικά. Η υψηλή ασφάλεια που εξασφαλίζεται από NSA Type 1 και ισχυρούς κρυπτογραγικούς μηχανισμούς [131], [137], η φορητότητα και ανθεκτικότητα των νεότερων εκδόσεων (π.χ. TACLANE Nano-KG-175N [112], οι υψηλές επιδόσεις κρυπτογράφησης σε ταχύτητες έως και 200 Mbps full duplex, με δυνατότητα αναβάθμισης ανάλογα με το μοντέλο [137], [112] και η διαλειτουργικότητα βάση HAIPE IS, εξασφαλίζοντας συμβατότητα με συσκευές διαφορετικών κατασκευαστών και απρόσκοπτη χρήση σε πολυεθνικά περιβάλλοντα, όπως το NATO [131], [137]. Η ευελιξία ανάπτυξης σε επίγειες, εναέριες, θαλάσσιες και δορυφορικές πλατφόρμες, καλύπτοντας ένα μεγάλο φάσμα επιχειρησιακών αναγκών [137], [112].

Τυπικά επιχειρησιακά σενάρια περιλαμβάνουν Διοίκηση και Έλεγχος (C2) με προστασία δεδομένων σε πραγματικό χρόνο μεταξύ στρατηγικών κέντρων και απομακρυσμένων μονάδων [137], SATCOM Links για ασφαλή δορυφορική επικοινωνία για μεταφορά δεδομένων ISR [126], [137], UAVs & ISR Platforms με προστασία τηλεμετρίας και εικόνων που μεταδίδονται από UAVs, κρίσιμο για την αξιοπιστία και την εμπιστευτικότητα πληροφοριών πεδίου [112] και Joint Operations: όπου απαιτείται κοινή πολιτική κρυπτογράφησης και τυποποίηση ασφάλειας σε πολυεθνικά οχήματα[129], [131].

Συνολικά, το TACLANE αποτελεί μία ώριμη και αξιόπιστη τεχνολογία που εξισορροπεί υψηλή ασφάλεια, φορητότητα και επιχειρησιακή ευελιξία, καθιστώντας το αναπόσπαστο κομμάτι των στρατιωτικών επικοινωνιών αιχμής.

Η TACLANE-Nano(KG-175N)(βλέπε Σχήμα 37) αποτελεί τη μικρότερη και ελαφρύτερη συσκευή της οικογένειας HAIPE, ειδικά σχεδιασμένη για φορητές και κινητές εφαρμογές. Υποστηρίζει κρυπτογράφηση έως και 100 Mbps full-duplex, καλύπτοντας απαιτήσεις για ασφαλή μετάδοση δεδομένων σε UAVs, απομακρυσμένες αποστολές ή σε μικρές μονάδες πεδίου που απαιτούν κρυπτογραφημένη επικοινωνία σε πραγματικό χρόνο. Η υψηλή ανθεκτικότητα σε κραδασμούς, θερμοκρασίες και υγρασία καθιστά την TACLANE-Nano αξιόπιστη ακόμα και στα πιο αντίξοα

επιχειρησιακά περιβάλλοντα, ενώ υποστηρίζει ασφαλείς διασυνδέσεις μεταξύ κόμβων με διαφορετικά επίπεδα ασφαλείας.



Σχήμα 37-TACLANE-Nano(KG-175N) [112]

4.3.4 Σύγχρονες απειλές και μελλοντικές κατευθύνσεις

Παρά την υψηλή αξιοπιστία που παρέχουν οι τεχνολογίες HAIPE και οι συσκευές TACLANE στις σημερινές στρατιωτικές τηλεπικοινωνίες, οι εξελίξεις στο κυβερνοχώρο και η αυξανόμενη πολυπλοκότητα των επιχειρησιακών δικτύων φέρνουν στο προσκήνιο νέες προκλήσεις που απαιτούν συνεχή προσαρμογή. Οι σύγχρονες προκλήσεις σχετίζονται τόσο με τη διαλειτουργικότητα και την κλιμάκωση των συστημάτων, όσο και με την εμφάνιση νέων τεχνολογικών παραμέτρων που απαιτούν επαναπροσδιορισμό στρατηγικών ασφαλείας.

Μία από τις πιο σοβαρές προκλήσεις είναι η ασυμβατότητα μεταξύ παλαιότερων (legacy) και νεότερων συσκευών κρυπτογράφησης. Η συνύπαρξη αυτών των συστημάτων συχνά δυσχεραίνει τη διαχείριση των δικτύων, καθώς απαιτείται πρόσθετος συντονισμός για την εξασφάλιση της διαλειτουργικότητας σε πολυεθνικές επιχειρήσεις του NATO, όπου συμμετέχουν δυνάμεις με διαφορετικά επίπεδα τεχνολογικού εξοπλισμού [138].

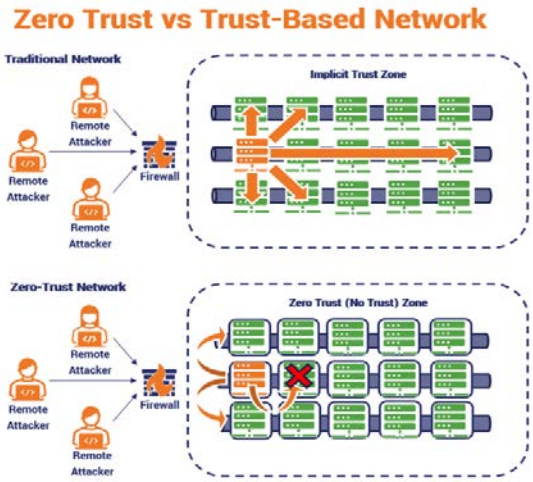
Εξίσου κρίσιμο ζήτημα αποτελεί η ασφαλής διανομή και διαχείριση κλειδιών κρυπτογράφησης. Σε δυναμικά περιβάλλοντα όπως τα MANETs, η συνεχής αλλαγή τοπολογίας και η κινητικότητα των κόμβων καθιστούν δυσχερή τη διατήρηση ασφαλών Security Associations (SAs). Αυτό καθιστά απαραίτητη την ανάπτυξη αυτοματοποιημένων, αποκεντρωμένων και ανθεκτικών μηχανισμών διαχείρισης κλειδιών, οι οποίοι θα μπορούν να προσαρμόζονται σε απρόβλεπτες επιχειρησιακές συνθήκες [123].

Η εφαρμογή της αρχιτεκτονικής Zero-Trust έρχεται να ενισχύσει το πλαίσιο ασφαλείας. Σε αντίθεση με τα παραδοσιακά μοντέλα που θεωρούσαν ασφαλή την εσωτερική επικοινωνία, το Zero-Trust επιβάλλει πιστοποίηση ταυτότητας και έλεγχο πρόσβασης σε κάθε σημείο του δικτύου. Έτσι μειώνεται η επιφάνεια επίθεσης τόσο από εξωτερικούς όσο και από εσωτερικούς κίνδυνους [139].

Σε μελλοντική προοπτική, η έρευνα επικεντρώνεται σε καινοτόμες τεχνολογίες που υπόσχονται ενίσχυση της ανθεκτικότητας:

- Οι μέθοδοι Post-Quantum Encryption προορίζονται να αντέχουν σε επιθέσεις από κβαντικούς υπολογιστές, οι οποίοι ενδέχεται να καταστήσουν αδύναμη την παραδοσιακή κρυπτογραφία (π.χ. RSA, ECC) [139].
- Η αξιοποίηση της Τεχνητής Νοημοσύνης (AI-driven Security) παρέχει δυνατότητα για έγκαιρη ανίχνευση ανωμαλιών και ταχύτερη απόκριση σε επιθέσεις, ακόμα και χωρίς ανθρώπινη παρέμβαση [140].
- Η ενσωμάτωση με δίκτυα 5G και συστήματα tactical edge μειώνει δραστικά την καθυστέρηση (latency) και επιτρέπει αποδοτικότερη συνεργασία με αισθητήρες, UAVs και άλλα δίκτυα πεδίου μάχης [141].

Τέλος, η τυποποίηση μέσω των NATO STANAGs διασφαλίζει ότι οι νέες τεχνολογίες παραμένουν διαλειτουργικές και μπορούν να χρησιμοποιηθούν σε πολυεθνικές επιχειρήσεις. Έτσι, παρά την πολυπλοκότητα των απειλών, οι στρατιωτικές επικοινωνίες θα παραμείνουν ασφαλείς και ανθεκτικές στο μέλλον [142].



Σχήμα 38-Zero-Trust vs. Παραδοσιακό δίκτυο [139]

Στο Σχήμα 38 γίνεται σύγκριση του παραδοσιακού (trust-based) μοντέλου και του Zero-Trust μοντέλου ασφαλείας. Στο Zero-Trust, καμία άτυπη εμπιστοσύνη δεν παραχωρείται όλες οι επικοινωνίες υποβάλλονται σε πιστοποίηση και έλεγχο για να ενισχυθεί η ασφάλεια και η ανθεκτικότητα

4.4 Δορυφορικά Συστήματα Επικοινωνιών(SATCOM) σε στρατιωτικές εφαρμογές

Η δορυφορική επικοινωνία (SATCOM) αποτελεί έναν από τους πιο κρίσιμους πυλώνες των σύγχρονων στρατιωτικών επιχειρήσεων, καθώς προσφέρει αξιόπιστη, μεγάλης εμβέλειας και ανθεκτική μετάδοση φωνής, δεδομένων και εικόνας, ακόμη και στις πιο απομακρυσμένες ή απρόσιτες περιοχές του πλανήτη. Σε αντίθεση με τις επίγειες υποδομές, τα δορυφορικά δίκτυα δεν εξαρτώνται από τοπική γεωγραφία, τις καιρικές συνθήκες ή την ύπαρξη σταθερών γραμμών επικοινωνίας, γεγονός

που τα καθιστά λιγότερο ευάλωτα σε φυσικές καταστροφές, εχθρικές επιθέσεις ή δολιοφθορά [140], [143], [144].

Η δυνατότητα συνεχούς και σχεδόν καθολικής κάλυψης που προσφέρει το SATCOM είναι ιδιαίτερα σημαντική για την υποστήριξη τόσο στρατηγικών όσο και τακτικών αποστολών. Στρατηγικά, τα δορυφορικά συστήματα εξασφαλίζουν τη σύνδεση ανώτατων διοίκησης κέντρων με δυνάμεις που επιχειρούν σε διαφορετικές γεωγραφικές ζώνες[65], επιτρέποντας τον συγχρονισμό πολλαπλών μονάδων σε διεθνείς επιχειρήσεις. Σε τακτικό επίπεδο, παρέχουν στις ομάδες πεδίου, στα οχήματα μάχης και στα μη επανδρωμένα συστήματα(UAVs) την απαραίτητη επικοινωνία με τα κέντρα ελέγχου και διοίκησης, υποστηρίζοντας τη ζωντανή μετάδοση δεδομένων αναγνώρισης, τηλεμετρίας και βίντεο [112], [145], [146].

Επιπλέον, τα δίκτυα SATCOM μπορούν να λειτουργούν αυτόνομα ή σε συνδυασμό με άλλα επίγεια και ad-hoc δίκτυα (όπως τα MANETs), σχηματίζοντας ένα πολυεπίπεδο επικοινωνιακό πλέγμα που αυξάνει την ανθεκτικότητα και την ευελιξία του στρατιωτικού δικτύου συνολικά [108], [147].

4.4.1 Κατηγορίες στρατιωτικών δορυφορικών συστημάτων

Ανάλογα με τον τύπο της αποστολής, τις απαιτήσεις σε ταχύτητα μετάδοσης, το εύρος ζώνης και επίπεδο ασφαλείας, τα στρατιωτικά δορυφορικά συστήματα κατατάσσονται σε κατηγορίες βάσει της τροχιάς τους γύρω από τη Γη [140].

- Η κατηγορία GEO(Geostationary Earth Orbit) περιλαμβάνει δορυφόρους που βρίσκονται σε ύψος περίπου 36.000 km από τον ισημερινό και παραμένουν σταθεροί σε σχέση με την επιφάνεια της Γης. Αυτό τους επιτρέπει να καλύπτουν μεγάλες γεωγραφικές περιοχές με σταθερή σύνδεση, καθιστώντας τους ιδανικούς για συνεχή παρακολούθηση, στρατηγική επικοινωνία και υπηρεσίες μετάδοσης μεγάλης κλίμακας όπως το Global Broadcast Service(GBS). Παρά το πλεονέκτημα της σταθερότητας, οι GEO δορυφόροι παρουσιάζουν αυξημένο χρόνο καθυστέρησης (latency) λόγω της μεγάλης απόστασης, που μπορεί να φτάνει τα 500-600ms, κάτι που επηρεάζει εφαρμογές που απαιτούν άμεση απόκριση [140].
- Οι δορυφόροι MEO(Medium Earth Orbit) τοποθετούνται σε μέση τροχιά, συνήθως μεταξύ 5.000 και 20.000 km από την επιφάνεια της Γης. Χρησιμοποιούνται κυρίως για πλοήγηση και συστήματα εντοπισμού θέσης όπως το GPS, καθώς προσφέρουν καλύτερη απόκριση σε σχέση με τους GEO και καλύπτουν ευρύτερες περιοχές από τους LEO. Σε στρατιωτικό επίπεδο, οι MEO δορυφόροι υποστηρίζουν εφαρμογές πλοήγησης ακριβείας, συγχρονισμό επιχειρήσεων και επικοινωνία σε μέση κλίμακα [140].

- Η κατηγορία LEO(Low Earth Orbit) αφορά δορυφόρους που βρίσκονται σε χαμηλές τροχιές, περίπου 500-2.000 km από την επιφάνεια της Γης. Αυτοί οι δορυφόροι διακρίνονται για το χαμηλό χρόνο καθυστέρησης και την ικανότητα υποστήριξης τακτικών και ευέλικτων αποστολών. Η χαμηλή τους τροχιά επιτρέπει την παροχή υπηρεσιών υψηλού bandwidth και real-time μεταφοράς δεδομένων, όπως για τη μετάδοση ζωντανού βίντεο από UAVs ή για την παρακολούθηση κινητών στόχων (mobility tracking). Ωστόσο, απαιτούνται μεγάλοι αστερισμοί LEO δορυφόρων για την εξασφάλιση συνεχούς κάλυψης, κάτι που αυξάνει το λειτουργικό κόστος και την πολυπλοκότητα διαχείρισης [140], [148].

Κάθε τροχιακή κατηγορία παρουσιάζει πλεονεκτήματα και μειονεκτήματα ως προς την κάλυψη περιοχών, τον χρόνο καθυστέρησης, το επίπεδο ασφαλείας και την ευπάθεια σε στοχευμένες επιθέσεις. Ο σωστός συνδυασμός διαφορετικών τροχιών -μέσω hybrid satellite networks – επιτρέπει στις ένοπλες δυνάμεις να εκμεταλλεύονται τα πλεονεκτήματα κάθε κατηγορίας για μέγιστη επιχειρησιακή ευελιξία και ανθεκτικότητα [141].

4.4.2 Στρατιωτικά συστήματα SATCOM

Οι ένοπλες δυνάμεις του ΝΑΤΟ και άλλων συμμαχικών κρατών αξιοποιούν ένα ευρύ φάσμα προηγμένων δορυφορικών συστημάτων επικοινωνίας (SATCOM) ώστε να καλύψουν τόσο στρατηγικές όσο και τακτικές επιχειρησιακές ανάγκες. Αυτά τα συστήματα σχεδιάζονται με γνώμονα την ανθεκτικότητα σε παρεμβολές, την προστασία της εμπιστευτικότητας των δεδομένων και την διαλειτουργικότητα μεταξύ πολλών εθνικών δικτύων, σύμφωνα με τα πρότυπα STANAGs.

Ένα από τα πρώτα και ιστορικά σημαντικά προγράμματα είναι το MILSTAR (Military Strategic and Tactical Relay), ήταν το πρώτο σύστημα που επικεντρώθηκε στην απόλυτη ανθεκτικότητα. Αποτελούμενο από γεωστατικούς(GEO) δορυφόρους, παρέχει επικοινωνία σε πολύ χαμηλούς ρυθμούς μετάδοσης(75 bps-1,5Mbps) με κορυφαία αξιοπιστία ακόμη και σε περιβάλλοντα έντονου ηλεκτρονικού πολέμου. Οι τεχνικές anti-jamming, η χρήση προηγμένων αλγορίθμων κωδικοποίησης και η δυνατότητα επιβίωσης σε πυρηνικά σενάρια(nuclear survivability) το κατέστησαν ακρογωνιαίο λίθο για στρατιωτικές επικοινωνίες [149].

Ως φυσικός διάδοχος του MILSTAR, το AEHF (Advanced Extremely High Frequency), ήρθε ως διάδοχος του MILSTAR, επίσης σε GEO τροχιές, και προσφέρει υψηλότερους ρυθμούς μετάδοσης μέσω της μπάντας EHF (44 GHz uplink / 20 GHz downlink). Το AEHF εξασφαλίζει στρατηγικές και τακτικές επικοινωνίες υψηλής προτεραιότητας, με end-to-end κρυπτογράφηση, ισχυρή ανθεκτικότητα σε παρεμβολές και δυνατότητα επιχειρήσεων σε περιβάλλοντα πυρηνικού πολέμου. Σήμερα καλύπτει βασικές ανάγκες επικοινωνίας σε παγκόσμια κλίμακα για ΗΠΑ και ΝΑΤΟ [150].

Μια νεότερη εξέλιξη αποτελεί το MUOS (Mobile User Objective System), ένα σύστημα νέας γενιάς που συνδυάζει LEO και GEO δορυφόρους, παρέχοντας δυνατότητα ταυτόχρονης μετάδοσης φωνής και δεδομένων με χρήση τεχνολογίας παρόμοιας με τα δίκτυα κινητής τηλεφωνίας 3G/4G. χάρη στη χρήση μικρών και φορητών τερματικών, το MUOS επιτρέπει σε κινητές μονάδες (UAVs, απομακρυσμένες περιπολίες, ειδικές δυνάμεις) να παραμένουν συνδεδεμένες σε πραγματικό χρόνο, αυξάνοντας σημαντικά την ευελιξία και την επιχειρησιακή κινητικότητα [151].

Το πιο σύγχρονο σύστημα ευρυζωνικών στρατιωτικών επικοινωνιών είναι το WGS (Wideband Global SATCOM) αποτελεί το πλέον σύγχρονο σύστημα ευρυζωνικών δορυφορικών επικοινωνιών. Λειτουργεί στις μπάντες X και Ka, παρέχοντας χωρητικότητα μετάδοσης που φτάνει τα Gbps. Χρησιμοποιείται κυρίως command & control, real-time ISR (Intelligence, Surveillance and Reconnaissance), μεταφορά δεδομένων μεγάλης κλίμακας και πολυεθνική συνεργασία μέσω του NATO [152].

4.4.3 STANAG και δορυφορικά συστήματα

Για να διασφαλιστεί η διαλειτουργικότητα μεταξύ δορυφορικών συστημάτων και επίγειων σταθμών που ανήκουν σε διαφορετικές χώρες-μέλη του NATO, εφαρμόζονται συγκεκριμένα STANAGs (Standardization Agreements). Τα πρότυπα αυτά καθορίζουν τις διαδικασίες, τα πρωτόκολλα, τις μορφές μηνυμάτων και τις τεχνικές παραμέτρους που πρέπει να ακολουθούν όλα τα κράτη ώστε να μπορούν να συνεργάζονται απρόσκοπτα σε κοινές επιχειρήσεις [153].

Ένα από τα σημαντικότερα πρότυπα είναι το STANAG 4484,το οποίο αφορά την διαλειτουργικότητα σε στρατιωτικά συστήματα SATCOM στην ζώνη Super High Frequency (SHF: 3-30GHz).Το πρότυπο αυτό καθορίζει τις τεχνικές απαιτήσεις για τη χρήση του φάσματος Super High Frequency και εξασφαλίζει ότι οι επίγειοι σταθμοί, τα κινητά οχήματα και εναέριες πλατφόρμες (όπως UAVs ή αεροσκάφη C4ISR) από διαφορετικά κράτη-μέλη του NATO μπορούν να λειτουργούν σε κοινό πλαίσιο. Το πρότυπο ορίζει παραμέτρους όπως την κωδικοποίηση του σήματος, τις απαιτήσεις ισχύος, τα συστήματα συγχρονισμού και την απόδοση του καναλιού. Χάρη στο STANAG 4484, είναι εφικτή η κοινή χρήση δορυφορικών πόρων ακόμα και σε περιβάλλοντα πολλαπλών εθνικοτήτων, χωρίς να απαιτούνται τροποποιήσεις στους τερματικούς σταθμούς κάθε χώρας [154].

Το STANAG 5040 αποτελεί κρίσιμο πρότυπο για τη δημιουργία αυτοματοποιημένων και ημι-αυτόματων διασυνδέσεων μεταξύ των εθνικών δικτυών στρατιωτικών τηλεπικοινωνιών και του ολοκληρωμένου δικτύου επικοινωνιών του NATO. Πρόκειται για κρίσιμο πρότυπο που καθορίζει τις διαδικασίες routing και addressing, τις διαδικασίες session initiation, τη μορφοποίηση πακέτων, και τους ενσωματωμένους ελέγχους ασφαλείας. Μέσω του STANAG 5040 εξασφαλίζεται ότι οι τηλεπικοινωνιακές υποδομές διαφορετικών κρατών μπορούν να συνεργάζονται με ασφάλεια και αποδοτικότητα, ακόμη και όταν χρησιμοποιούν διαφορετικές τεχνολογίες ή επίπεδα ασφαλείας.

Επιπλέον, η υιοθέτησή του απλοποιεί τη διαδικασία ένταξης νέων κρατών-μελών στα δίκτυα του ΝΑΤΟ και μειώνει σημαντικά το χρόνο ανάπτυξης κρίσιμων επικοινωνιακών υποδομών στο πεδίο επιχειρήσεων [155].

Ιδιαίτερης σημασίας για τα δορυφορικά δίκτυα πληροφοριών είναι το STANAG 7085, το οποίο ρυθμίζει τη μετάδοση δεδομένων αναγνώρισης και επιτήρησης μέσω ευρυεκπομπής σε συμμαχικές δυνάμεις. Υποστηρίζει τη χρήση του Global Broadcast Service (GBS), ενός συστήματος παθητικής λήψης δορυφορικών δεδομένων σε πραγματικό χρόνο, το οποίο επιτρέπει τη διανομή ζωντανών εικόνων και βίντεο, γεωχωρικών πληροφοριών, προειδοποιήσεων απειλών (threat alerts) και στρατηγικών δελτίων πληροφοριών. Το STANAG 7085 προσδιορίζει το format των αρχείων, τα πρωτόκολλα ασφαλείας και τις απαιτήσεις bandwidth ώστε να είναι εφικτή η ταυτόχρονη λήψη από πολλαπλές μονάδες χωρίς συμφόρηση. Παίζει καθοριστικό ρόλο στην ενίσχυση του situational awareness σε στρατιωτικές επιχειρήσεις υψηλής ταχύτητας και δυναμικής εξέλιξης [156].

4.4.4 Εφαρμογές στο πεδίο επιχειρήσεων

Τα στρατιωτικά δορυφορικά συστήματα επικοινωνιών αποτελούν βασικό εργαλείο για την υποστήριξη επιχειρήσεων σε όλα τα επίπεδα – τακτικό, επιχειρησιακό και στρατηγικό. Ο ρόλος τους είναι κρίσιμος, καθώς παρέχουν συνεχή, ασφαλή και ευρείας εμβέλειας επικοινωνία, ξεπερνώντας γεωγραφικούς περιβαλλοντικούς και τεχνολογικούς περιορισμούς.

Στα σύγχρονα συστήματα C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), το SATCOM επιτρέπει την απευθείας διασύνδεση ανώτερων κέντρων διοίκησης με μονάδες πεδίου, εξασφαλίζοντας την ταχεία και ασφαλή μετάδοση πληροφοριών ελέγχου, συντονισμού, συλλογής πληροφοριών και αναγνώρισης στόχων. Αυτό αυξάνει κατακόρυφα το επίπεδο situational awareness, βελτιώνοντας την ποιότητα των αποφάσεων υπό πίεση χρόνου [109], [157].

Η χρήση δορυφορικών καναλιών είναι επίσης ζωτικής σημασίας στον έλεγχο μη επανδρωμένων αεροσκαφών (UAVs) και drones, τα οποία επιχειρούν συχνά σε απομακρυσμένα ή επικίνδυνα πεδία. Το SATCOM εξασφαλίζει τη μετάδοση βίντεο υψηλής ανάλυσης και δεδομένων τηλεμετρίας από απομακρυσμένα ή δυσπρόσιτα θέατρα επιχειρήσεων. Η ασφαλής σύνδεση με το κέντρο ελέγχου επιτρέπει την καθοδήγηση μη επανδρωμένων πλατφορμών σε μεγάλες αποστάσεις και την έγκαιρη επιστροφή πολύτιμων πληροφοριών αναγνώρισης [110], [146].

Τα Battlefield Networks, που αναπτύσσονται σε τακτικό επίπεδο, επωφελούνται άμεσα από τα SATCOM ειδικά σε περιοχές με ανεπαρκή ή κατεστραμμένη επίγεια υποδομή – όπως ορεινές περιοχές, θαλάσσια περιβάλλοντα ή έρημο. Τα δορυφορικά δίκτυα παρέχουν συνεχή σύνδεση μεταξύ μονάδων, ενισχύοντας τον συντονισμό, την ανταλλαγή πληροφοριών και τη δυνατότητα αντίδρασης σε δυναμικές καταστάσεις [108], [158].

Σε σενάρια καταστροφών ή εχθρικών επιθέσεων, όπου τα τοπικά δίκτυα έχουν υποστεί μερική ή ολική καταστροφή, οι φορητοί δορυφορικοί τερματικοί επιτρέπουν την άμεση επαναφορά της επικοινωνίας με τα ανώτερα κλιμάκια διοίκησης. Αυτή η ικανότητα είναι θεμελιώδης για την συνέχιση των επιχειρήσεων, την υποστήριξη αλληλεπίδρασης με συμμαχικές δυνάμεις, καθώς και για την άμεση λήψη ενισχύσεων ή νέων εντολών [101], [159].

Η πρακτική αξία των φορητών συστημάτων απεικονίζεται στο Σχήμα 39, όπου παρουσιάζεται στρατιώτης εξοπλισμένος με φορητό SATCOM manpack τερματικό. Η συσκευή αυτή επιτρέπει την ασφαλή και άμεση σύνδεση με τα στρατηγικά δίκτυα επικοινωνιών, ακόμη και σε απομονωμένα σημεία, διασφαλίζοντας τη συνέχεια της επικοινωνίας και τη ροή κρίσιμων πληροφοριών προς τα ανώτερα κλιμάκια [159].



Σχήμα 39- Στρατιώτης εξοπλισμένος με φορητό SATCOM manpack τερματικό [159]

Συνολικά, η δυνατότητα εκμετάλλευσης των SATCOM από τακτικές και στρατηγικές μονάδες ενισχύει την αποτελεσματικότητα των δυνάμεων στο πεδίο, βελτιώνει την επιχειρησιακή συντονισμένη δράση και διασφαλίζει την αδιάλειπτη ροή πληροφοριών ακόμα και στις πιο αποκομμένες ή ασταθείς περιοχές.

4.4.5 Τεχνικές προκλήσεις και ανάγκες ασφάλειας

Παρά τα αναμφισβήτητα πλεονεκτήματα που προσφέρουν τα συστήματα δορυφορικής επικοινωνίας (SATCOM) στις στρατιωτικές επιχειρήσεις, δεν είναι άτρωτα απέναντι σε μια σειρά από τεχνικές και επιχειρησιακές προκλήσεις που παραμένουν στο επίκεντρο της έρευνας και ανάπτυξης νέων τεχνολογιών.

Μία από τις πιο σοβαρές απειλές είναι οι σκόπιμες παρεμβολές (jamming) και οι τεχνικές spoofing, οι οποίες εφαρμόζονται συχνά από εχθρικές δυνάμεις ή στο πλαίσιο κυβερνοεπιθέσεων. Το jamming μπορεί να υποβαθμίσει ή να καταστήσει αδύνατη την επικοινωνία με μονάδες πεδίου, επηρεάζοντας κρίσιμες αποστολές. Αντίστοιχα, το spoofing- μέσω της μετάδοσης παραπλανητικών

σημάτων GPS- μπορεί να προκαλέσει σοβαρές αποκλίσεις σε πλοήγηση UAVs ή καθοδήγηση όπλων, οδηγώντας σε αποτυχία στόχων ή σε απώλεια κρίσιμου εξοπλισμού [93], [160].

Ένα δεύτερο κρίσιμο ζήτημα είναι η υψηλή καθυστέρηση (latency), ιδίως στα συστήματα γεωστατικής τροχιάς (GEO), όπου οι αποστάσεις προκαλούν καθυστερήσεις άνω των 500 ms ανά κύκλο επικοινωνίας. Αυτό καθιστά τις real-time εφαρμογές -όπως τηλεχειριζόμενα συστήματα ή επιχειρήσεις με απευθείας μετάδοση ISR- λιγότερο αποδοτικές [140].

Η εξάρτηση από τροχιακές πλατφόρμες αποτελεί επίσης ευπάθεια. Οι στρατιωτικοί δορυφόροι αποτελούν υψηλής αξίας στόχους σε περίπτωση σύγκρουσης ή ακόμα και σε περιβάλλοντα “γκρίζων ζωνών”, όπως έχουν δείξει τα πρόσφατα περιστατικά καταστροφής δορυφόρων με antisatellite (ASAT) όπλα ή επιθέσεις με λέιζερ και spoofing σε τροχιά [161].

Τέλος, η ασφάλεια κρυπτογράφησης και διαχείρισης πρόσβασης σε συστήματα SATCOM είναι ζωτικής σημασίας, ιδιαίτερα σε πολυεθνικά σενάρια, όπου δυνάμεις με διαφορετικά επίπεδα ασφαλείας καλούνται να συνεργαστούν. Η ανταλλαγή διαβαθμισμένων δεδομένων απαιτεί την υιοθέτηση πρωτοκόλλων HAIPE/IPsec, τη συμμόρφωση με STANAGs και την ύπαρξη πολιτικών zero-trust, προκειμένου να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα της πληροφορίας [97], [131].

4.4.6 Τεχνολογικές λύσεις & μελλοντικές τάσεις

Για να αντιμετωπιστούν οι τεχνικές προκλήσεις και να διατηρηθεί η επιχειρησιακή υπεροχή των στρατιωτικών δορυφορικών επικοινωνιών (SATCOM), η έρευνα και η αμυντική βιομηχανία επενδύουν συστηματικά στην ανάπτυξη προηγμένων τεχνολογικών λύσεων.

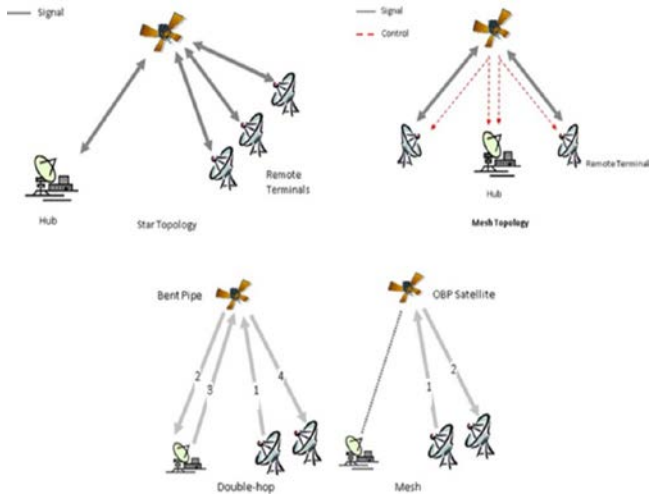
Μία από τις πλέον κρίσιμες τεχνολογίες είναι η δυναμική κατεύθυνση δέσμης (beam steering), σε συνδυασμό με τεχνικές εναλλαγής συχνοτήτων (frequency hopping). Αυτά τα συστήματα επιτρέπουν τη συνεχή προσαρμογή της εκπομπής στον χώρο και τη συχνότητα, καθιστώντας εξαιρετικά δύσκολη την εντόπιση και παρεμβολή από εχθρικούς αναμεταδότες ή παρεμβολείς(anti-jamming) [150],[82].

Η ενσωμάτωση τεχνητής νοημοσύνης για dynamic routing αποτελεί πλέον αναδυόμενη πραγματικότητα. Μέσω αλγορίθμων μηχανικής μάθησης, τα δίκτυα μπορούν να αναγνωρίζουν περιοχές συμφόρησης, πιθανές παρεμβολές ή διακοπές, και να ανακατευθύνουν αυτόματα την κυκλοφορία προς πιο αποδοτικές διαδρομές [105], [162].

Τα υβριδικά πλέγματα επίγειων και δορυφορικών κόμβων (hybrid mesh-satellite networks) δημιουργούν πλέον δυναμικά, επεκτάσιμα και ανθεκτικά δίκτυα πεδίου. Οι κόμβοι μπορούν να επαναδρομολογούν την κυκλοφορία σε περίπτωση διακοπής ή βλάβης ενός δορυφόρου, ενώ

ενισχύεται η redundancy και η επιχειρησιακή συνέχεια ακόμη και σε σενάρια έντονων παρεμβολών [141], [163].

Η λειτουργία αυτών των υβριδικών δικτύων απεικονίζεται στο Σχήμα 40, το οποίο παρουσιάζει διαφορετικές αρχιτεκτονικές δορυφορικών επικοινωνιών-όπως star, mesh, bent-pipe και double-top. Η συγκριτική απεικόνιση αναδεικνύει τα πλεονεκτήματα κάθε τοπολογίας ως προς την ανθεκτικότητα, την αποδοτικότητα δρομολόγησης και τη διαχείριση παρεμβολών.



Σχήμα 40- Αρχιτεκτονικά μοντέλα δορυφορικών επικοινωνιών star topology, mesh topology, bent-pipe και double-hop αρχιτεκτονικές [140]

Αυτές οι αρχιτεκτονικές επιτρέπουν την αποδοτική διαχείριση της κυκλοφορίας, τη χρήση μηχανισμών αποτροπής παρεμβολών και την εξασφάλιση επικοινωνίας ακόμη και σε σενάρια έντονης απειλής.

Από πλευράς ασφάλειας, η ενσωμάτωση τεχνολογιών HAIPE/IPsec σε φορητούς τερματικούς σταθμούς (π.χ. TACLANE devices) εξασφαλίζει υψηλή διαλειτουργικότητα με τα STANAGs του NATO, διασφαλίζοντας ότι η ανταλλαγή διαβαθμισμένων πληροφοριών γίνεται με ασφαλή και συμβατό τρόπο σε διεθνές επίπεδο [137], [164].

ΚΕΦΑΛΑΙΟ 5

5 Κυβερνοαπειλές & Προκλήσεις

Η ανάγκη για ασφαλή, σταθερή και αξιόπιστη επικοινωνία είναι θεμελιώδης σε κάθε σύγχρονη στρατιωτική επιχείρηση. Από την κίνηση μιας μικρής μονάδας στο πεδίο, μέχρι τη μετάδοση κρίσιμων πληροφοριών από ένα κέντρο διοίκησης προς ένα απομακρυσμένο UAV, η επικοινωνία λειτουργεί ως το «νευρικό σύστημα» των Ένοπλων Δυνάμεων [54], [59]. Ακόμη και μια σύντομη διακοπή ή αλλοίωση του καναλιού επικοινωνίας μπορεί να αποβεί καταστροφική: να προκαλέσει σύγχυση στις μονάδες, καθυστέρηση στη λήψη αποφάσεων, ή και απώλεια ανθρώπινων ζωών.

Σε αυτό το πλαίσιο, οι επιθέσεις που στοχεύουν τα συστήματα επικοινωνίας αποκτούν καθοριστικό ρόλο. Οι πιο χαρακτηριστικές από αυτές είναι το jamming και το spoofing –τεχνικές που αποσκοπούν είτε στην παρεμπόδιση της μετάδοσης πληροφορίας είτε στην αλλοίωση ή παραπλάνηση των δεκτών. Ενώ η πρώτη επιδιώκει τη διακοπή της επικοινωνίας μέσω παρεμβολών [6], [77], η δεύτερη λειτουργεί πιο ύπουλα, εισάγοντας ψευδείς πληροφορίες ως αυθεντικές [60].

Αξίζει να σημειωθεί ότι οι απειλές αυτές δεν περιορίζονται πλέον σε απλές ηλεκτρονικές παρενοχλήσεις. Έχουν εξελιχθεί σε πολυεπίπεδα εργαλεία του ηλεκτρονικού πολέμου, ενταγμένα σε ολοκληρωμένες επιχειρήσεις πληροφοριών (information operations), σε ασύμμετρες τακτικές και σε συνδυασμένα σενάρια κυβερνοπολέμου [70], [65]. Στη σύγχρονη επιχειρησιακή πραγματικότητα, το jamming και το spoofing συχνά εφαρμόζονται σε συνδυασμό με κυβερνοεπιθέσεις ή με τη χρήση κακόβουλου λογισμικού, ώστε να επιτευχθεί το μέγιστο αποτέλεσμα: όχι απλά η παρεμπόδιση της επικοινωνίας, αλλά ο πλήρης αποπροσανατολισμός του αντιπάλου.

5.1 Jamming, Spoofing και Ηλεκτρονικός Πόλεμος

Η ανάγκη για ασφαλή, σταθερή και αξιόπιστη επικοινωνία είναι θεμελιώδης σε κάθε σύγχρονη στρατιωτική επιχείρηση. Από την κίνηση μιας μικρής μονάδας στο πεδίο, μέχρι τη μετάδοση κρίσιμων πληροφοριών από ένα κέντρο διοίκησης προς ένα απομακρυσμένο UAV, η επικοινωνία λειτουργεί ως το «νευρικό σύστημα» των Ένοπλων Δυνάμεων [54], [59]. Ακόμη και μια σύντομη διακοπή ή αλλοίωση του καναλιού επικοινωνίας μπορεί να αποβεί καταστροφική: να προκαλέσει σύγχυση στις μονάδες, καθυστέρηση στη λήψη αποφάσεων, ή και απώλεια ανθρώπινων ζωών.

Σε αυτό το πλαίσιο, οι επιθέσεις που στοχεύουν τα συστήματα επικοινωνίας αποκτούν καθοριστικό ρόλο. Οι πιο χαρακτηριστικές από αυτές είναι το jamming και το spoofing –τεχνικές που αποσκοπούν είτε στην παρεμπόδιση της μετάδοσης πληροφορίας είτε στην αλλοίωση ή παραπλάνηση

των δεκτών. Ενώ η πρώτη επιδιώκει τη διακοπή της επικοινωνίας μέσω παρεμβολών [6], [77], η δεύτερη λειτουργεί πιο ύπουλα, εισάγοντας ψευδείς πληροφορίες ως αυθεντικές [60].

Αξίζει να σημειωθεί ότι οι απειλές αυτές δεν περιορίζονται πλέον σε απλές ηλεκτρονικές παρενοχλήσεις. Έχουν εξελιχθεί σε πολυεπίπεδα εργαλεία του ηλεκτρονικού πολέμου, ενταγμένα σε ολοκληρωμένες επιχειρήσεις πληροφοριών (information operations), σε ασύμμετρες τακτικές και σε συνδυασμένα σενάρια κυβερνοπολέμου [70], [65]. Στη σύγχρονη επιχειρησιακή πραγματικότητα, το jamming και το spoofing συχνά εφαρμόζονται σε συνδυασμό με κυβερνοεπιθέσεις ή με τη χρήση κακόβουλου λογισμικού, ώστε να επιτευχθεί το μέγιστο αποτέλεσμα: όχι απλά η παρεμπόδιση της επικοινωνίας, αλλά ο πλήρης αποπροσανατολισμός του αντιπάλου.

5.1.1 Jamming : Τύποι και Επιχειρησιακή επίδραση

Το jamming αποτελεί μία από τις πιο χαρακτηριστικές μεθόδους ηλεκτρονικού πολέμου και χρησιμοποιείται εδώ και δεκαετίες σε στρατιωτικά περιβάλλοντα. Ο όρος περιγράφει τη σκόπιμη εκπομπή ηλεκτρομαγνητικής ακτινοβολίας σε συγκεκριμένες συχνότητες με τέτοιο τρόπο ώστε να «σκεπάζει» ή να αλλοιώνει το χρήσιμο σήμα. Στόχος είναι η μείωση του λόγου σήματος προς θόρυβο (Signal- to-Noise Ratio-SNR) στον δείκτη κάτω από το αποδεκτό όριο, με αποτέλεσμα το κανάλι να καταστεί μη λειτουργικό [6], [77].

Το jamming αποτελεί μία από τις πιο διαδεδομένες μορφές ηλεκτρονικού πολέμου, στοχεύοντας στην παρεμβολή ή διακοπή κρίσιμων επικοινωνιών. Ανάλογα με το χρονικό σημείο της επίθεσης, διακρίνεται σε προληπτικό (preventive), ώστε να εξουδετερωθούν οι επικοινωνίες του αντιπάλου πριν χρησιμοποιηθούν και αντιδραστικό (reactive), στοχεύοντας την παρεμπόδιση κρίσιμων συστημάτων την ώρα της χρήσης τους.

<u>Κατηγορίες Jamming</u>

Το Spot Jamming αποτελεί την πιο απλή μορφή παρεμβολής. Σε αυτήν, ο παρεμβολέας συγκεντρώνει όλη την ισχύ εκπομπής του σε μία μόνο συχνότητα, με αποτέλεσμα να «σκεπάζει» ολοκληρωτικά το χρήσιμο σήμα [6]. Η τεχνική αυτή είναι εξαιρετικά αποτελεσματική όταν ο στόχος χρησιμοποιεί σταθερό κανάλι εκπομπής, όπως συμβαίνει με ορισμένους παλαιότερους αναλογικούς πομποδέκτες. Ωστόσο, παρουσιάζει σοβαρά μειονεκτήματα απέναντι σε σύγχρονα δίκτυα που εφαρμόζουν frequency hopping ή τεχνικές spread spectrum, τα οποία καθιστούν δύσκολη τη συνεχή στόχευση της ίδιας συχνότητας [77].

Το Sweep Jamming αποτελεί μία πιο εξελιγμένη παραλλαγή, κατά την οποία ο παρεμβολέας «σαρώνει» διαδοχικά πολλές συχνότητες σε υψηλή ταχύτητα [77]. Έτσι, μπορεί να πλήξει δυναμικά δίκτυα που εναλλάσσουν κανάλια μετάδοσης, μειώνοντας την αποτελεσματικότητα τους. Παρόλα

αυτά, το sweep jamming δεν μπορεί να καλύψει ταυτόχρονα όλο το φάσμα, αφήνοντας κενά χρονικά διαστήματα στα οποία ο στόχος ενδέχεται να συνεχίσει να επικοινωνεί κανονικά.

Το Barrage Jamming είναι μια πιο «βίαιη» προσέγγιση, κατά την οποία ο παρεμβολέας εκπέμπει ισχυρά σήματα σε ολόκληρο το εύρος ενός φάσματος συχνοτήτων [6]. Έτσι, οποιοδήποτε κανάλι μέσα στο φάσμα αυτό καθίσταται μη λειτουργικό. Η μέθοδος είναι ιδιαίτερα αποτελεσματική σε περιβάλλοντα με πολλαπλά κανάλια, ωστόσο είναι εξαιρετικά ενεργοβόρα και εντοπίζεται εύκολα, καθώς η συνεχής εκπομπή σε μεγάλο εύρος φάσματος αποκαλύπτει άμεσα την παρουσία παρεμβολέα [54]. Ιστορικά, το barrage jamming χρησιμοποιήθηκε ευρέως κατά τον Πόλεμο του Κόλπου(1991) εναντίον ραντάρ έγκαιρης προειδοποίησης, προκειμένου να διευκολυνθεί η είσοδος συμμαχικών αεροσκαφών σε εχθρικό εναέριο χώρο [65].

Το Smart Jamming αποτελεί την πιο σύγχρονη και τεχνολογικά προηγμένη μορφή. Σε αυτήν την περίπτωση, ο παρεμβολέας δεν εκπέμπει συνεχώς, αλλά «ακούει» πρώτα το κανάλι και παρεμβαίνει μόνο όταν ανιχνεύει πραγματική εκπομπή [77]. Η μέθοδος αυτή βασίζεται σε εξελιγμένους αλγορίθμους επεξεργασίας σήματος και, όλο και συχνότερα, σε εφαρμογές τεχνητής νοημοσύνης (AI), που επιτρέπουν την επιλογή της κατάλληλης χρονικής στιγμής για παρεμβολή [70]. Με τον τρόπο αυτό μειώνεται η κατανάλωση ενέργειας, δυσκολεύεται ο εντοπισμός του παρεμβολέα και επιτυγχάνεται ακριβής στόχευση σε κρίσιμες φάσεις επικοινωνίας, όπως η μετάδοση εντολών ή δεδομένων πλοήγησης UAVs. Η χρήση «έξυπνου» jamming έχει αναφερθεί σε σύγχρονες συγκρούσεις, όπως στην Ουκρανία, όπου συστήματα ηλεκτρονικού πολέμου αξιοποιούν συνδυαστικά τεχνικές παρεμβολής και ανάλυσης σήματος για την αποδυνάμωση των εχθρικών UAVs [60].

<u>Εφαρμογές στο Στρατιωτικό Περιβάλλον</u>

Η επίδραση του jamming στο πεδίο μάχης είναι πολυεπίπεδη και μπορεί να επηρεάσει κρίσιμα υποσυστήματα των Ένοπλων Δυνάμεων. Ακόμη και μία απλή απώλεια επικοινωνίας μεταξύ μιας μονάδας πεζικού και του κέντρου διοίκησης αρκεί για να προκαλέσει αποδιοργάνωση, καθυστέρηση στη λήψη αποφάσεων και αυξημένο ρίσκο αποτυχίας αποστολής. Η αποκοπή της ροής πληροφοριών σε πραγματικό χρόνο μπορεί να στερήσει από τους διοικητές την επιχειρησιακή εικόνα, οδηγώντας σε λανθασμένες ή καθυστερημένες ενέργειες [54].

Εξίσου κρίσιμη είναι η παρεμβολή στα συστήματα δορυφορικών επικοινωνιών. Τα στρατηγικά δίκτυα διοίκησης και ελέγχου (C2) βασίζονται σε δορυφορικά uplinks και downlinks για τη μετάδοση δεδομένων σε μεγάλες αποστάσεις. Η παρεμβολή σε αυτά τα κανάλια μπορεί να οδηγήσει σε μερική ή ολική απώλεια επικοινωνιών με απομακρυσμένες δυνάμεις, μειώνοντας την ικανότητα συντονισμού επιχειρήσεων μεγάλης κλίμακας [60].

Σημαντικός στόχος αποτελούν επίσης τα UAVs και οι τηλεχειριζόμενες πλατφόρμες. Η παρεμβολή στα κανάλια τηλεχειρισμού μπορεί να προκαλέσει πλήρη απώλεια ελέγχου, οδηγώντας σε

πτώση, σε αδυναμία ολοκλήρωσης αποστολής ή ακόμη και σε κατάληψη της πλατφόρμας από τον αντίπαλο μέσω spoofing ή συνδυασμένων επιθέσεων [70]. Το φαινόμενο αυτό έχει παρατηρηθεί σε σύγχρονες συγκρούσεις, όπου UAVs αναγκάστηκαν να προσγειωθούν εκτός ελέγχου των χειριστών τους.

Από τις πλέον σοβαρές συνέπειες είναι η παρεμβολή στην πλοήγηση μέσω GPS. Τα στρατιωτικά όπλα ακριβείας, τα οχήματα και οι μονάδες πεδίου εξαρτώνται σε μεγάλο βαθμό από το στίγμα που παρέχουν τα δορυφορικά συστήματα. Η απώλεια ή η αλλοίωση των σημάτων GPS μπορεί να οδηγήσει σε αδυναμία εντοπισμού θέσης, απόκλιση πορείας, ή πλήρη ακύρωση των όπλων καθοδηγούμενων με GPS, όπως οι πύραυλοι cruise [54].

Τέλος, οι επιπτώσεις στις δομές διοίκησης και ελέγχου (C2/C4ISR) είναι στρατηγικής σημασίας. Ένα αποτελεσματικό jamming σε αυτά τα δίκτυα μπορεί να προκαλέσει καθυστέρηση στη λήψη αποφάσεων, έλλειψη συνοχής στη διοίκηση και μείωση της επιχειρησιακής ετοιμότητας. Στο σύγχρονο δόγμα επιχειρήσεων, όπου η πληροφορία θεωρείται κρίσιμος πολλαπλασιαστής ισχύος, η απώλεια επικοινωνίας ισοδυναμεί με απώλεια ελέγχου του ίδιου του πεδίου μάχης [60], [70].

Επιχειρησιακές Επιπτώσεις

Οι επιπτώσεις του jamming στις στρατιωτικές επιχειρήσεις είναι συχνά υποτιμημένες, ωστόσο μπορούν να αποδειχθούν καθοριστικές για την έκβαση μιας αποστολής. Η παρεμβολή δεν επηρεάζει απλώς την ποιότητα επικοινωνίας, αλλά δύναται να ανατρέψει πλήρως τον επιχειρησιακό σχεδιασμό, προκαλώντας σοβαρές απώλειες σε τακτικό και στρατηγικό επίπεδο [54].

Μία από τις πιο εμφανείς επιπτώσεις είναι η απώλεια UAVs και τηλεχειριζόμενων πλατφορμών. Σε περίπτωση που η σύνδεση με τον σταθμό ελέγχου διακοπεί, το UAV καθίσταται μη λειτουργικό μπορεί να καταρριφθεί εύκολα, να πέσει εκτός ελέγχου ή ακόμη και να «αιχμαλωτιστεί» από τον αντίπαλο μέσω spoofing και εκτροπής της πορείας του. Η απώλεια τέτοιων μέσων δεν συνεπάγεται μόνο οικονομικό κόστος αλλά και σοβαρή αποδυνάμωση των δυνατοτήτων ISR μιας δύναμης [60].

Εξίσου σημαντική είναι η αποτυχία όπλων ακριβείας. Η σύγχρονη πολεμική βιομηχανία στηρίζεται σε μεγάλο βαθμό στη GPS για την καθοδήγηση πυραύλων cruise και πυρομαχικών με συντεταγμένες. Όταν το σήμα GPS παρεμποδίζεται, αυτά τα όπλα είτε αποτυγχάνουν να πλήξουν τον στόχο είτε χάνουν την κατεύθυνση τους, μειώνοντας δραματικά την αποτελεσματικότητα τους και αυξάνοντας τον κίνδυνο παράπλευρων απωλειών [54], [70].

Μία τρίτη διάσταση είναι η καθυστέρηση στη λήψη αποφάσεων. Σε επιχειρήσεις που απαιτούν συγχρονισμό πολλών μονάδων, η απώλεια επικοινωνίας ακόμη και για λίγα λεπτά μπορεί να έχει δυσανάλογες συνέπειες. Η μη έγκαιρη μετάδοση εντολών οδηγεί σε απώλεια πρωτοβουλίας, μειώνει

την αποτελεσματικότητα της συνεργασίας και μπορεί να επιτρέψει στον αντίπαλο να αποκτήσει πλεονέκτημα στο πεδίο της μάχης [60].

Τέλος, δεν πρέπει να παραβλέπεται ο ψυχολογικός αντίκτυπος. Η ξαφνική «σιγή» εν μέσω μάχης προκαλεί αβεβαιότητα και σύγχυση στις δυνάμεις, ενώ υπονομεύει την εμπιστοσύνη στο σύστημα διοίκησης και ελέγχου. Η έλλειψη εμπιστοσύνης αυτής της μορφής μπορεί να αποδειχθεί καταστροφική, καθώς το ηθικό και η πειθαρχία είναι παράγοντες κρίσιμης σημασίας στη διατήρηση της επιχειρησιακής συνοχής [70].

Συνολικά, το jamming δεν αποτελεί απλώς μία τεχνική παρενόχλησης μπορεί να λειτουργήσει ως καταλύτης αποτυχίας μιας ολόκληρης επιχείρησης, επιδρώντας ταυτόχρονα σε τεχνικό, τακτικό και ψυχολογικό επίπεδο [54], [60], [70].

5.1.2 Spoofing : GPS και δικτυακές επιθέσεις

Ενώ το jamming είναι μια φανερή και άμεση ενέργεια, που αποσκοπεί στη διακοπή της επικοινωνίας, το spoofing δρα με ακριβώς αντίθετο τρόπο: είναι μια ύπουλη και σχεδόν αόρατη επίθεση. Στην πράξη, πρόκειται για τη μετάδοση ψευδών σημάτων ή πληροφοριών που έχουν σχεδιαστεί ώστε να μοιάζουν με τα αυθεντικά, με σκοπό να παραπλανήσουν τον δέκτη [6], [77]. Η ίδια η λέξη «spoof» σημαίνει «εξαπατώ», αποτυπώνοντας με ακρίβεια τον χαρακτήρα της τεχνικής. Αυτό που κάνει το spoofing ιδιαίτερα επικίνδυνο είναι το γεγονός ότι δεν συνοδεύεται από εμφανή σημάδια: σε αντίθεση με το jamming, που προκαλεί άμεση διακοπή ή θόρυβο, το spoofing αφήνει την ψευδαίσθηση ότι όλα λειτουργούν κανονικά.

GPS Spoofing

Η πιο συνηθισμένη και ταυτόχρονα πιο επικίνδυνη μορφή spoofing αφορά τα συστήματα πλοήγησης GNSS/GPS, τα οποία αποτελούν τη «ραχοκοκαλιά» του σύγχρονου πολέμου. Σχεδόν όλα τα στρατιωτικά μέσα – από UAVs και πύραυλους cruise, μέχρι τεθωρακισμένα οχήματα και μονάδες πεζικού – στηρίζονται στο GPS για καθοδήγηση, συγχρονισμό και προσανατολισμό. Η ακρίβεια που παρέχει η δορυφορική πλοήγηση είναι απαραίτητη για την εκτέλεση επιθέσεων ακριβείας και για το συντονισμό πολλαπλών μονάδων σε ένα δυναμικό πεδίο μάχης [54].

Σε μια επίθεση GPS spoofing, ο επιτιθέμενος δημιουργεί ένα τεχνητό σήμα GNSS, σχεδιασμένο ώστε να μιμείται το αυθεντικό αλλά με λανθασμένα δεδομένα θέσης ή χρόνου. Επειδή το πλαστό σήμα εκπέμπεται συχνά με μεγαλύτερη ισχύ, ο δέκτης «κλειδώνει» σε αυτό, θεωρώντας το ως έγκυρο. Το πρόβλημα εντείνεται από το γεγονός ότι οι περισσότερες στρατιωτικές πλατφόρμες, αν και χρησιμοποιούν κρυπτογραφημένες εκδόσεις του GPS (π.χ. P(Y) code, M-code), δεν διαθέτουν πάντα πρόσθετους αισθητήρες ή μηχανισμούς επαλήθευσης για να διακρίνουν το γνήσιο σήμα από το πλαστό. Έτσι, ένα UAV μπορεί να εκτραπεί από την πορεία του χωρίς οι χειριστές να το αντιληφθούν

εγκαίρως, ενώ ένα χερσαίο όχημα μπορεί να οδηγηθεί σε λάθος τοποθεσία, αποτυγχάνοντας την αποστολή του [60].

Η επιχειρησιακή σημασία του spoofing γίνεται αντιληπτή μέσα από πραγματικά παραδείγματα. Το πιο χαρακτηριστικό ήταν το περιστατικό του 2011, όταν οι ιρανικές δυνάμεις ισχυρίστηκαν ότι κατάφεραν να παραπλανήσουν με GPS spoofing το αμερικάνικο stealth drone RQ-170 Sentinel. Σύμφωνα με τις δηλώσεις τους, κατάφεραν να εισάγουν ψεύτικο GPS σήμα, προκαλώντας την αποσύνδεση του UAV από τον σταθμό ελέγχου και αναγκάζοντας το να προσγειωθεί με ασφάλεια σε ιρανικό έδαφος [165]. Αν και οι ΗΠΑ δεν επιβεβαίωσαν ποτέ επίσημα τη μέθοδο, η υπόθεση αυτή έλαβε μεγάλη δημοσιότητα και προκάλεσε διεθνή ανησυχία για την ευπάθεια των στρατιωτικών συστημάτων πλοήγησης [83]. Το γεγονός ότι ένα υψηλής τεχνολογίας UAV, σχεδιασμένο για αποστολές στρατηγικής σημασίας, μπορούσε θεωρητικά να πέσει θύμα spoofing, έδειξε ότι η απειλή δεν είναι θεωρητική αλλά πρακτική και άμεσα εφαρμόσιμη [60].

Δικτυακό Spoofing

Το spoofing δεν περιορίζεται μόνο στα δορυφορικά σήματα GPS αντίθετα μπορεί να εφαρμοστεί και σε τακτικά δίκτυα επικοινωνίας, με ακόμη πιο επικίνδυνες συνέπειες. Σε αυτή την περίπτωση, ο επιτιθέμενος μπορεί να προσποιηθεί ότι είναι ένας φιλικός κόμβος μέσα στο δίκτυο, εκμεταλλευόμενος αδυναμίες στα πρωτόκολλα αυθεντικοποίησης ή στην διαχείριση ταυτότητας των συστημάτων [70]. Με τον τρόπο αυτό καταφέρνει να διεισδύσει «αθόρυβα» στο δίκτυο και να αποκτήσει πρόσβαση σε κρίσιμες ροές δεδομένων.

Μόλις εξασφαλιστεί η πρόσβαση, ο επιτιθέμενος έχει τη δυνατότητα να παρακολουθεί την κυκλοφορία δεδομένων, να συλλέγει ευαίσθητες πληροφορίες (όπως θέσεις μονάδων, σχέδια επιχειρήσεων ή καταστάσεις ανεφοδιασμού) ή ακόμη και να εισάγει παραποιημένα μηνύματα. Η αλλοίωση αυτή μπορεί να οδηγήσει σε καταστροφικές συνέπειες, καθώς οι χειριστές και οι διοικητές θεωρούν ότι λαμβάνουν αυθεντικές εντολές. Σε προχωρημένες περιπτώσεις έχουν καταγραφεί σενάρια όπου πλαστές εντολές C2 μεταδόθηκαν σε στρατιωτικά δίκτυα, με αποτέλεσμα οι μονάδες να εκτελέσουν αποστολές που δεν είχαν εγκριθεί ή να κινηθούν σε λάθος κατευθύνσεις [80].

Η απειλή γίνεται ακόμη μεγαλύτερη στο πλαίσιο των συστημάτων C4ISR. Σε αυτά, η αξιοπιστία των δεδομένων είναι εξίσου σημαντική με τη διαθεσιμότητα της επικοινωνίας. Ενώ το jamming «σιωπά» το κανάλι, το δικτυακό spoofing μπορεί να δημιουργήσει μια ψευδή επιχειρησιακή εικόνα, οδηγώντας σε εσφαλμένες αποφάσεις σε στρατηγικό επίπεδο. Αυτό σημαίνει ότι η αλλοίωση της πληροφορίας μέσω spoofing μπορεί να αποβεί εξίσου επικίνδυνη με την πλήρη απώλεια επικοινωνιών, καθώς παραπλανά τη διοίκηση, υπονομεύοντας την εμπιστοσύνη στο ίδιο το σύστημα [70].

Επιχειρησιακές Επιπτώσεις

Η ισχύς του spoofing έγκειται στην αόρατη φύση του. Σε αντίθεση με το jamming, που γίνεται άμεσα αντιληπτό λόγω θορύβου ή ξαφνικής απώλειας σήματος, το spoofing επιτρέπει στον επιτιθέμενο να χειραγωγεί πλατφόρμες και δίκτυα επικοινωνίας χωρίς να κινεί υποψίες. Έτσι, οι χειριστές πιστεύουν ότι το σύστημα λειτουργεί κανονικά, ενώ στην πραγματικότητα εκτελεί παραπλανημένες εντολές.

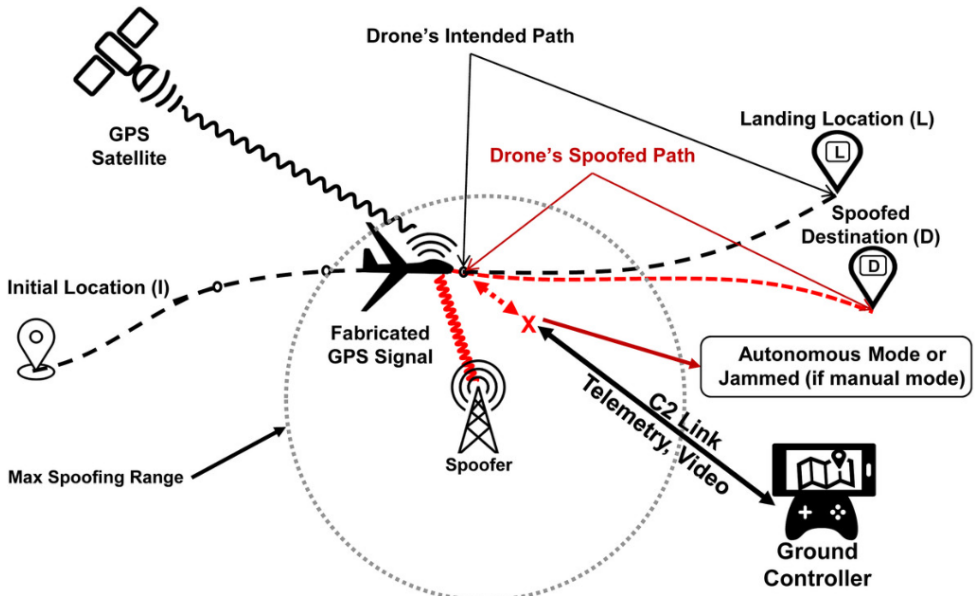
Για παράδειγμα, ένα UAV μπορεί να φαίνεται στον σταθμό ελέγχου ότι ακολουθεί κανονικά το σχέδιο πτήσης, τα δεδομένα τηλεμετρίας να παρουσιάζουν κανονικές τιμές και οι συντεταγμένες να μοιάζουν αξιόπιστες, στην πραγματικότητα όμως το αεροσκάφος να έχει εκτραπεί από την πορεία του λόγω παραποιημένων GPS σημάτων [60]. Η αδυναμία άμεσης ανίχνευσης καθιστά το spoofing ιδιαίτερα επικίνδυνο, καθώς ο χειριστής συνειδητοποιεί την επίθεση μόνο όταν οι συνέπειες έχουν ήδη επέλθει.

Οι επιχειρησιακές επιπτώσεις μπορεί να είναι πολλαπλές και κρίσιμες. Ενδεικτικά η απώλεια ελέγχου UAVs: Ένα drone μπορεί να οδηγηθεί εκτός πορείας, να χαθεί ή ακόμη και να προσγειωθεί σε εχθρικό έδαφος. Η αποτυχία όπλων ακριβείας: Πύραυλοι ή κατευθυνόμενα πυρομαχικά που βασίζονται σε GPS μπορεί να πλήξουν λανθασμένο στόχο, ακυρώνοντας την αποστολή. Η εκτροπή στρατευμάτων: Χερσαίες μονάδες που χρησιμοποιούν GPS για πλοήγηση μπορεί να κατευθυνθούν σε λάθος περιοχή, με αποτέλεσμα καθυστέρηση ή αποτυχία επιχειρήσεων. Τέλος η παραπλάνηση δικτύων C2/C4ISR: Η εισαγωγή πλαστών δεδομένων σε δίκτυα διοίκησης μπορεί να αλλοιώσει την επιχειρησιακή εικόνα και να οδηγήσει σε λανθασμένες αποφάσεις στρατηγικού επιπέδου.

Αυτές οι επιπτώσεις δεν είναι μόνο τεχνικής φύσης, αλλά έχουν και στρατηγικό και ψυχολογικό αντίκτυπο. Η παραπλάνηση δημιουργεί αβεβαιότητα στη διοίκηση, μειώνει την εμπιστοσύνη στα ίδια συστήματα και μπορεί να οδηγήσει σε αναστολή επιχειρήσεων μέχρι να επιβεβαιωθεί η αξιοπιστία των δεδομένων. Στο σύγχρονο δόγμα επιχειρήσεων, όπου η πληροφορία θεωρείται «πολλαπλασιαστής ισχύος», η απώλεια εμπιστοσύνης στην πληροφορία λόγω spoofing μπορεί να έχει ανυπολόγιστο επιχειρησιακό κόστος [60].

Το Σχήμα 41 αποτυπώνει με χαρακτηριστικό τρόπο τις συνέπειες ενός GPS spoofing attack. Ενώ η κανονική πορεία του UAV θα το οδηγούσε στο προγραμματισμένο σημείο προσγείωσης, το πλαστό σήμα GPS που εκπέμπεται από τον επιτιθέμενο το παρασύρει σε διαφορετικό προορισμό. Ο χειριστής συνεχίζει να λαμβάνει δεδομένα τηλεμετρίας και βίντεο μέσω του καναλιού C2, τα οποία φαίνονται κανονικά, χωρίς να μπορεί να αντιληφθεί εγκαίρως την παραπλάνηση. Σε περιπτώσεις όπου το C2 link παρεμβάλλεται ταυτόχρονα με jamming, η δυνατότητα επαναφοράς του ελέγχου χάνεται εντελώς, με αποτέλεσμα το UAV να καταλήγει σε ακούσια ή ελεγχόμενη προσγείωση από τον αντίπαλο. Το σενάριο αυτό δείχνει πώς το spoofing μπορεί να συνδυαστεί με jamming για να ενισχύσει την

αποτελεσματικότητα του, καθιστώντας τις συνδυασμένες επιθέσεις εξαιρετικά επικίνδυνες για στρατιωτικές επιχειρήσεις.



Σχήμα 41- Παράδειγμα GPS spoofing σε UAV [83]

5.1.3 Συνδυασμένες επιθέσεις(EW,Cyber)

Στο σύγχρονο πεδίο μάχης, οι επιθέσεις ηλεκτρονικού πολέμου σπάνια εκδηλώνονται μεμονωμένα. Αντίθετα, συχνά υλοποιούνται ως συνδυασμένες επιθέσεις (multi-vector attacks), όπου τεχνικές όπως jamming και spoofing ενισχύονται μέσω κυβερνοεπιθέσεων (malware, trojans δικτυακή διείσδυση) ή και επιθέσεων στην αλυσίδα εφοδιασμού λογισμικού. Αυτού του είδους οι επιθέσεις είναι πολυδιάστατες και έχουν μεγαλύτερη πιθανότητα επιτυχίας, διότι δεν στοχεύουν μόνο στην παρεμβολή επικοινωνιών, αλλά και στην αλλοίωση της πληροφορίας και την αποσταθεροποίηση της διοίκησης [60], [70].

Η αποτελεσματικότητα αυτών των επιθέσεων οφείλεται στο ότι εκτελούνται με συγχρονισμό, ταχύτητα και γνώση των συστημάτων-στόχων. Ένας επιτιθέμενος μπορεί να εκμεταλλευθεί τις αδυναμίες των στρατηγικών δικτύων και να προκαλέσει σύγχυση και παράλυση σε πολλαπλά επίπεδα ταυτόχρονα.

<u>Παραδείγματα Πραγματικών Επιχειρήσεων</u>

<u>Συρία(2017-2018):</u>

Στην εμπόλεμη ζώνη της Συρίας καταγράφηκαν πολλαπλές περιπτώσεις όπου τα ρωσικά συστήματα ηλεκτρονικού πολέμου Krasukha-4 χρησιμοποιήθηκαν για εκτεταμένο jamming εναντίον UAVs των ΗΠΑ και των συμμάχων. Σύμφωνα με αναφορές, αρκετά drones έχασαν προσωρινά τον έλεγχο ή αναγκάστηκαν να τερματίσουν την αποστολή τους. Ερευνητές υποστήριξαν ότι οι επιθέσεις δεν περιορίστηκαν σε απλό jamming, αλλά πιθανόν συνδυάστηκαν με GPS spoofing, προκαλώντας

εκτροπή UAVs από τις προκαθορισμένες διαδρομές τους [77], [80]. Αυτό το περιστατικό ανέδειξε την ικανότητα των συνδυασμένων επιθέσεων να ακυρώνουν αποστολές ISR με ελάχιστο κόστος για τον επιτιθέμενο.

Ουκρανία (2022-σήμερα):

Η συνεχιζόμενη σύγκρουση στην Ουκρανία αποτελεί κορυφαίο παράδειγμα συνδυασμένων επιθέσεων EW και cyber. Τα ρωσικά συστήματα Murmansk-BN και Tirada-2 χρησιμοποιήθηκαν ευρέως για την παρεμβολή δορυφορικών επικοινωνιών και GPS, προκαλώντας απώλειες UAVs, αποτυχίες όπλων ακριβείας και διακοπές επικοινωνίας [54], [60]. Παράλληλα, έχουν καταγραφεί στοχευμένες κυβερνοεπιθέσεις σε δίκτυα διοίκησης, με σκοπό την παρακολούθηση ή και την εισαγωγή παραποιημένων δεδομένων [80]. Το πιο γνωστό περιστατικό ήταν η επίθεση στο δίκτυο δορυφορικών επικοινωνιών Viasat τον Φεβρουάριο του 2022, λίγες ώρες πριν την έναρξη της ρωσικής εισβολής. Η επίθεση προκάλεσε μαζική διακοπή δορυφορικών υπηρεσιών, επηρεάζοντας όχι μόνο στρατιωτικά συστήματα στην Ουκρανία, αλλά και πολιτικές υποδομές σε πολλές ευρωπαϊκές χώρες [60], [58]. Το γεγονός αυτό έδειξε πώς ένας συνδυασμός ηλεκτρονικού πολέμου και cyber μπορεί να λειτουργήσει ως προοίμιο στρατιωτικής επιχείρηση μεγάλης κλίμακας.

Θάλασσα της Νότιας Κίνας:

Στην περιοχή αυτή έχουν αναφερθεί επανειλημμένα περιστατικά GPS spoofing σε πολεμικά και εμπορικά πλοία. Οι ναυτικοί παρατηρούσαν τα στίγματα των πλοίων τους να σχηματίζουν «κυκλικές διαδρομές» ή να εμφανίζονται σε εντελώς λανθασμένες τοποθεσίες [60]. Οι επιθέσεις αυτές φέρεται να συνδυάστηκαν με παρεμβολές επικοινωνιών, προκαλώντας σύγχυση στη ναυσιπλοΐα και δημιουργώντας σοβαρούς κινδύνους σύγκρουσης [58], [79]. Εκτός από τις τεχνικές συνέπειες, τέτοια περιστατικά έχουν και στρατηγική διάσταση, καθώς δημιουργούν ένα περιβάλλον αβεβαιότητας και αποσταθεροποίησης σε μια γεωπολιτικά κρίσιμη περιοχή.

Μέση Ανατολή:

Στην Μέση Ανατολή, UAVs που χρησιμοποιούνταν για επιτήρηση και αναγνώριση φέρονται να εκτράπηκαν μέσω spoofing και να έχασαν τον έλεγχο λόγω jamming [54]. Σε αρκετές περιπτώσεις αναφέρθηκε ότι τα drones οδηγήθηκαν σε μη προγραμματισμένες προσγειώσεις, με αποτέλεσμα την απώλεια στρατηγικού υλικού και πολύτιμων δεδομένων ISR [60], [77]. Παράλληλα, έχουν καταγραφεί περιστατικά παραβίασης δικτύων C2, με εισαγωγή παραποιημένων εντολών που έμοιαζαν αυθεντικές [80]. Το γεγονός αυτό ανέδειξε ότι οι συνδυασμένες επιθέσεις δεν στοχεύουν μόνο στην απώλεια μεμονωμένων πλατφορμών, αλλά μπορούν να προκαλέσουν συστημική αποδιοργάνωση σε ολόκληρα δίκτυα διοίκησης.

Επιχειρησιακή Σημασία

Οι συνδυασμένες επιθέσεις ηλεκτρονικού πολέμου και κυβερνοεπιθέσεων έχουν ιδιαίτερη επιχειρησιακή σημασία, καθώς επηρεάζουν πολλαπλά επίπεδα της στρατιωτικής δραστηριότητας ταυτόχρονα. Η ιδιαιτερότητα τους δεν έγκειται μόνο στη δυσκολία ανίχνευσης, αλλά και στο γεγονός ότι μπορούν να προκαλέσουν συστημικές επιπτώσεις, από το τακτικό έως το στρατηγικό επίπεδο.

Σε στρατηγικό επίπεδο, οι συνδυασμένες επιθέσεις προσφέρουν τη δυνατότητα στον επιτιθέμενο να «τυφλώσει» ή να αποσταθεροποιήσει μια ολόκληρη δύναμη χωρίς να χρειαστεί να εκτοξεύσει πυρομαχικά. Αυτό αποτελεί σημαντικό πλεονέκτημα, καθώς με χαμηλό κόστος μπορεί να ακυρώσει την επιχειρησιακή υπεροχή του αντιπάλου. Εάν ο αντίπαλος στερηθεί για μικρό χρονικό διάστημα την πρόσβαση σε κρίσιμα δεδομένα, μπορεί να χάσει την πρωτοβουλία κινήσεων, με συνέπειες που καθορίζουν την έκβαση μιας σύγκρουσης.

Οι ψυχολογικές συνέπειες είναι εξίσου σημαντικές. Η ξαφνική απώλεια επικοινωνιών ή η αποκάλυψη ότι έχουν δοθεί ψευδείς εντολές μέσω spoofing δημιουργεί αβεβαιότητα και δυσπιστία στα στρατεύματα και στο προσωπικό διοίκησης. Η έλλειψη εμπιστοσύνης στα ίδια τα συστήματα μπορεί να οδηγήσει σε αναστολή επιχειρήσεων μέχρι να αποκατασταθεί η αξιοπιστία του δικτύου, κάτι που αποτελεί από μόνο του σημαντική νίκη για τον επιτιθέμενο [60], [70], [80].

5.1.4 Μέτρα Αντιμετώπισης και σύγχρονες τεχνολογίες

Η προστασία απέναντι σε επιθέσεις jamming και spoofing αποτελεί ένα από τα πιο απαιτητικά πεδία έρευνας στον ηλεκτρονικό πόλεμο [60]. Δεδομένου ότι οι απειλές εξελίσσονται συνεχώς, η άμυνα δεν μπορεί να στηρίζεται σε μία μόνο λύση. Αντίθετα, απαιτείται ένας συνδυασμός τεχνολογιών, τακτικών και οργανωτικών μέτρων, προσαρμοσμένων στο εκάστοτε περιβάλλον επιχειρήσεων και στον τύπο του συστήματος-στόχου.

Τεχνικές Προστασίας

Η προστασία των στρατιωτικών δικτύων από επιθέσεις παρεμβολής και παραπλάνησης βασίζεται σε ένα σύνολο τεχνολογικών μεθόδων που έχουν εξελιχθεί σημαντικά τα τελευταία χρόνια. Μία από τις πιο διαδεδομένες τεχνικές είναι η Frequency Hopping (FH) δηλαδή η ταχεία εναλλαγή συχνοτήτων μετάδοσης δυσκολεύει τον εντοπισμό και την παρεμβολή από τον αντίπαλο. Η τεχνολογία αυτή εφαρμόζεται σε σύγχρονα στρατιωτικά ραδιόφωνα, όπως τα Harris Falcon IV, τα οποία έχουν σχεδιαστεί για επιχειρήσεις σε περιβάλλον με έντονη ηλεκτρονική παρενόχληση [60].

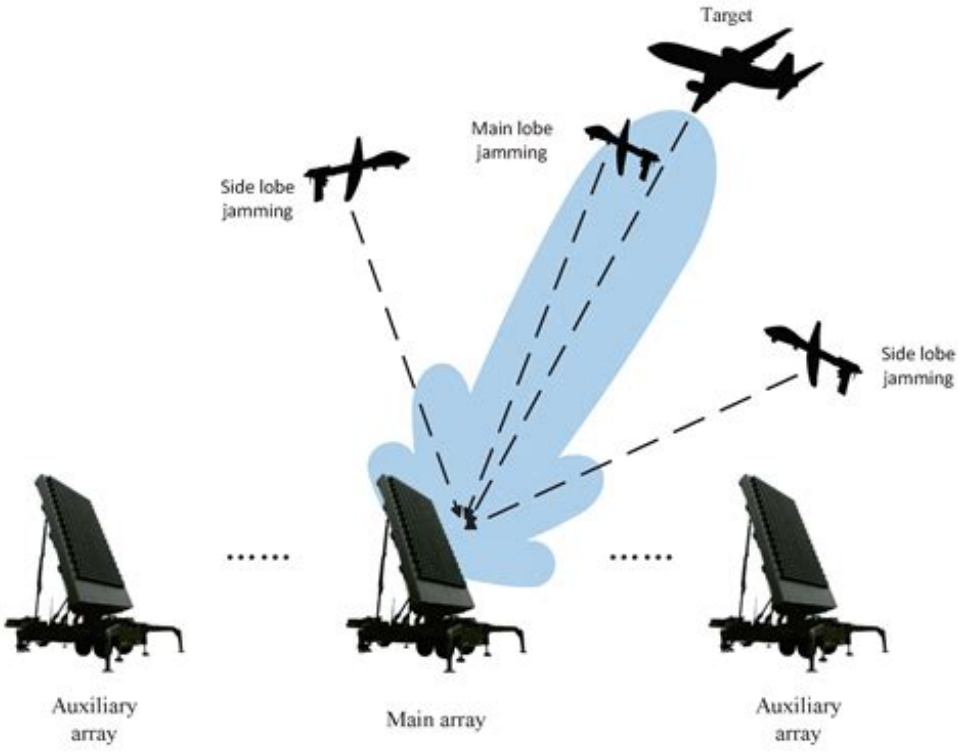
Εξίσου κρίσιμη εξέλιξη αποτελεί και η ανάπτυξη του στρατιωτικού GPS M-code της νέας γενιά στρατιωτικών δορυφορικών συστημάτων GPS ενσωματώνει ισχυρή κρυπτογράφηση, αυθεντικοποίηση και δυνατότητες ανίχνευσης spoofing. Το M-code μειώνει σημαντικά την πιθανότητα παραπλάνησης μέσω ψεύτικων σημάτων [77], [80].

Παράλληλα, η χρήση πολυαισθητηριακής πλοήγησης (Sensor Fusion) ενισχύει την επιχειρησιακή ανθεκτικότητα. Ο συνδυασμός GPS με αδρανειακά συστήματα πλοήγησης (INS-Inertial Navigation System), μαγνητόμετρα και αισθητήρες απεικόνισης παρέχει ανθεκτικότητα. Ακόμη και αν το GPS μπλοκαριστεί ή παραποιηθεί, το UAV ή το όχημα μπορεί να συνεχίσει με βάση τους εναλλακτικούς αισθητήρες [54], [80].

Η αξιοποίηση κατευθυντικών κεραιών & Beamforming αποτελεί επίσης κρίσιμο μέτρο προστασίας. Οι συστοιχίες φάσης (Phased Array Antennas) και τεχνικών beamforming μειώνει την επίδραση του jamming, επιτρέποντας στο δέκτη να εστιάζει μόνο στο χρήσιμο σήμα και να απορρίπτει παρεμβολές [60], [166].

Περαιτέρω ενίσχυση της ασφάλειας παρέχουν τα AI-based Ανίχνευση Ανωμαλιών, τα οποία αξιοποιούν τεχνικές Machine Learning και AI μπορούν να αναλύουν μοτίβα σημάτων και να εντοπίζουν έγκαιρα ύποπτες ανωμαλίες που υποδηλώνουν spoofing ή jamming. Έτσι, η απειλή μπορεί να εντοπιστεί πριν οδηγήσει σε επιχειρησιακή αποτυχία [80].

Τέλος, η εφαρμογή πλεονασμού Δικτύου(Redundancy) εξασφαλίζει τη συνέχιση της επικοινωνίας ακόμη και όταν μεμονωμένοι κόμβοι ή συνδέσεις τεθούν εκτός λειτουργίας. Η ύπαρξη εναλλακτικών κόμβων και καναλιών επικοινωνίας επιτρέπει τη συνέχιση των επιχειρήσεων ακόμη και όταν ένας κόμβος ή σύνδεση υποστεί επίθεση [54].



Σχήμα 42- Παράδειγμα τεχνικής beamforming με συστοιχίες κεραιών για την απόρριψη παρεμβολών [166]

Η τεχνική beamforming μέσω συστοιχιών κεραιών (CRPA- Controlled Reception Pattern Antennas) αποτελεί ένα από τα πιο αποτελεσματικά μέτρα προστασίας απέναντι στο jamming. Όπως φαίνεται και στο Σχήμα 42, η κατευθυντική δέσμη του δέκτη μπορεί να «στρίψει» ώστε να μεγιστοποιεί την απολαβή προς τον δορυφόρο ή τον φίλιο πομπό, ενώ ταυτόχρονα δημιουργεί «nulls» προς τις κατευθύνσεις των παρεμβολέων. Με αυτόν τον τρόπο, το σήμα του εχθρού απορρίπτεται χωρικά, μειώνοντας τον λόγο παρεμβολής προς σήμα (J/S) σε επίπεδα που επιτρέπουν τη συνέχιση της επικοινωνίας [60], [166].

Οργανωτικά και Επιχειρησιακά Μέτρα

Η τεχνολογία δεν είναι αρκετή χωρίς κατάλληλη εκπαίδευση. Οι χειριστές πρέπει να είναι σε θέση να αναγνωρίζουν τα πρώιμα σημάδια spoofing ή jamming και να αντιδρούν γρήγορα. Επιπλέον, οι δοκιμές σε πραγματικές συνθήκες – μέσω ασκήσεων ηλεκτρονικού πολέμου- αποκαλύπτουν τρωτά σημεία και επιτρέπουν τη βελτίωση των διαδικασιών αντίδρασης [54], [80]. Η συνεχείς επίγνωση ραδιοφάσματος (Spectrum Awareness) μέσω παρακολούθησης του ραδιοφάσματος πριν και κατά τη διάρκεια της αποστολής βοηθά στον εντοπισμό ύποπτων δραστηριοτήτων, προσφέροντας προειδοποίηση σε πραγματικό χρόνο [60].

Στρατηγική Προσέγγιση

Ο στόχος δεν είναι η πλήρης αποτροπή της επίθεσης- κάτι που συχνά είναι αδύνατο- αλλά η επίτευξη ανθεκτικότητας (resilience). Αυτό σημαίνει ότι τα συστήματα πρέπει να μπορούν να συνεχίσουν να λειτουργούν, έστω και με περιορισμένες δυνατότητες, ακόμη και κάτω από εχθρική πίεση. Η λογική αυτή βασίζεται στην ανοχή σε σφάλματα και στη διατήρηση κρίσιμων λειτουργιών, ώστε να εξασφαλίζεται η συνέχιση της αποστολής [54], [80].

5.2 Επιθέσεις σε IoMT & Data Leakage

Το IoMT περιγράφει το οικοσύστημα διασυνδεδεμένων στρατιωτικών αισθητήρων, πλατφορμών και κόμβων edge (UAVs, οχήματα, έξυπνα κράνη, φορητοί βιοαισθητήρες, ρομποτικές μονάδες, σταθμοί προκεχωρημένης διοίκησης, που ανταλλάσσουν δεδομένα σε πραγματικό χρόνο για να ενισχύσουν επιχειρησιακή επίγνωση, συνέργεια C2/C4ISR και αυτοματοποίηση αποστολών [167]. Η συνεχής ροή τηλεμετρίας (θέση, κατάσταση συστημάτων, βίντεο/EO-IR, logistics) επιταχύνει τη λήψη αποφάσεων και μειώνει τους κύκλους παρατήρησης- προσανατολισμού-απόφασης-ενέργειας(OOAD-Object Oriented Analysis and Design).

Η ίδια όμως δικτύωση εισάγει νέες επιφάνειες επίθεσης. Το IoMT χαρακτηρίζεται από ετερογένεια συσκευών, κατανεμημένη τοποθέτηση σε εχθρικά περιβάλλοντα και περιορισμούς SWaP (ισχύς/υπολογισμός/βάρος), που δυσκολεύουν την ισχυρή κρυπτογράφηση, το συνεχές patching και το ασφαλές lifecycle management [168]. Έτσι, αυξάνεται η έκθεση σε:

- Κακόβουλη εισαγωγή λογισμικού (trojans, backdoors, APT),
- Παραποίηση ή έγχυση δεδομένων (data integrity attacks) στην αλυσίδα C2/ISR,
- Ακούσια ή σκόπιμη διαρροή δεδομένων (data leakage/exfiltration) από μη εγκεκριμένες εφαρμογές, κακή ρύθμιση προσβάσεων ή ασθενή πολιτική χειρισμού διαβαθμισμένων πληροφοριών [169].

Σε επιχειρησιακούς όρους, ένα συμβάν data leakage μπορεί να αποκαλύψει τοποθεσίες μονάδων, μοτίβα κινήσεων, τεχνικές ικανότητες αισθητήρων ή ακόμη και κανόνες εμπλοκής – πληροφορίες με άμεσο αντίκτυπο στην ασφάλεια δυνάμεων και στην επιτυχία αποστολών [170]. Παράλληλα, στοχευμένες επιθέσεις σε IoMT κόμβους δύνανται να λειτουργήσουν ως «μοχλός» για πλάγια κίνηση (lateral movement) προς κρίσιμες υπηρεσίες C2 ή SATCOM backhauls, υπονομεύοντας διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα σε επίπεδο σχηματισμού.

5.2.1 Μορφές επιθέσεων και τεχνικές παρέμβασης

Οι επιθέσεις στα στρατιωτικά δίκτυα και ιδιαίτερα στο IoMT λαμβάνουν ποικίλες μορφές, από κακόβουλο λογισμικό μέχρι εξελιγμένες, στοχευμένες απειλές μεγάλης διάρκειας. Οι πλέον συχνές και επικίνδυνες μορφές περιλαμβάνουν επιθέσεις μέσω τροποποιημένου λογισμικού(Trojanized Software) , backdoors και κρυφών καναλιών επικοινωνίας, spyware και advanced persistent threats(APTs).

Μια από τις πιο διαδεδομένες τεχνικές είναι η εισαγωγή κακόβουλου κώδικα σε φαινομενικά «αθώες» εφαρμογές ή firmware-μία μορφή επίθεσης γνωστή ως Trojanized software. Ιδιαίτερα επικίνδυνες είναι οι επιθέσεις εφοδιαστικής αλυσίδας (supply chain attacks), όπου ένας ενημερωτής λογισμικού (software updater) περιέχει «κρυφές» λειτουργίες. Το κακόβουλο payload παραμένει αδρανές μέχρι να ενεργοποιηθεί στο πεδίο επιχειρήσεων [168]. Για παράδειγμα, ένας μη πιστοποιημένος driver UAV μπορεί να επιτρέψει στον αντίπαλο να παρακάμψει τα πρωτόκολλα ασφαλείας και να αποκτήσει απομακρυσμένο έλεγχο [171].

Εξίσου σοβαρή απειλή αποτελούν τα backdoors και τα covert channels δηλαδή μη εξουσιοδοτημένες «θύρες» που τοποθετούνται στο λογισμικό ή στο υλικό και επιτρέπουν στον επιτιθέμενο να εισέλθει στο δίκτυο χωρίς να περάσει από κανονικούς μηχανισμούς ελέγχου ταυτότητας. Σε στρατιωτικά σενάρια, τα backdoors μπορούν να αξιοποιηθούν για πρόσβαση σε δίκτυα C2/C4ISR ή ακόμα και σε δεδομένα αισθητήρων μάχης [168]. Οι covert channels (κρυφά κανάλια επικοινωνίας) μπορούν να χρησιμοποιηθούν για την αθόρυβη εξαγωγή πληροφοριών (data exfiltration) χωρίς να γίνουν αντιληπτά από παραδοσιακά IDS. [172].

Μια πιο ύπουλη κατηγορία είναι τα spyware, προγράμματα που εγκαθίστανται σε IoMT κόμβους (UAVs, στρατιωτικά tablets, φορητούς αισθητήρες) με στόχο να συλλέγουν τηλεμετρία, επικοινωνίες ή ακόμα και βιομετρικά δεδομένα στρατιωτών. Σε αντίθεση με το malware που προκαλεί

βλάβες, τα spyware λειτουργούν «σιωπηρά» και εστιάζουν σε data exfiltration [171], [169]. Σενάρια περιλαμβάνουν καταγραφή πορειών εφοδιαστικών οχημάτων ή αποκάλυψη της θέσης ομάδων πεζικού σε πραγματικό χρόνο.

Ακόμη πιο επικίνδυνες είναι οι APT οι οποίες χαρακτηρίζονται από μακροχρόνια παραμονή, χαμηλό θόρυβο και στόχο τη συνεχή συλλογή πληροφοριών. Σε περιβάλλον IoMT, μια APT μπορεί να ξεκινήσει με phishing ή supply chain injection, να εξαπλωθεί (lateral movement) μέσα στο δίκτυο, και να διατηρήσει «κρυφή» πρόσβαση για μήνες. Η ενεργοποίηση μπορεί να γίνει σε κρίσιμη φάση, οδηγώντας σε αλλοίωση δεδομένων αισθητήρων, αποδιοργάνωση C2 ή παραπλάνηση UAVs [172].

Ακόμη και χωρίς φυσική καταστροφή συστημάτων, η διαρροή ή παραποίηση πληροφορίας μπορεί να έχει ως αποτέλεσμα αποδιοργάνωση επιχειρήσεων, καθυστερήσεις στη λήψη αποφάσεων και απώλεια εμπιστοσύνης στις ίδιες τις υποδομές IoMT. Το τελικό αποτέλεσμα μπορεί να είναι η αποτυχία αποστολής, γεγονός που καθιστά τις παραπάνω απειλές εξίσου επικίνδυνες με συμβατικές επιθέσεις φυσικής καταστροφής [173], [174].

5.2.2 Διαρροή δεδομένων και επιχειρησιακό ρίσκο

Η διαρροή δεδομένων (data leakage) στα στρατιωτικά δίκτυα αποτελεί έναν από τους πλέον κρίσιμους κινδύνους που συνδέονται με την εκτεταμένη χρήση του IoMT [169]. Σε αντίθεση με τις κλασικές κυβερνοεπιθέσεις που έχουν ως στόχο τη διακοπή λειτουργίας ή την άμεση καταστροφή, η διαρροή δεδομένων επικεντρώνεται στη σιωπηρή εξαγωγή πληροφοριών. Αυτό καθιστά ιδιαίτερα επικίνδυνη, καθώς μπορεί να περάσει απαρατήρητη για μεγάλα χρονικά διαστήματα [173].

Η διαρροή μπορεί να προκύψει από:

- Εξωτερικές απειλές: κακόβουλο λογισμικό, APTs που εγκαθίστανται σε IoMT κόμβους, επιθέσεις Man-in-the-Middle σε μη κρυπτογραφημένα κανάλια επικοινωνίας, ή υποκλοπές δορυφορικών uplinks/downlinks [168], [172].
- Εσωτερικές αδυναμίες: παραλείψεις προσωπικού, λανθασμένες ρυθμίσεις (misconfigurations), χρήση μη πιστοποιημένων εφαρμογών, ή αμέλεια στην ενημέρωση λογισμικού [173], [175].

Είδη Περιστατικών Διαρροής Δεδομένων στο IoMT

Τα περιστατικά διαρροής δεδομένων IoMT αποτελούν έναν από τους πλέον κρίσιμους παράγοντες απώλειας εμπιστευτικότητας και επιχειρησιακής αποτελεσματικότητας. Οι κυριότερες μορφές τέτοιων περιστατικών σχετίζονται με τη χρήση μη ασφαλών καναλιών επικοινωνίας, την απουσία σαφών πολιτικών πρόσβασης, την ανεπαρκή διαχείριση συσκευών και τη μη κρυπτογραφημένη μεταφορά δεδομένων.

Ένα από τα πιο συχνά προβλήματα αφορά τη χρήση ακατάλληλων καναλιών επικοινωνίας, όπως εμπορικές εφαρμογές επικοινωνίας (π.χ. email providers, cloud storage) που δεν πληρούν στρατιωτικά πρότυπα ασφαλείας. Σε αυτές τις περιπτώσεις, ακόμη και αν οι πληροφορίες είναι διαβαθμισμένες, μεταφέρονται μέσω μη ασφαλών καναλιών, με αποτέλεσμα να εκτίθενται σε πιθανή παρακολούθηση, υποκλοπή ή καταγραφή. Ένα παράδειγμα είναι η αποστολή συντεταγμένων ή αναφορών αποστολών μέσω μη στρατιωτικά πιστοποιημένων εφαρμογών messaging. Η πρακτική αυτή, πέραν του άμεσου κινδύνου διαρροής, υπονομεύει την εμπιστοσύνη στο δίκτυο ασφαλείας συνολικά [169].

Εξίσου σημαντική αιτία παραβίασης αποτελεί η απουσία μηχανισμών Role-Based Access Control(RBAC).Η έλλειψη σαφώς ορισμένων πολιτικών πρόσβασης βάσει ρόλων σημαίνει ότι μέλη του προσωπικού αποκτούν δικαιώματα πέρα από όσα είναι απολύτως αναγκαία. Αυτό μπορεί να οδηγήσει είτε σε ακούσιες διαρροές (π.χ. μη εξειδικευμένο προσωπικό να αντιγράψει ευαίσθητα δεδομένα χωρίς να κατανοεί την κρισιμότητα τους) είτε σε κατάχρηση πρόσβασης. Σε περιβάλλον IoMT, όπου διαφορετικοί αισθητήρες και πλατφόρμες συγκεντρώνουν δεδομένα, η απουσία RBAC πολλαπλασιάζει τον κίνδυνο απώλειας κρίσιμης πληροφορίας [175].

Η ανεπαρκής διαχείριση των IoMT συσκευών αποτελεί επίσης έναν από τους πιο αδύναμους κρίκους στην αλυσίδα ασφάλειας. Η ετερογένεια και η μαζικότητα των συσκευών IoMT καθιστούν δύσκολη τη συνεχή επιτήρηση τους. Συσκευές που λειτουργούν με παλιές εκδόσεις λογισμικού ή χωρίς πιστοποίηση ασφαλείας γίνονται εύκολοι στόχοι. Οι αντίπαλοι μπορούν να εκμεταλλευτούν γνωστές ευπάθειες (CVEs) για να εισάγουν κακόβουλο κώδικα ή να αποκτήσουν πρόσβαση σε δίκτυα διοίκησης. Ειδικά σε forward-deployed συσκευές (π.χ. φορητοί αισθητήρες πεζικού ή drones), η μη τήρηση προτύπων ασφαλείας μπορεί να οδηγήσει σε ταχεία διαρροή δεδομένων με υψηλό επιχειρησιακό κόστος [169].

Τέλος, η μεταφορά δεδομένων χωρίς κρυπτογράφηση εκθέτει τα πακέτα επικοινωνίας σε επιθέσεις Man-in-the-Middle (MITM). Σε τέτοιες περιπτώσεις, ο επιτιθέμενος μπορεί να υποκλέψει, να αλλοιώσει ή να εισαγάγει δεδομένα στη ροή επικοινωνίας. Αυτό είναι ιδιαίτερα επικίνδυνο για δεδομένα πλοήγησης UAVs, τηλεμετρίας logistics ή βιοαισθητήρων στρατιωτών, τα οποία αν αλλοιωθούν μπορούν να δημιουργήσουν παραπλανητική εικόνα στο επίπεδο C2 [172].

Οι παραπάνω αδυναμίες δεν υπονομεύουν μόνο την εμπιστευτικότητα, αλλά και την ακεραιότητα και τη διαθεσιμότητα των επιχειρησιακών δεδομένων (CIA triad) [173]. Ακόμη και μια περιορισμένη διαρροή οδηγεί σε λανθασμένη επιχειρησιακή εικόνα: τα δεδομένα που φτάνουν στο κέντρο επιχειρήσεων δεν αντικατοπτρίζουν την πραγματικότητα, καθυστερήσεις στη λήψη αποφάσεων: η αξιοπιστία της πληροφορίας τίθεται υπό αμφισβήτηση, με αποτέλεσμα η διοίκηση να διστάζει να δράσει και τελικά σε αποτυχία αποστολής: σε κρίσιμες περιπτώσεις, η παραπλανητική ή ελλιπής πληροφορία μπορεί να οδηγήσει σε απώλειες, αποδιοργάνωση ή ακύρωση επιχειρήσεων.

Συνεπώς, οι διαρροές δεδομένων -είτε εκούσιες είτε ακούσιες- αποτελούν καταλυτικό παράγοντα αποσταθεροποίησης για τις επιχειρήσεις που βασίζονται στο IoMT.

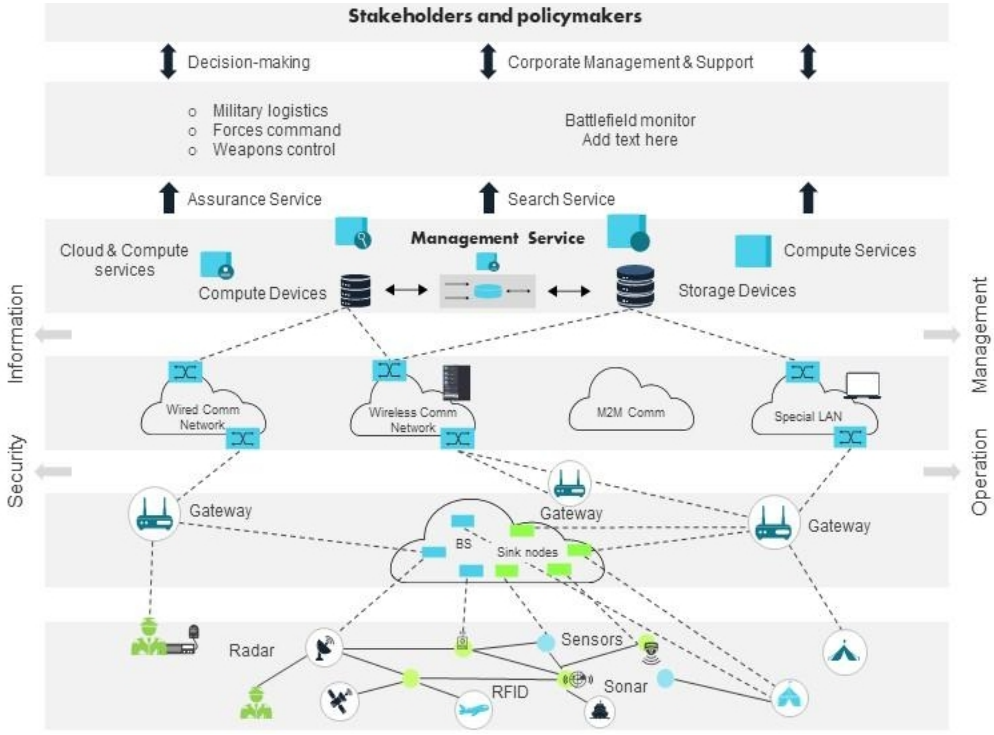
Παράδειγμα Πραγματικού Περιστατικού

Σε μια άσκηση του ΝΑΤΟ, φορητές συσκευές IoMT που είχαν αναπτυχθεί για την παρακολούθηση της εφοδιαστικής αλυσίδας (logistics monitoring) λειτούργησαν με μη εγκεκριμένη εμπορική εφαρμογή. Η εφαρμογή, χωρίς να το γνωρίζει το στρατιωτικό προσωπικό, μετέδιδε δεδομένα τοποθεσίας και άλλες παραμέτρους λειτουργίας σε servers τρίτων παροχών εκτός του στρατιωτικού δικτύου. Η διαδικασία αυτή έγινε αυτόματα, χωρίς την επίγνωση των χειριστών, με αποτέλεσμα να διαρρεύσουν ευαίσθητες πληροφορίες σχετικά με τις κινήσεις και την τοποθεσία των μονάδων [173].

Το περιστατικό ανέδειξε με ιδιαίτερα εμφατικό τρόπο τρεις βασικές αδυναμίες. Πρώτον διαπιστώθηκε απουσία προληπτικών ελέγχων λογισμικού καθώς δεν υπήρξε πλήρης αξιολόγηση των εφαρμογών πριν την επιχειρησιακή χρήση τους. Ένα αυστηρό πλαίσιο πιστοποίησης θα είχε αποτρέψει τη χρήση μη ασφαλών εφαρμογών. Δεύτερον, η μη συμμόρφωση με τις πολιτικές κυβερνοασφάλειας του ΝΑΤΟ ανέδειξε την ανάγκη για ενοποιημένα και υποχρεωτικά πρότυπα ασφάλειας. παράλειψη αυτή έδειξε ότι η τυπική πιστοποίηση ασφαλείας δεν είναι απλώς διοικητική διαδικασία, αλλά προϋπόθεση για την επιχειρησιακή προστασία. Τρίτον, διαπιστώθηκε ανεπαρκής εκπαίδευση προσωπικού καθώς οι χρήστες των συσκευών δεν είχαν την κατάλληλη εκπαίδευση ώστε να αναγνωρίσουν την επικινδυνότητα χρήσης μη εγκεκριμένου λογισμικού, γεγονός που οδήγησε σε ακούσια, αλλά σοβαρή παραβίαση.

Η σημασία του περιστατικού είναι διττή. Σε τεχνικό κομμάτι, έδειξε ότι ακόμη και εφαρμογές που φαίνονται ακίνδυνες μπορούν να οδηγήσουν σε διαρροή κρίσιμων επιχειρησιακών δεδομένων, θέτοντας σε κίνδυνο την ασφάλεια μονάδων. Σε επιχειρησιακό κομμάτι, υπογράμμισε ότι οι ακούσιες διαρροές (λόγω λάθους ή αμέλειας) μπορεί να έχουν εξίσου σοβαρές συνέπειες με τις εσκεμμένες επιθέσεις του εχθρού. Ακόμα και χωρίς κυβερνοεπιθέσεις, η κακή διαχείριση του IoMT είναι αρκετή για να δημιουργήσει στρατηγικό πλεονέκτημα για τον αντίπαλο.

Συνεπώς, το παράδειγμα αυτό αναδεικνύει την ανάγκη για αυστηρούς ελέγχους και πιστοποίηση λογισμικού πριν από την επιχειρησιακή χρήση, πλήρη αξιολόγηση συμβατότητας με στρατιωτικές πολιτικές ασφαλείας καθώς και για συνεχή εκπαίδευση και ευαισθητοποίηση προσωπικού, ώστε να περιορίζονται τα ανθρώπινα λάθη.



Σχήμα 43- Αρχιτεκτονική IoMT για στρατιωτικά δίκτυα με πολυεπίπεδη διάρθρωση [176]

Το Σχήμα 43 παρουσιάζει την πολυεπίπεδη αρχιτεκτονική ενός δικτυωμένου στρατιωτικού IoMT. Η πληροφορία συλλέγεται από αισθητήρες (radars, RFID, sonar) και μεταφέρεται μέσω gateways σε δίκτυα επικοινωνίας (wired, wireless, M2M), τα οποία τροφοδοτούν υπηρεσίες αποθήκευσης και cloud. Στη συνέχεια, τα δεδομένα ενσωματώνονται σε επίπεδα υποστήριξης αποφάσεων, παρέχοντας κρίσιμη επιχειρησιακή εικόνα στους φορείς διοίκησης.

Ωστόσο, κάθε επίπεδο αυτής της αλυσίδας αποτελεί δυνητικό σημείο ευπάθειας. Στους αισθητήρες, η απουσία πιστοποιημένου firmware μπορεί να οδηγήσει σε παραποίηση δεδομένων. Στα gateways, ανεπαρκής έλεγχος ταυτότητας ή μη κρυπτογραφημένες συνδέσεις ενδέχεται να επιτρέψουν μη εξουσιοδοτημένη πρόσβαση στα δίκτυα επικοινωνίας, επιθέσεις τύπου Man-in-the-Middle και spoofing μπορούν να αλλοιώσουν την ακεραιότητα των δεδομένων. Ενώ στο cloud και στα συστήματα αποθήκευσης, αδυναμίες στις πολιτικές πρόσβασης ή στη διαχείριση λογισμικού μπορεί να προκαλέσουν εκτεταμένες διαρροές [173].

5.2.3 Zero Trust: Στρατηγική μηδενικής εμπιστοσύνης

Η αρχιτεκτονική Zero Trust (ZTA) έχει αναδειχθεί ως μία από τις σημαντικότερες στρατηγικές κυβερνοάμυνας, ειδικά στο περιβάλλον του IoMT. Σε αντίθεση με τις παραδοσιακές προσεγγίσεις ασφαλείας που θεωρούν ότι οι απειλές προέρχονται κυρίως από το «εξωτερικό» του δικτύου, το Zero Trust ξεκινά από την παραδοχή ότι ο κίνδυνος μπορεί να βρίσκεται παντού- ακόμη και εντός των ίδιων των στρατιωτικών δικτύων. Έτσι, κανένας χρήστης, συσκευή ή υπηρεσία δεν θεωρείται έμπιστος από προεπιλογή, ακόμη κι αν βρίσκεται ήδη «μέσα» στο σύστημα [174].

Αντίθετα, κάθε ενέργεια πρόσβασης υπόκειται σε αυστηρό έλεγχο ταυτότητας (authentication) δηλαδή χρήση ισχυρών μηχανισμών, όπως multi-factor authentication (MFA) και πιστοποιητικά [174]. Παράλληλα εφαρμόζεται αξιολόγηση κινδύνου σε πραγματικό χρόνο (risk-based assessment), η οποία λαμβάνεται υπόψη παραγόντων όπως η τοποθεσία της συσκευής, η συμπεριφορά χρήστη ή το ιστορικό ασφαλείας. Τέλος, οι πολιτικές περιορισμού πρόσβασης (policy enforcement) ακολουθούν την αρχή least privilege, ώστε κάθε οντότητα να έχει μόνο τα δικαιώματα που είναι απολύτως απαραίτητα για τον ρόλο της [174].

Η λογική αυτή στηρίζεται σε τρεις θεμελιώδεις άξονες. Πρώτον η μικροτμηματοποίηση (microsegmentation) χωρίζει το δίκτυο σε ανεξάρτητες ζώνες ασφάλειας. Έτσι, ακόμη κι αν ένας αισθητήρας, UAV ή κόμβος IoMT παραβιαστεί, η ζημιά περιορίζεται τοπικά και δεν εξαπλώνεται στο υπόλοιπο σύστημα. Για παράδειγμα, παραβίαση σε έναν αισθητήρα logistics δεν σημαίνει αυτόματα πρόσβαση σε συστήματα C2 [174]. Δεύτερον, η κρυπτογράφηση end-to-end εξασφαλίζει την προστασία όλων των επικοινωνίων –από δεδομένα αισθητήρων μέχρι τηλεμετρία UAV και ροές πληροφοριών C2– κρυπτογραφούνται με ισχυρά πρωτόκολλα (π.χ. AES-256, TLS 1.3). Αυτό εξασφαλίζει ότι ακόμη και αν τα δεδομένα υποκλαπούν, δεν μπορούν να αξιοποιηθούν χωρίς το αντίστοιχο κλειδί [177]. Τρίτον, η συνεχής παρακολούθηση και ανάλυση ανωμαλιών όπου χρησιμοποιούνται συστήματα ανάλυσης βασισμένα σε AI/ML, τα οποία εντοπίζουν ασυνήθιστη ή ύποπτη συμπεριφορά σε πραγματικό χρόνο. Για παράδειγμα, η ξαφνική αποστολή μεγάλου όγκου δεδομένων από έναν IoMT κόμβο μπορεί να αποτελεί ένδειξη data exfiltration και να σημάνει συναγερμό [178].

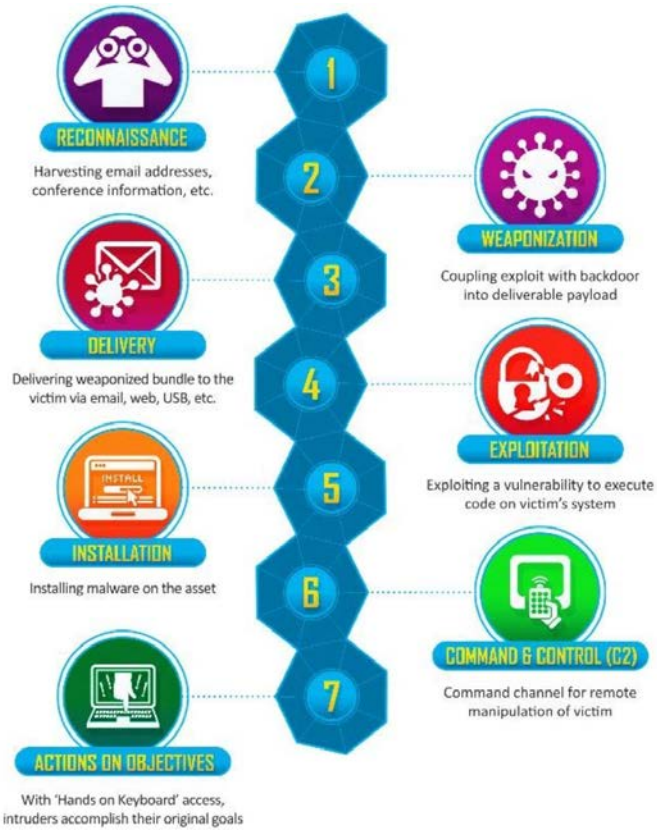
Η υιοθέτηση του Zero Trust δεν αποτελεί μόνο τεχνικό μέτρο· είναι μια ολιστική στρατηγική επιλογή που ενισχύει την ανθεκτικότητα (resilience) των δικτύων. Σε περιβάλλοντα όπου οι απειλές είναι συνεχείς, όπως τα πεδία επιχειρήσεων, η ZTA διασφαλίζει ότι ακόμα και μια επιτυχημένη διείσδυση δεν θα οδηγήσει σε συστημική κατάρρευση, αλλά θα περιοριστεί τοπικά.

Το Cyber Kill Chain, που αναπτύχθηκε από τη Lockheed Martin, περιγράφει την τυπική πορεία μιας κυβερνοεπίθεσης μέσα από επτά στάδια. Η ανάλυση αυτής της «αλυσίδας» βοηθά στη συστηματική κατανόηση του τρόπου με τον οποίο οι επιτιθέμενοι σχεδιάζουν και υλοποιούν τις επιθέσεις τους, και κατ' επέκταση, στον εντοπισμό των κατάλληλων σημείων παρέμβασης για την άμυνα [179].

<u>Στάδια του Cyber Kill Chain:</u>

1. Reconnaissance (Αναγνώριση): Συλλογή πληροφοριών για τον στόχο, π.χ. μη ασφαλείς IoMT συσκευές, ανοιχτές θύρες, εκτεθειμένα APIs [180].
2. Weaponization (Εξοπλισμός): Δημιουργία κακόβουλου payload, όπως trojanized firmware ή κακόβουλα scripts [168].

3. Delivery (Παράδοση): Μεταφορά του payload στον στόχο μέσω email, USB, ασύρματων καναλιών ή ενημερώσεων λογισμικού.
4. Exploitation (Εκμετάλλευση): Εκμετάλλευση ευπάθειας για εκτέλεση κακόβουλου κώδικα (π.χ. buffer overflow, μη ενημερωμένο firmware) [172].
5. Installation (Εγκατάσταση): Εγκατάσταση malware ή backdoors σε IoMT κόμβους για μόνιμη πρόσβαση [174].
6. Command & Control : Δημιουργία κρυφών καναλιών επικοινωνίας με τον επιτιθέμενο για απομακρυσμένο έλεγχο [178].
7. Actions on Objectives (Ενέργειες στον Στόχο): Υλοποίηση του τελικού σκοπού, όπως data exfiltration, παραπλάνηση UAVs ή υπονόμευση C2 συστημάτων [181].



Σχήμα 44- Επτά στάδια μιας τυπικής κυβερνοεπίθεσης σύμφωνα με το μοντέλο Cyber Kill Chain [179]

Κάθε στάδιο(βλέπε Σχήμα 44) περιγράφει μία φάση επίθεσης και αντιστοιχεί σε σημεία όπου είναι δυνατή η ανίχνευση και η αναχαίτιση, ειδικά σε περιβάλλον IoMT.

Η κατανόηση της Kill Chain επιτρέπει στις στρατιωτικές δυνάμεις να εφαρμόσουν αμυντικά μέτρα πολλαπλών επιπέδων (defense in depth), εντοπίζοντας την επίθεση όσο το δυνατόν νωρίτερα. Σε συνδυασμό με την αρχιτεκτονική Zero Trust, κάθε στάδιο μετατρέπεται σε σημείο ελέγχου που μειώνει τις πιθανότητες επιτυχίας του αντιπάλου.

5.2.4 Μέτρα αντιμετώπισης και πολιτικές ασφάλειας

Η προστασία του IoMT δεν μπορεί να βασιστεί σε μία και μοναδική λύση, καθώς οι απειλές εξελίσσονται διαρκώς και προέρχονται από πολλαπλά επίπεδα – τεχνικό, οργανωτικό και επιχειρησιακό. Για τον λόγο αυτόν απαιτείται ένας πολυεπίπεδος συνδυασμός μέτρων που περιλαμβάνει τεχνολογικούς μηχανισμούς, σαφείς διαδικασίες και συνεχή επιμόρφωση του προσωπικού [182]. Μόνο έτσι μπορεί να επιτευχθεί η ανθεκτικότητα σε ένα περιβάλλον όπου οι κυβερνοαπειλές και οι κίνδυνοι διαρροής δεδομένων γίνονται ολοένα και πιο σύνθετοι.

Σε τεχνολογικό επίπεδο, καθοριστικό ρόλο διαδραματίζει η κρυπτογράφηση end-to-end, στην οποία γίνεται χρήση ισχυρών αλγορίθμων (AES-256, elliptic curve cryptography) σε όλα τα επίπεδα διασφαλίζει ότι τα δεδομένα IoMT προστατεύονται τόσο στη μεταφορά όσο και στην αποθήκευση. Έτσι, ακόμα και αν παγιδευτούν από αντίπαλο, δεν μπορούν να αξιοποιηθούν χωρίς τα κλειδιά αποκρυπτογράφησης [177].

Εξίσου κρίσιμη είναι η ενσωμάτωση συστημάτων ανίχνευσης και πρόληψης εισβολών (IDS/IPS). Η ενσωμάτωση τεχνικών τεχνητής νοημοσύνης και machine learning επιτρέπει τον εντοπισμό ανωμαλιών στη ροή δεδομένων. Ένα IDS μπορεί να αναγνωρίσει απόπειρες jamming ή spoofing, ενώ ένα IPS μπορεί να αποκλείσει σε πραγματικό χρόνο ύποπτη δραστηριότητα [178].

Επιπλεόν, η πρόσβαση βάσει ρόλων (RBAC) ενισχύει την ασφάλεια με την εφαρμογή της αρχής least privilege περιορίζει την πρόσβαση μόνο στις απολύτως απαραίτητες λειτουργίες, μειώνοντας τις πιθανότητες ακούσιας ή κακόβουλης διαρροής [175]. Παράλληλα, η ανάπτυξη redundancy & εφεδρικών υποδομών όπως η ύπαρξη εναλλακτικών κόμβων επικοινωνίας, δορυφορικών καναλιών και εφεδρικών servers επιτρέπει τη συνέχιση των επιχειρήσεων ακόμα και σε περίπτωση κυβερνοεπίθεσης ή αστοχίας ενός συστήματος [181]. Εξίσου σημαντική είναι η αξιολόγηση και πιστοποίηση IoMT συσκευών που πρέπει κάθε συσκευή που εισέρχεται στο δίκτυο πρέπει να έχει περάσει από penetration testing, ελέγχους συμμόρφωσης με τα πρότυπα NIST ή τα NATO STANAGs, ώστε να διασφαλίζεται ότι δεν αποτελεί «κρυφή πύλη» για τον αντίπαλο [181], [183].

Σε οργανωτικό επίπεδο, το ανθρώπινο στοιχείο παραμένει η μεγαλύτερη ευπάθεια. Η εκπαίδευση χειριστών και διοικητών μειώνει τον κίνδυνο λαθών, όπως χρήση μη πιστοποιημένων εφαρμογών ή ακούσια διαρροή δεδομένων [177]. Παράλληλα, η τακτική ανασκόπηση πολιτικών ασφαλείας εξασφαλίζει ότι οι διαδικασίες πρέπει να αναθεωρούνται συχνά με βάση τις νέες απειλές και τις τεχνολογικές εξελίξεις. Έτσι, αποφεύγονται κενά που μπορεί να εκμεταλλευτεί ο αντίπαλος [182]. Η καθιέρωση μιας κουλτούρας cyber hygiene και awareness μέσα από απλές πρακτικές, όπως η συχνή αλλαγή κωδικών, ο έλεγχος πρόσβασης συσκευών και η αναφορά ύποπτης δραστηριότητας, μειώνουν δραστικά την επιφάνεια επίθεσης [177]. Τέλος, η εφαρμογή της αρχιτεκτονικής ZTA όπως αναλύθηκε στο προηγούμενο υποκεφάλαιο, κανένας χρήστης ή συσκευή δεν θεωρείται αξιόπιστος εκ

προοιμίου. Η ZTA λειτουργεί συμπληρωματικά με την αρχή του defense in depth, δημιουργώντας πολλαπλές «γραμμές άμυνας» [174].

Στο στρατιωτικό επίπεδο, το IoMT έχει μεταμορφώσει τον τρόπο διεξαγωγής των επιχειρήσεων, προσφέροντας ταχύτητα, ακρίβεια και πλήρη επιχειρησιακή εικόνα (situational awareness). Όμως, αυτή η δυνατότητα συνοδεύεται από αυξημένες απαιτήσεις σε ζητήματα ασφάλειας. Οι επιθέσεις (jamming, spoofing, APTs) και οι διαρροές δεδομένων δεν είναι υποθετικές, αλλά πραγματικές απειλές που συμβαίνουν με ολοένα αυξανόμενη συχνότητα και πολυπλοκότητα[107]. Η προστασία των πληροφοριών σε ένα δικτυοκεντρικό πεδίο μάχης δεν αποτελεί απλώς τεχνικό ζήτημα· είναι ζήτημα επιχειρησιακής επιβίωσης.

Συνεπώς, η εφαρμογή συνδυασμένων τεχνικών, η συνεχής επαγρύπνηση και η διαρκής βελτίωση των μηχανισμών ασφαλείας αποτελούν βασικές προϋποθέσεις για την ασφαλή και αποτελεσματική αξιοποίηση των δυνατοτήτων που προσφέρει το IoMT.

5.3 Επιθετικές Κυβερνοεπιχειρήσεις και Άμυνα

Ο κυβερνοχώρος έχει καθιερωθεί ως το πέμπτο επιχειρησιακό πεδίο πολέμου, δίπλα στη στεριά, τη θάλασσα, τον αέρα και το διάστημα. Στη σύγχρονη εποχή, οι κυβερνοεπιθέσεις δεν αποτελούν μελλοντικό σενάριο, αλλά μια διαρκή και κλιμακούμενη πραγματικότητα που επηρεάζει την ισορροπία ισχύος μεταξύ κρατών και συμμαχιών [184].

Η φύση του κυβερνοπολέμου διαφέρει ριζικά από τα συμβατικά μέσα ισχύος, καθώς χαρακτηρίζεται από χαμηλό κόστος σε σύγκριση με τα συμβατικά όπλα και από τη δυνατότητα μαζικής κλιμάκωσης με μικρά μέσα. Οι επιθέσεις μπορούν να εξαπολυθούν από οποιοδήποτε σημείο του κόσμου, χωρίς την ανάγκη φυσικής παρουσίας, ενώ τα εθνικά σύνορα χάνουν την επιχειρησιακή τους σημασίας. Εξίσου σημαντικό χαρακτηριστικό αποτελεί η δυσκολία απόδοσης ευθύνης (attribution), που περιπλέκει τη στρατηγική απόκριση.

Οι κυβερνοεπιχειρήσεις στοχεύουν σε πολλαπλά επίπεδα. Καταρχάς, επικεντρώνονται στην πληροφόρηση (παραπλάνηση, αλλοίωση ή κλοπή δεδομένων), επηρεάζοντας τη λήψη αποφάσεων και τη στρατηγική εικόνα του αντιπάλου. Παράλληλα, πλήττουν τις υποδομές (διακοπή λειτουργίας κρίσιμων συστημάτων C2, GPS, SATCOM). Τέλος, επιδρούν στην επιχειρησιακή ετοιμότητα (καθυστέρηση, αποδιοργάνωση, ψυχολογικός αντίκτυπος) [185].

Η ανάπτυξη εξειδικευμένων στρατιωτικών δομών στον κυβερνοχώρο από ΗΠΑ, Ρωσία, Κίνα, ΝΑΤΟ και άλλους διεθνείς παίκτες καταδεικνύει ότι ο κυβερνοπόλεμος δεν είναι πλέον αποκλειστικό πεδίο δράσης «χακερικών ομάδων», αλλά οργανωμένο εργαλείο κρατικής ισχύος και κεντρικό στοιχείο της στρατηγικής ασφάλειας [186].

5.3.1 Μορφές επιθετικών κυβερνοεπιχειρήσεων

Η ποικιλία των τεχνικών επιθέσεων στον κυβερνοχώρο είναι μεγάλη — ακολουθεί πλήρης ανάλυση των σημαντικότερων μορφών που χρησιμοποιούνται σε στρατιωτικά/παραστρατιωτικά σενάρια και πώς αυτές σχετίζονται με τα θέματα jamming, spoofing, IoMT.

- DDoS(Distributed Denial of Service)

Οι επιθέσεις τύπου DDoS αποσκοπούν στη μείωση ή στον πλήρη αποκλεισμό της διαθεσιμότητας μίας υπηρεσίας με την πλημμύρα του στόχου από μεγάλο όγκο αιτήσεων ή με την εξάντληση κρίσιμων πόρων (π.χ. εύρος ζώνης, CPU, πίνακες συνδέσεων). Τεχνικά, οι επιθέσεις αυτές μπορεί να υλοποιούνται σε επίπεδο δικτύου (TCP/UDP floods), σε επίπεδο εφαρμογής (HTTP floods) ή με υβριδικούς συνδυασμούς και συχνά αξιοποιούν botnets — δηλαδή δίκτυα μολυσμένων συσκευών — για κλιμάκωση. Σε στρατιωτικά περιβάλλοντα, ένα συντονισμένο DDoS εναντίον ενός κέντρου επιχειρήσεων (C2) ή ενός SATCOM gateway μπορεί να αποκόψει προσωρινά την επικοινωνία μεταξύ μονάδων και διοίκησης, προκαλώντας καθυστερήσεις, σύγχυση και αποδιοργάνωση· στο λογικό επίπεδο, το αποτέλεσμα μοιάζει με αυτό του RF jamming αλλά ενεργεί στο IP/λογισμικό στρώμα. Στο IoMT επιπλέον, μολυσμένες ή παραβιασμένες IoMT συσκευές μπορούν να χρησιμοποιηθούν ως “σκλάβοι” ενός botnet, αυξάνοντας την επιφάνεια επίθεσης και δυσχεραίνοντας την ανίχνευση. Δείκτες συμβάντος (IoC- Indicator of Compromise) μπορεί να περιλαμβάνουν αιφνίδια και παρατεταμένα spikes στο εισερχόμενο traffic, ασυνήθιστες θύρες ή πρωτόκολλα, πολλαπλές αιτήσεις από χιλιάδες διευθύνσεις IP και εξάντληση πινάκων συνδέσεων. Η άμυνα βασίζεται σε συνδυασμό τεχνικών: φιλτράρισμα στο δίκτυο/blackholing/scrubbing σε επίπεδο ISP, rate-limiting και web application firewalls για επιθέσεις επιπέδου εφαρμογής, γεωγραφική κατανομή υπηρεσιών και redundancy (load balancing, CDNs- Content Delivery Networks), καθώς και στην ενσωμάτωση Zero Trust πρακτικών ώστε να απαιτείται αυθεντικοποίηση πριν δεχθούν κρίσιμες εντολές. Τέλος, οι προετοιμασμένες διαδικασίες (playbooks) για detection→ mitigation → failover και οι ασκήσεις προσομοίωσης είναι κρίσιμες για γρήγορη ανάκτηση [187].

- APT(Advanced Persistent Threats)

Τα APT χαρακτηρίζονται από μακροχρόνια, στοχευμένη και κρυφή πρόσβαση σε κρίσιμους πόρους με σκοπό τη συλλογή πληροφοριών, την αλλοίωση δεδομένων ή την προπαρασκευή μελλοντικών ενεργειών. Η δομή μίας APT συνήθως περιλαμβάνει πολλά στάδια: στοχευμένες phishing επιθέσεις ή εκμετάλλευση αδυναμιών για αρχική διείσδυση, lateral movement για επέκταση εντός του δικτύου, εγκατάσταση persistence μηχανισμών και τελικά slow exfiltration χρήσιμων δεδομένων. Σε στρατιωτικά/IoMT σενάρια, μία APT που στοχεύει υποδομές ISR ή κόμβους C2 μπορεί να εγκαταστήσει backdoors σε συσκευές τηλεμετρίας και να συλλέξει εικόνες, στίγματα και άλλα ευαίσθητα δεδομένα, ενώ παράλληλα να παραποιεί πληροφορίες που προωθούνται στην αλυσίδα λήψης αποφάσεων,

υποσκάπτοντας την αξιοπιστία της εικόνας πεδίου. Δείκτες μιας APT περιλαμβάνουν μη φυσιολογικές, επαναλαμβανόμενες συνδέσεις σε απομακρυσμένους hosts, αθόρυβες και περιοδικές μεταφορές μικρών πακέτων (slow exfiltration), χρήση εργαλείων τύπου “living-off-the-land” και ασυνήθιστες προγραμματισμένες εργασίες ή μηχανισμοί persistence. Η άμυνα απαιτεί συνεχή παρακολούθηση με SIEM συστήματα και ML-based ανίχνευση ανωμαλιών, τακτικό hardening και patching, διαχείριση προνομιακών λογαριασμών και εφαρμογή RBAC/least-privilege, δικτυακή μικροτμηματοποίηση (microsegmentation) και Zero Trust πολιτικές για περιορισμό lateral movement, καθώς και ομάδες threat-hunting, feeds threat intelligence και συστηματικές red-/blue-team ασκήσεις μαζί με καλά τεκμηριωμένα incident-response playbooks [188].

❖ Zero-day Exploits

Ως zero-day exploit ορίζεται η εκμετάλλευση μίας ευπάθειας για την οποία δεν υπάρχει ακόμη διαθέσιμο patch ή διόρθωση από την κοινότητα. Η χρήση τέτοιων ευπαθειών δίνει στον επιτιθέμενο σημαντικό χρονικό πλεονέκτημα και μπορεί να οδηγήσει σε απομακρυσμένη εκτέλεση κώδικα ή πλήρη διείσδυση στο σύστημα πριν γίνει γνωστό το πρόβλημα. Σε περιβάλλον IoMT, ένα zero-day σε λογισμικό τηλεμετρίας UAV ή σε πρωτόκολλο επικοινωνίας ενός gateway μπορεί να επιτρέψει στον επιτιθέμενο να εγκαταστήσει backdoor και να ελέγχει πλατφόρμες χωρίς να εντοπιστεί. Δείκτες ενός τέτοιου συμβάντος είναι ασυνήθιστες συμπεριφορές χωρίς υπάρχουσα signature, νέα μοτίβα εκμετάλλευσης που δεν ταιριάζουν με γνωστές υπογραφές και ασυνήθιστα crash logs. Η αντιμετώπιση πρέπει να βασίζεται στην αρχή του defense-in-depth: η ύπαρξη πολλαπλών στρωμάτων προστασίας (WAF, IDS/IPS, endpoint protection) μειώνει το τελικό αντίκτυπο, ενώ παράλληλα είναι αναγκαία η ταχεία διαδικασία patch management, σαφής πολιτική vulnerability disclosure, application whitelisting, secure boot και signed firmware για IoMT συσκευές. Επιπλέον τεχνικές όπως Runtime Application Self-Protection(RASP) και behavior-based detection βοηθούν στον εντοπισμό ανεξάρτητα από τις γνωστές υπογραφές [189].

❖ Supply-Chain Attacks

Οι επιθέσεις στην εφοδιαστική αλυσίδα εκμεταλλεύονται την εξάρτηση οργανισμών από τρίτους παρόχους λογισμικού ή υλικού, όπου ένας τροποποιημένος updater, μια βιβλιοθήκη ή ένα firmware με ενσωματωμένο κακόβουλο κώδικα διανέμονται νόμιμα και εγκαθίστανται από τελικούς χρήστες. Τέτοιου είδους επιθέσεις είναι ιδιαιτέρως επικίνδυνες επειδή «εισέρχονται» στο περιβάλλον με φαινομενικά έγκυρο τρόπο και μπορούν να δώσουν οριζόντια πρόσβαση σε μεγάλα σύνολα συσκευών. Στο στρατιωτικό πεδίο, μία trojanized βιβλιοθήκη ή κακόβουλο firmware που διανέμεται σε αισθητήρες ή gateways μπορεί να δημιουργήσει κρυφές πύλες πρόσβασης σε πολλαπλές πλατφόρμες IoMT. Ιστορικά παραδείγματα σε μη-στρατιωτικό επίπεδο (π.χ. SolarWinds) δείχνουν το μέγεθος της απειλής. Δείκτες supply-chain συμβάντων περιλαμβάνουν μη αναμενόμενες αλλαγές σε

υπογεγραμμένα builds, πακέτα με αμφίβολα credentials και την εμφάνιση backdoor επικοινωνιών μετά από επίσημη ενημέρωση. Για την πρόληψη απαιτούνται πρακτικές signed code & strict code-signing verification, ισχυρό supply chain risk management (auditing προμηθευτών, χρήση SBOM — Software Bill of Materials), ανεξάρτητος έλεγχος τρίτων πακέτων, δοκιμές σε απομονωμένα staging περιβάλλοντα πριν το deployment και hardened CI/CD pipelines με integrity checks και provenance tracking [190].

- Social Engineering(Human centric Attacks

Οι επιθέσεις κοινωνικής μηχανικής εκμεταλλεύονται τον ανθρώπινο παράγοντα και περιλαμβάνουν τεχνικές όπως phishing, spear-phishing, vishing, pretexting και baiting, με τελικό στόχο την απόκτηση credentials, την εκτέλεση κακόβουλου λογισμικού ή την πρόκληση ενεργειών που υπονομεύουν συστήματα. Στο στρατιωτικό και IoMT περιβάλλον, το στοχευμένο spear-phishing σε χειριστές ή διοικητές μπορεί να οδηγήσει σε εκτέλεση payload σε κρίσιμες συσκευές, σε αλλαγές ρυθμίσεων gateways ή ακόμη και σε φυσική πρόσβαση (π.χ. με τοποθετημένα USB). Δείκτες τέτοιων επιθέσεων περιλαμβάνουν μη αναμενόμενα emails προς προσωπικό, αιτήματα αλλαγής προνομίων, ή ασυνήθιστες συνδέσεις αμέσως μετά την παραλαβή ύποπτου μηνύματος. Η άμυνα προϋποθέτει συνεχή εκπαίδευση και phishing awareness drills, τεχνολογικούς ελέγχους όπως email filtering και attachment sandboxing, χρήση DMARC/DKIM/SPF για επαλήθευση αποστολέα, εφαρμογή least-privilege και step-up authentication για κρίσιμες ενέργειες, καθώς και αυστηρές πολιτικές ελέγχου συσκευών USB και φυσικής πρόσβασης [191].

- Συνδυασμένες(Hybrid) Επιθέσεις

Στη σύγχρονη επιχειρησιακή πρακτική σπάνια συναντάμε μονολιθικές, απλές επιθέσεις· οι αντίπαλοι προτιμούν πολυδιάστατα σενάρια που συνδυάζουν τεχνικές από διαφορετικά πεδία. Ένας αντίπαλος μπορεί, για παράδειγμα, να συγχρονίσει spoofed GPS σήματα που αποπροσανατολίζουν ένα UAV, με παράλληλη διακοπή C2 σύνδεσης μέσω jamming ή DDoS, ενώ ένα ήδη εγκατεστημένο APT συλλέγει και εξάγει κρίσιμη τηλεμετρία. Το αποτέλεσμα ενός τέτοιου συνδυασμού μπορεί να είναι η απώλεια ελέγχου των πλατφορμών, η κατάληψη ή η καταστροφή τους, αλλά και η συστηματική υπονόμευση της επιχειρησιακής εικόνας. Η αντιμετώπιση απαιτεί ολιστική προσέγγιση: ολοκληρωμένα playbooks που συνδυάζουν EW, cyber και φυσικά μέτρα, cross-domain situational awareness που συνδυάζει RF monitoring, network telemetry και sensor fusion, γρήγορες διαδικασίες isolation & failover, εφεδρικές επικοινωνίες και fallback (π.χ. αδρανειακή πλοήγηση), καθώς και κοινή εκπαίδευση (joint training) μεταξύ cyber, EW και επιχειρησιακών μονάδων για ομαδική αντίδραση και συντονισμό σε επίπεδο διοίκησης [192].

5.3.2 Στρατιωτικές δομές και διεθνής διάσταση

Με την αναγνώριση του κυβερνοχώρου ως κρίσιμου επιχειρησιακού πεδίου, κράτη και διεθνείς οργανισμοί έχουν αναπτύξει μόνιμες δομές για την άμυνα και (σε ορισμένες περιπτώσεις) την επίθεση στον κυβερνοχώρο. Η ύπαρξη τέτοιων δομών αντικατοπτρίζει τη στρατηγική βαρύτητα του cyber: όχι μόνο ως εργαλείο πληροφοριών αλλά και ως όπλο ικανό να επηρεάσει άμεσα την έκβαση επιχειρήσεων.

Ένας από τους σημαντικότερους πυλώνες της στρατιωτικής κυβερνοασφάλειας είναι η ύπαρξη Εθνικών Διοικήσεων Κυβερνοδυνάμεων (National Cyber Commands). Οι διοικήσεις αυτές έχουν ως κύριο ρόλο τον συνολικό συντονισμό της προστασίας κρίσιμων στρατιωτικών δικτύων και, σε ορισμένες περιπτώσεις, και πολιτικών υποδομών. Παράλληλα, είναι επιφορτισμένες με την εκτέλεση αμυντικών επιχειρήσεων, ενώ υπό συγκεκριμένες συνθήκες και πολιτικές εγκρίσεις, αναλαμβάνουν και επιθετικές κυβερνοδράσεις στο πλαίσιο της εθνικής στρατηγικής.Ένα χαρακτηριστικό παράδειγμα αποτελεί η U.S. Cyber Command, η οποία οργανώνει, εκπαιδεύει και διεξάγει επιχειρήσεις για την προστασία αμερικανικών αμυντικών δικτύων και την υποστήριξη ευρύτερων στρατιωτικών επιχειρήσεων. Σημαντικό σημείο προσοχής εδώ είναι ότι οι αρμοδιότητες «άμυνας» και «επίθεσης» διαφέρουν από χώρα σε χώρα, ενώ η διαχείριση αυτών των εξουσιών εμπλέκει ευαίσθητα νομικά και πολιτικά ζητήματα που σχετίζονται με το ποιος δίνει εντολές, ποιος επιβλέπει και ποια είναι τα όρια δράσης [193].

Ένα δεύτερο επίπεδο αφορά τις Ειδικές Μονάδες Στοχευμένης Δράσης ή Κακόβουλης Πληροφορίας, οι οποίες λειτουργούν συνήθως εντός στρατιωτικών μυστικών υπηρεσιών. Οι μονάδες αυτές αναπτύσσουν εξειδικευμένα εργαλεία, τεχνικές και διαδικασίες (TTPs – Tools, Techniques, Procedures) με σκοπό την προσβολή συγκεκριμένων αντιπάλων, την εκμετάλλευση ευπαθειών και την απόκτηση στρατηγικού πλεονεκτήματος στο κυβερνοχώρο. Παραδείγματα που έχουν καταγραφεί διεθνώς περιλαμβάνουν την κινεζική Unit 61398, η οποία αποδίδεται σε εκτεταμένες επιχειρήσεις κυβερνοκατασκοπείας, καθώς και την ρωσική APT28 (Fancy Bear), η οποία έχει εμπλακεί σε κυβερνοεπιθέσεις εναντίον Νατοϊκών δικτύων, στρατιωτικών ασκήσεων και πολιτικών κομμάτων [194].

Εξίσου κρίσιμο ρόλο διαδραματίζουν τα Κέντρα Συνεργασίας και Έρευνας, όπως το NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) και ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA). Τα κέντρα αυτά οργανώνουν κοινές ασκήσεις, αναπτύσσουν πρότυπα ασφαλείας, παράγουν μελέτες και προωθούν τη συνεργασία μεταξύ των κρατών-μελών. Παράλληλα, λειτουργούν ως κόμβοι ανταλλαγής βέλτιστων πρακτικών και εκπαίδευσης, ενισχύοντας την ετοιμότητα απέναντι σε επιθέσεις μεγάλης κλίμακας. Ωστόσο, η αποτελεσματικότητά τους εξαρτάται σε μεγάλο βαθμό από τον βαθμό διαλειτουργικότητας και την εμπιστοσύνη που αναπτύσσεται μεταξύ των συμμάχων, καθώς η ανταλλαγή ευαίσθητων πληροφοριών απαιτεί αυστηρούς μηχανισμούς ελέγχου πρόσβασης και σαφές νομικό πλαίσιο [195].

Τέλος, σημαντική διάσταση έχουν τα Διακλαδικά Cyber Centres και οι Συνεργασίες με τη Βιομηχανία. Τα κέντρα αυτά λειτουργούν ως δίαυλοι επικοινωνίας και συνεργασίας ανάμεσα σε στρατιωτικές δομές και την ιδιωτική βιομηχανία, με στόχο την ενίσχυση της ανθεκτικότητας κρίσιμων υποδομών και την ανάπτυξη ασφαλών λύσεων σε τομείς όπως οι δορυφορικές επικοινωνίες (SATCOM) και τα UAVs. Μέσα από τέτοιες συνεργασίες, ενισχύεται η ασφάλεια της εφοδιαστικής αλυσίδας, ενώ παράλληλα αξιοποιείται η τεχνογνωσία και η καινοτομία του ιδιωτικού τομέα. Η στενή αυτή σχέση κράτους-βιομηχανίας είναι απαραίτητη, καθώς πολλές από τις κρίσιμες υποδομές ανήκουν ή διαχειρίζονται από ιδιωτικούς φορείς, γεγονός που καθιστά τη συνεργασία μονόδρομο για τη συνολική κυβερνοάμυνα.

5.3.3 Διεθνής διάσταση, κανόνες και νομιμότητα

Η διεθνής διάσταση των κυβερνοεπιχειρήσεων συνδέεται άμεσα με ζητήματα νομιμότητας και με την εφαρμογή κανόνων που δεν είναι πάντοτε σαφείς. Ένα από τα πιο κρίσιμα ζητήματα είναι το attribution, δηλαδή η αξιόπιστη απόδοση ευθύνης για μια κυβερνοεπίθεση. Η διαδικασία αυτή δεν είναι μόνο τεχνικά περίπλοκη, καθώς απαιτεί συνδυασμό ψηφιακών ιχνών, γεωπολιτικών ενδείξεων και μυστικών πληροφοριών, αλλά και πολιτικά φορτισμένη [184]. Η έλλειψη σαφούς και κοινά αποδεκτού μηχανισμού απόδοσης ευθύνης καθιστά δύσκολη τη λήψη αποφάσεων για αντίποινα ή ακόμη και για νόμιμη άμυνα, καθώς η οποιαδήποτε ενέργεια μπορεί να αμφισβητηθεί στο διεθνές δίκαιο.

Παράλληλα, έχουν γίνει σημαντικές προσπάθειες για την ανάπτυξη διεθνών κανόνων και κανονιστικών πλαισίων στον κυβερνοχώρο. Οργανισμοί όπως τα Ηνωμένα Έθνη (UN Groups of Governmental Experts) και το ΝΑΤΟ έχουν επιχειρήσει να θεσπίσουν κανόνες συμπεριφοράς και δεσμεύσεις που θα περιορίσουν τις ανεξέλεγκτες ενέργειες στον κυβερνοπόλεμο [185]. Ωστόσο, η εφαρμογή αυτών των κανόνων είναι άνιση και εξαρτάται από το επίπεδο συνεργασίας και εμπιστοσύνης μεταξύ κρατών. Οι αποκλίνουσες ερμηνείες για το τι συνιστά «χρήση βίας» στον κυβερνοχώρο καθιστούν δυσχερή την ενοποίηση ενός δεσμευτικού πλαισίου.

Ένα τρίτο σημαντικό στοιχείο αφορά τη νομική κάλυψη των ενεργειών σε εθνικό και διεθνές επίπεδο. Οι κυβερνοεπιχειρήσεις μπορεί να καταταχθούν είτε ως επιθετικές πράξεις που εμπίπτουν στο Διεθνές Δίκαιο της Ένοπλης Σύγκρουσης (Law of Armed Conflict - LOAC), είτε ως ενέργειες χαμηλότερης έντασης, οι οποίες συχνά αντιμετωπίζονται ως εγκληματικές ή ως κατασκοπεία Η διάκριση αυτή έχει άμεσες συνέπειες στις επιλογές αποτροπής και απόκρισης ενός κράτους. Επιπλέον, κάθε χώρα εφαρμόζει το δικό της πλαίσιο εσωτερικού δικαίου για τη ρύθμιση κυβερνοεπιχειρήσεων, το οποίο μπορεί να επιβάλλει διαφορετικά όρια ή διαδικασίες σε σχέση με τη διεθνή πρακτική.

Συνολικά, η διεθνής διάσταση του κυβερνοπολέμου φανερώνει ένα πεδίο που χαρακτηρίζεται από ρευστότητα και αντιφάσεις. Η απουσία κοινά αποδεκτών κανόνων, η δυσκολία απόδοσης ευθύνης

και οι διαφορές μεταξύ εθνικών και διεθνών νομικών πλαισίων καθιστούν τον κυβερνοχώρο πεδίο έντονης αβεβαιότητας, όπου η πολιτική και η στρατηγική υπερισχύουν συχνά της νομικής σαφήνειας.

Σημαντικά ζητήματα οργάνωσης και επιχειρησιακής λειτουργίας :

Η οργάνωση και λειτουργία των κυβερνοδυνάμεων δεν περιορίζεται σε τεχνικό επίπεδο, αλλά περιλαμβάνει κρίσιμες θεσμικές και πολιτικές πτυχές. Ένα βασικό ζήτημα είναι τα κέντρα λήψης αποφάσεων και ο πολιτικός έλεγχος. Οι ενέργειες στον κυβερνοχώρο συχνά έχουν διεθνείς προεκτάσεις και μπορούν να προκαλέσουν σοβαρές διπλωματικές ή στρατιωτικές συνέπειες. Για τον λόγο αυτό, απαιτείται σαφής κατανομή ευθυνών και ιεραρχία εντολών (chain-of-command), καθώς και η ύπαρξη μηχανισμών νομικού και ηθικού ελέγχου [196]. Η διαφάνεια και η πολιτική εποπτεία είναι αναγκαίες προϋποθέσεις για να διασφαλίζεται ότι οι επιθετικές ή αμυντικές κυβερνοενέργειες κινούνται εντός του πλαισίου του διεθνούς δικαίου και των εθνικών πολιτικών.

Εξίσου σημαντική είναι η διαλειτουργικότητα (interoperability) και η ανταλλαγή πληροφοριών (information sharing). Σε περιβάλλοντα συλλογικής άμυνας, όπως το NATO, είναι απαραίτητο οι τεχνικές λύσεις, τα δόγματα και οι διαδικασίες των κρατών-μελών να είναι συμβατές, ώστε να μπορούν να διεξάγονται συντονισμένες επιχειρήσεις στον κυβερνοχώρο. Οι συμφωνίες αμοιβαίας συνδρομής (mutual assistance agreements) και η γρήγορη ανταλλαγή πληροφοριών για κυβερνοαπειλές αποτελούν κρίσιμους παράγοντες για την έγκαιρη ανίχνευση και απόκρουση επιθέσεων μεγάλης κλίμακας [197].

Παράλληλα, η ενίσχυση δυνατοτήτων (capacity building) αποτελεί καθοριστικό πεδίο, ιδιαίτερα για τα μικρότερα κράτη που συχνά δεν διαθέτουν τους πόρους ή το εξειδικευμένο προσωπικό για να προστατεύσουν τις κρίσιμες υποδομές τους. Μέσα από εκπαιδεύσεις, κοινές ασκήσεις και τεχνική βοήθεια, τα κράτη με μεγαλύτερη εμπειρία συμβάλλουν στη δημιουργία ενός πιο ανθεκτικού διεθνούς περιβάλλοντος, περιορίζοντας τις αδυναμίες που θα μπορούσαν να εκμεταλλευτούν αντίπαλοι.

Επιπτώσεις στην τακτική και στρατηγική επιχειρησιακή σχεδίαση

Η ύπαρξη ειδικών cyber commands μετασχηματίζει την επιχειρησιακή αρχιτεκτονική των σύγχρονων στρατών. Οι επιχειρήσεις πλέον σχεδιάζονται με το κυβερνοχώρο ως οργανικό και αναπόσπαστο κομμάτι (network-enabled operations), αντί να αντιμετωπίζεται ως δευτερεύουσα διάσταση. Αυτό σημαίνει ότι από τα πρώτα στάδια σχεδιασμού, η προστασία και η εκμετάλλευση του κυβερνοχώρου αποτελούν παράγοντες εξίσου σημαντικούς με τις χερσαίες, θαλάσσιες ή αεροπορικές επιχειρήσεις.

Σε επίπεδο επιμέρους αποστολών, κρίσιμες λειτουργίες όπως η ISR, τα δίκτυα C2 και τα logistics οφείλουν να διαθέτουν ενσωματωμένα σχέδια απομόνωσης, εναλλακτικές υποδομές (failover systems)

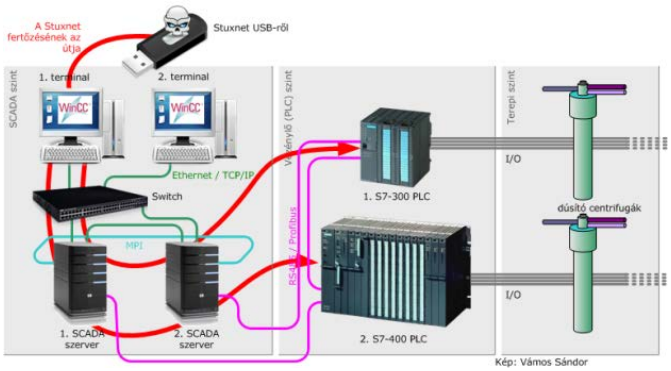
και δυνατότητες λειτουργίας ακόμη και υπό έντονες ψηφιακές επιθέσεις. Η ανθεκτικότητα των συστημάτων αυτών καθορίζει άμεσα την επιχειρησιακή συνέχεια και την επιτυχία της αποστολής.

Τέλος, δεν πρέπει να παραβλέπεται η ψυχολογική διάσταση των κυβερνοεπιθέσεων. Ο δημόσιος χαρακτήρας πολλών επιθέσεων, η πιθανότητα δυσφήμισης κρατικών δομών ή η υπονόμευση της εμπιστοσύνης των πολιτών και των ενόπλων δυνάμεων στις ίδιες τους τις υποδομές, αποτελούν ένα ακόμη εργαλείο πίεσης. Ο αντίπαλος μπορεί να επιδιώξει όχι μόνο την τεχνική καταστροφή ή αποδιοργάνωση, αλλά και την πρόκληση ανασφάλειας, αμφιβολίας και πολιτικού κόστους [198].

5.3.4 Παραδείγματα επιθετικών επιχειρήσεων

Stuxnet(2009-2010)

Το Stuxnet αποτελεί ίσως το πιο διάσημο κυβερνοόπλο που ανακαλύφθηκε μέχρι σήμερα. Ήταν ένα προηγμένο, στοχευμένο worm που σχεδιάστηκε για να εκμεταλλευτεί ευπάθειες σε Windows συστήματα και να εισάγει εντολές σε PLCs (Programmable Logic Controllers) που έλεγχαν συστήματα SCADA σε ιρανικές εγκαταστάσεις εμπλουτισμού ουρανίου. Η πολυπλοκότητά του ήταν πρωτοφανής: χρησιμοποίησε πολλαπλά zero-day exploits, κλεμμένες ψηφιακές υπογραφές και ένα payload που τροποποιούσε τις συχνότητες περιστροφής φυγοκεντρητών. Σε επιχειρησιακό επίπεδο, προκάλεσε μετρήσιμες φθορές σε κρίσιμες εγκαταστάσεις και ανέδειξε πώς ο κυβερνοπόλεμος μπορεί να έχει απτές φυσικές συνέπειες. Το βασικό μάθημα ήταν η ανάγκη για πλήρη απομόνωση (segmentation) μεταξύ IT και OT, αυστηρές διαδικασίες update και χρήση υπογεγραμμένου firmware.



Σχήμα 45- Αναπαράσταση της λειτουργίας του Stuxnet : μόλυνση μέσω USB [199]

Viasat (Φεβρουάριος 2022)

Λίγες ώρες πριν από την εισβολή της Ρωσίας στην Ουκρανία, σημειώθηκε μαζική διακοπή δορυφορικών επικοινωνιών που αποδόθηκε σε επίθεση κατά του παρόχου Viasat. Το περιστατικό προκάλεσε απώλεια λειτουργικότητας σε χιλιάδες modems και edge devices, οδηγώντας σε εκτεταμένη απώλεια συνδεσιμότητας σε στρατιωτικές και πολιτικές υποδομές σε όλη την Ευρώπη. Παράλληλα, αναφέρθηκαν παρεμβολές σε δορυφορική πλοήγηση, γεγονός που επιδείνωσε τις επιχειρησιακές συνέπειες. Η επίθεση αυτή υπογράμμισε την εξάρτηση των δυνάμεων από εμπορικούς

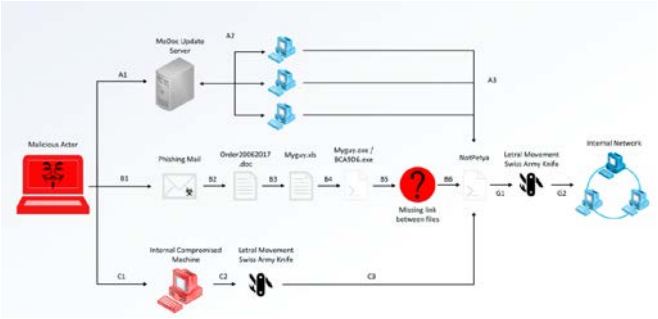
παρόχους SATCOM και την ανάγκη για redundancy, ασφαλείς διαδικασίες provisioning και δυνατότητες offline failover.

SolarWinds/SUNBURST (2020-2021)

Η επίθεση κατά της SolarWinds αποτελεί χαρακτηριστικό παράδειγμα supply chain compromise. Μέσω παραποίησης ενός επίσημου update της πλατφόρμας Orion, οι επιτιθέμενοι εισήγαγαν το backdoor SUNBURST, αποκτώντας πρόσβαση σε εκατοντάδες οργανισμούς διεθνώς, περιλαμβανομένων κυβερνητικών υπηρεσιών και κρίσιμων υποδομών. Η stealth φύση της επίθεσης, με έμφαση σε lateral movement και μακροχρόνια παραμονή, απέδειξε πόσο ευάλωτες μπορεί να είναι ακόμα και οι πιο «εμπιστευμένες» αλυσίδες λογισμικού. Τα μαθήματα περιλαμβάνουν την ανάγκη για SBOM (Software Bill of Materials), αυστηρό auditing προμηθευτών, sandbox testing updates και εφαρμογή αυστηρής πολιτικής code-signing [190].

NotPetya (Ιούνιος 2017)

Η επίθεση NotPetya ξεκίνησε ως ransomware αλλά σύντομα αναγνωρίστηκε ως wiper με στόχο την καταστροφή. Χρησιμοποίησε exploits όπως το EternalBlue και μηχανισμούς lateral movement για να εξαπλωθεί ταχύτατα. Οι συνέπειες ήταν καταστροφικές: εταιρείες logistics, χρηματοπιστωτικά ιδρύματα και κρατικοί οργανισμοί υπέστησαν τεράστιες οικονομικές απώλειες. Η επίθεση απέδειξε ότι ο κυβερνοπόλεμος μπορεί να προκαλέσει παγκόσμιο οικονομικό αντίκτυπο, ακόμα και αν ο στόχος είναι τοπικός. Τα μαθήματα περιλαμβάνουν γρήγορο patching, δικτυακό segmentation, offline backups και προετοιμασμένα σχέδια αποκατάστασης.



Σχήμα 46- Διαδρομή μόλυνσης από την επίθεση [200]

RQ-170 Sentinel (2011)

Ένα διαφορετικό περιστατικό αφορά την πτώση ενός αμερικανικού UAV RQ-170 Sentinel στο Ιράν. Σύμφωνα με ισχυρισμούς της ιρανικής πλευράς, η κατάληψή του επιτεύχθηκε μέσω spoofing σημάτων GPS και παρεμβολών στο C2 link, με αποτέλεσμα το UAV να χάσει τον έλεγχο και να προσγειωθεί. Αν και οι λεπτομέρειες παραμένουν ασαφείς, το περιστατικό ανέδειξε την απειλή υβριδικών επιθέσεων που συνδυάζουν spoofing, jamming και cyber ενέργειες. Το βασικό μάθημα ήταν

η ανάγκη για multi-sensor fusion (INS + GPS + vision), χρήση authenticated GNSS (M-code) και ενίσχυση της ασφάλειας των C2 links.



Σχήμα 47- Το UAV-RQ-170 Sentinel [201]

Οπτική Αναπαράσταση

Η χρήση του κυβερνοχώρου ως πεδίου στρατηγικών επιχειρήσεων δεν περιορίζεται πλέον σε μεμονωμένα περιστατικά, αλλά εξελίσσεται σε καθημερινό φαινόμενο με παγκόσμια διάσταση. Οι κυβερνοεπιθέσεις πραγματοποιούνται σε πραγματικό χρόνο, στοχεύοντας κρίσιμες υποδομές, δίκτυα και στρατιωτικές μονάδες, με αποτέλεσμα η ένταση και η συχνότητά τους να αποτελούν πλέον βασικό δείκτη της διεθνούς ασφάλειας.

Η Check Point ThreatCloud Live Cyber Threat Map παρουσιάζει σε πραγματικό χρόνο την προέλευση και τους στόχους ενεργών επιθέσεων ανά τον κόσμο. Στην απεικόνιση που ακολουθεί Σχήμα 48, καταγράφονται επιθέσεις με προορισμό την Ελλάδα, γεγονός που υπογραμμίζει ότι οι απειλές στον κυβερνοχώρο δεν περιορίζονται σε χώρες με υψηλό τεχνολογικό προφίλ, αλλά επηρεάζουν εξίσου μικρότερα κράτη και περιφερειακές δυνάμεις.



Σχήμα 48- Live Cyber Threat Map : Διεθνής ροή επιθέσεων

Η οπτική αυτή αναπαράσταση αποδεικνύει ότι ο κυβερνοπόλεμος αποτελεί διαρκές και ορατό φαινόμενο. Οι απειλές δεν κάνουν διακρίσεις μεταξύ μεγάλων ή μικρών κρατών, γεγονός που

αναδεικνύει την ανάγκη για συνεχή ενίσχυση της άμυνας, της παρακολούθησης και της διεθνούς συνεργασίας απέναντι στις ψηφιακές συγκρούσεις.

5.3.5 Στρατηγικές άμυνας

Η προστασία από επιθετικές ενέργειες στον κυβερνοχώρο δεν μπορεί να περιοριστεί σε ένα μόνο μέτρο. Οι απειλές είναι πολυδιάστατες και εξελίσσονται διαρκώς, άρα απαιτείται ολιστική στρατηγική, που συνδυάζει τεχνικούς μηχανισμούς, οργανωτικές διαδικασίες, διεθνή συνεργασία και συνεχή εκπαίδευση.

Μια από τις πιο θεμελιώδεις στρατηγικές είναι η αρχιτεκτονική μηδενικής εμπιστοσύνης(Zero Trust Architrcture-ZTA) Σε αντίθεση με παραδοσιακά μοντέλα που θεωρούν έμπιστους τους χρήστες ή τις συσκευές εντός του δικτύου, η ZTA αντιμετωπίζει κάθε αίτημα πρόσβασης ως δυνητικά κακόβουλο. Αυτό σημαίνει ότι απαιτείται αυστηρή αυθεντικοποίηση (π.χ. multi-factor authentication, ψηφιακά πιστοποιητικά) και δυναμική αξιολόγηση κινδύνου σε πραγματικό χρόνο, με βάση παράγοντες όπως η γεωγραφική θέση του χρήστη ή η συμπεριφορά της συσκευής. Με αυτόν τον τρόπο, ακόμη και αν ένας αντίπαλος αποκτήσει νόμιμα credentials, η πρόσβασή του μπορεί να περιοριστεί ή να μπλοκαριστεί έγκαιρα.

Συμπληρωματικά, κρίσιμο ρόλο διαδραματίζουν τα συστήματα SIEM(Security information and event management), τα οποία συγκεντρώνουν και συσχετίζουν logs από πολλαπλές πηγές – δίκτυα, endpoints, servers, IoMT συσκευές – σε μια κεντρική πλατφόρμα. Χρησιμοποιώντας προηγμένους αλγορίθμους και τεχνικές ανάλυσης, τα SIEM μπορούν να ανιχνεύσουν ανωμαλίες που δεν θα γίνονταν αντιληπτές σε τοπικό επίπεδο [200]. Για παράδειγμα, μια σειρά από αποτυχημένες συνδέσεις σε διαφορετικά σημεία του δικτύου μπορεί να ενοποιηθεί ως «μοτίβο» brute force επίθεσης. Σε στρατιωτικά περιβάλλοντα, τα SIEM προσφέρουν κρίσιμο πλεονέκτημα: ορατότητα σε πραγματικό χρόνο για όλο το φάσμα των δικτύων, από τα logistics έως τα C2 συστήματα.

Παράλληλα, τα συστήματα IDS/IPS(Intrusion detection/Prevention systems) αποτελούν βασικά εργαλεία για τον εντοπισμό και την αποτροπή εισβολών. Τα IDS λειτουργούν σαν «συναγερμοί», εντοπίζοντας ύποπτη δραστηριότητα μέσω signatures γνωστών απειλών ή με ανάλυση ανωμαλιών. Τα IPS πηγαίνουν ένα βήμα παραπέρα, αποκλείοντας αυτόματα την κακόβουλη δραστηριότητα σε πραγματικό χρόνο. Έτσι, μια προσπάθεια SQL injection, ένα exploit ή μια απόπειρα μη εξουσιοδοτημένης πρόσβασης μπορεί να μπλοκαριστεί πριν εξαπλωθεί. Στο πλαίσιο του IoMT, τα IDS/IPS είναι κρίσιμα, καθώς οι διασυνδεδεμένοι κόμβοι (UAVs, φορητοί αισθητήρες, κινητές μονάδες) αποτελούν ελκυστικούς στόχους για επιτιθέμενους.

Στην κορυφή αυτή της στρατηγικής βρίσκεται η αρχή της άμυνας σε βάθος (defense in depth). Η φιλοσοφία αυτή βασίζεται στην παραδοχή ότι καμία μεμονωμένη λύση δεν μπορεί να προσφέρει πλήρη προστασία. Έτσι, εφαρμόζεται ένας συνδυασμός από πολλαπλά επίπεδα ασφαλείας, όπως

firewalls, antivirus, μηχανισμοί anomaly detection, microsegmentation και redundancy. Αν, για παράδειγμα, μια επίθεση καταφέρει να διαπεράσει το firewall, μπορεί να εντοπιστεί από το IDS, ενώ αν καταφέρει να παρακάμψει και αυτό, η αρχιτεκτονική microsegmentation θα περιορίσει την εξάπλωση της στο δίκτυο. Με τον τρόπο αυτό, ακόμα και αν παραβιαστεί ένα επίπεδο, τα υπόλοιπα θα συνεχίσουν να προστατεύουν τις κρίσιμες λειτουργίες.

Η εφαρμογή όλων αυτών των μέτρων μαζί συνθέτει ένα πολυεπίπεδο τείχος προστασίας, που καθιστά τις στρατιωτικές δομές πολύ πιο ανθεκτικές απέναντι στις πολυδιάστατες επιθέσεις του σύγχρονου κυβερνοχώρου.

Εκπαίδευση προσωπικού(Human factor defence)

Ο ανθρώπινος παράγοντας εξακολουθεί να θεωρείται ο πιο ευάλωτος κρίκος στην αλυσίδα ασφαλείας. Ακόμη και τα πιο εξελιγμένα τεχνικά συστήματα μπορούν να καταρρεύσουν εάν ένα μέλος του προσωπικού παραπλανηθεί μέσω phishing ή χειριστεί λανθασμένα κρίσιμο εξοπλισμό. Για τον λόγο αυτό, η εκπαίδευση αποτελεί θεμέλιο της κυβερνοάμυνας. Η χρήση phishing simulations επιτρέπει στο προσωπικό να εξοικειωθεί με τα χαρακτηριστικά των κακόβουλων e-mails και να αναπτύξει την απαιτούμενη εγρήγορση. Παράλληλα, η συνεχής security awareness training παρέχει ενημέρωση για νέες τεχνικές social engineering, όπως spear-phishing, pretexting ή vishing, και βοηθά στον εντοπισμό των «κόκκινων σημείων». Επιπλέον, η διαχείριση κρίσεων με σαφή playbooks (incident response plans) είναι απαραίτητη: κάθε στρατιώτης, χειριστής ή αναλυτής πρέπει να γνωρίζει βήμα-βήμα πώς να αντιδράσει σε περίπτωση κυβερνοεπίθεσης, ώστε να αποφευχθεί η πανικόβλητη αντίδραση που μπορεί να οδηγήσει σε κλιμάκωση των επιπτώσεων.

Ασκήσεις κυβερνοπολέμου(Cyber warfare exercises)

Η θεωρητική γνώση, όσο σημαντική κι αν είναι, δεν αρκεί για να εξασφαλίσει επιχειρησιακή ετοιμότητα. Οι ασκήσεις κυβερνοπολέμου αποτελούν το πιο αποτελεσματικό εργαλείο για την αποκάλυψη τρωτών σημείων και τη δοκιμή της ανταπόκρισης σε πραγματικές συνθήκες. Οι tabletop exercises, με συμμετοχή επιτελών, βοηθούν στην εξάσκηση διαδικασιών λήψης αποφάσεων σε σενάρια κρίσης. Παράλληλα, τα Red team vs Blue team drills φέρνουν αντιμέτωπες ομάδες επίθεσης και άμυνας, αναδεικνύοντας τις πραγματικές δυνατότητες ανίχνευσης και απόκρισης των δικτύων. Τέλος, οι combined cyber–EW exercises συνδυάζουν κυβερνοεπιθέσεις με επιχειρήσεις ηλεκτρονικού πολέμου, όπως jamming και spoofing, ώστε να προσομοιώνεται ρεαλιστικά το περιβάλλον μάχης [192]. Μέσα από τέτοιες ασκήσεις οι δυνάμεις αποκτούν την ικανότητα να λειτουργούν υπό καθεστώς έντονης ψηφιακής πίεσης, διατηρώντας την επιχειρησιακή συνέχεια.

5.4 Redundancy και προστασία δεδομένων

5.4.1 Βασικές έννοιες και επιχειρησιακοί στόχοι εφεδρείας και προστασίας δεδομένων

Η εφεδρεία (redundancy) και η προστασία δεδομένων (data protection) αποτελούν τους δύο θεμελιώδεις άξονες για τη διατήρηση της επιχειρησιακής συνέχειας σε στρατιωτικά δίκτυα. Η ύπαρξη σχεδιασμένου πλεονασμού (π.χ. εφεδρικοί κόμβοι, παράλληλες ζεύξεις, αποθηκευτικά συστήματα με replication) εξασφαλίζει ότι η αποτυχία ενός στοιχείου δεν οδηγεί σε κατάρρευση της υπηρεσίας. Αντίστοιχα, η προστασία δεδομένων εγγυάται ότι η πληροφορία διατηρείται εμπιστευτική, ακριβής και διαθέσιμη σε όλα τα στάδια της διακίνησης και αποθήκευσης [201].

Στρατιωτικά τακτικά και στρατηγικά δίκτυα λειτουργούν συχνά σε ακραία περιβάλλοντα DIL (Disconnected –Intermittent– Limited), όπου η συνδεσιμότητα είναι περιορισμένη, οι κόμβοι μεταβάλλονται δυναμικά και οι αντίπαλοι εφαρμόζουν τεχνικές jamming και spoofing για να διακόψουν την επικοινωνία [160], [165]. Σε τέτοιες συνθήκες, οι απαιτήσεις διαθεσιμότητας και ασφάλειας αποκτούν στρατηγικό χαρακτήρα.

Οι βασικές λειτουργικές απαιτήσεις που πρέπει να καλύπτουν τα στρατιωτικά δίκτυα είναι:

- **Διαθεσιμότητα (Availability):** συνεχής παροχή υπηρεσιών C2/C3/C5ISR, ακόμα και σε περίπτωση καταστροφής μέρους της υποδομής. Αυτό συνεπάγεται πολλαπλές εναλλακτικές διαδρομές, δυναμικό routing, καθώς και γεωγραφικά διασκορπισμένα data centers.
- **Ακεραιότητα (Integrity):** διασφάλιση ότι τα δεδομένα δεν αλλοιώνονται ούτε κατά τη μετάδοση ούτε κατά την αποθήκευση. Η χρήση immutable snapshots, hash-based verification και forensic auditing επιτρέπει την ανίχνευση κάθε παραποίησης.
- **Εμπιστευτικότητα (Confidentiality):** προστασία δεδομένων μέσω end-to-end κρυπτογράφησης (π.χ. HAIPE, IPsec, AES-256) και έλεγχος πρόσβασης βάσει ρόλων (RBAC) ή γνωρισμάτων (ABAC) [123], [131].
- **Ανθεκτικότητα (Resilience):** δυνατότητα λειτουργίας σε degraded mode, με fallback σε εφεδρικά πρωτόκολλα ή χαμηλότερο εύρος ζώνης, διασφαλίζοντας τη συνέχιση κρίσιμων επικοινωνιών.
- **Διαλειτουργικότητα (Interoperability):** συμμόρφωση με διεθνείς τυποποιήσεις (STANAGs, NIST, DoD guidelines), ώστε οι πολυεθνικές δυνάμεις να συνεργάζονται χωρίς κενά ασφαλείας [181].

Για να είναι μετρήσιμη η ανθεκτικότητα ενός δικτύου, καθορίζονται συγκεκριμένοι λειτουργικοί δείκτες. Ο δείκτης RTO (Recovery Time Objective) προσδιορίζει το μέγιστο χρόνο αποκατάστασης υπηρεσίας. Σε εφαρμογές ISR, το RTO πρέπει να είναι μερικά δευτερόλεπτα, καθώς κάθε καθυστέρηση μειώνει την επιχειρησιακή επίγνωση. Αντίστοιχα, ο δείκτης RPO (Recovery Point Objective) ορίζει το μέγιστο χρονικό διάστημα απώλειας δεδομένων που είναι αποδεκτό. Για real-time feeds (π.χ.

δορυφορικές εικόνες ή βίντεο UAVs), το RPO τείνει στο μηδέν, ενώ για λιγότερο κρίσιμα δεδομένα (π.χ. αρχειοθετημένες αναφορές) μπορεί να είναι μεγαλύτερο.

Σημαντικό ρόλο έχουν και οι δείκτες MTTR (Mean Time To Recover) όπου μετρά τον μέσο χρόνο επαναφοράς μετά από αστοχία. Όσο χαμηλότερος ο MTTR, τόσο πιο αποτελεσματικό το redundancy design και ο MTBF (Mean Time Between Failures) όπου δείχνει τον μέσο χρόνο μεταξύ αστοχιών. Η αύξηση του MTBF αποτελεί δείκτη υψηλής αξιοπιστίας του συστήματος [202].

Η εφαρμογή αυτών των αρχών οδηγεί στην επιλογή διαφορετικών επιπέδων εφεδρείας και μηχανισμών προστασίας, ανάλογα με την κατηγορία πληροφορίας.Για κρίσιμα επιχειρησιακά δεδομένα (π.χ. ISR βίντεο, C2 εντολές) απαιτείται synchronous replication κοντά στον χρήστη και real-time failover. Αντίθετα για δεδομένα στρατηγικού χαρακτήρα (π.χ. βάσεις δεδομένων logistics) μπορεί να αρκεί asynchronous replication με μεγαλύτερο RPO. Τέλος, για την προστασία έναντι advanced cyberattacks χρησιμοποιούνται air-gapped αντίγραφα και immutable backups, ώστε να διατηρείται ένα ασφαλές «καταφύγιο δεδομένων» [204].

Με αυτόν τον τρόπο, η αρχιτεκτονική redundancy & data protection δεν αποτελεί απλώς τεχνική προσθήκη, αλλά βασικό εργαλείο στρατηγικής υπεροχής, εξασφαλίζοντας ότι η ροή πληροφορίας θα συνεχιστεί απρόσκοπτα ακόμα και σε συνθήκες έντονου κυβερνοπολέμου ή φυσικής καταστροφής [192].

5.4.2 Redundancy :Εφεδρικές αρχιτεκτονικές και διαθεσιμότητα

Η έννοια της εφεδρείας (redundancy) αποτελεί θεμελιώδη παράγοντα στη σχεδίαση στρατιωτικών τηλεπικοινωνιακών δικτύων. Στόχος είναι η επιχειρησιακή συνέχεια, ακόμη και όταν τμήματα του συστήματος πλήττονται από τεχνικές βλάβες, φυσικές καταστροφές ή εχθρικές ενέργειες [157], [163]. Η ύπαρξη πλεονασμού —σε εξοπλισμό, διαδρομές, ζεύξεις ή data centers— εξαλείφει το «single point of failure» και διασφαλίζει ότι οι κρίσιμες υπηρεσίες παραμένουν λειτουργικές.

Επίπεδα υλοποίησης εφεδρείας :

1. Hardware Redundancy

Η εφεδρεία σε επίπεδο υλικού αποτελεί τη βάση κάθε ανθεκτικής υποδομής. Κρίσιμοι κόμβοι, όπως servers, routers, switches και αισθητήρες, υλοποιούνται σε διπλά αντίγραφα, τα οποία βρίσκονται σε κατάσταση clustering ή hot-standby. Έτσι, όταν παρουσιαστεί αστοχία στο κύριο σύστημα, η εναλλακτική μονάδα ενεργοποιείται αυτόματα, χωρίς να διακοπεί η παροχή υπηρεσιών [157]. Σε στρατιωτικά δίκτυα, όπως αυτά του NATO C3, κάθε κόμβος προστατεύεται από εφεδρικό εξοπλισμό ώστε να διασφαλίζεται η απρόσκοπτη λειτουργία κρίσιμων υπηρεσιών διοίκησης και ελέγχου (C2).

2. Link-level Redundancy

Η εφεδρεία στο επίπεδο των ζεύξεων αφορά τη χρήση πολλαπλών και εναλλακτικών καναλιών επικοινωνίας. Στρατιωτικά δίκτυα συνδυάζουν δορυφορικές ζεύξεις (SATCOM), γραμμές οπτικής επαφής (LOS) και επίγεια HF/VHF/UHF συστήματα. Με την τεχνολογία Multipath TCP (MPTCP), το δίκτυο μπορεί να αξιοποιήσει ταυτόχρονα πολλαπλές διαδρομές. Αυτό σημαίνει ότι, ακόμη κι αν μια σύνδεση δεχθεί παρεμβολή (jamming), η επικοινωνία συνεχίζεται απρόσκοπτα μέσω εναλλακτικού καναλιού, μειώνοντας δραστικά την πιθανότητα πλήρους απώλειας επικοινωνίας [115], [160].

3. Network Path Redundancy

Σε πιο προχωρημένο επίπεδο, η εφεδρεία εφαρμόζεται στο ίδιο το δίκτυο δεδομένων μέσω εναλλακτικών διαδρομών. Σε mesh ή MANET αρχιτεκτονικές, τα δεδομένα μπορούν να μετακινηθούν από διαφορετικούς κόμβους, χωρίς να εξαρτώνται από έναν συγκεκριμένο. Στο πεδίο μάχης, UAVs χρησιμοποιούνται ως εναέριοι αναμεταδότες, παρέχοντας νέες διαδρομές και εξαλείφοντας τον κίνδυνο «single point of failure» [116], [110]. Αυτή η μορφή redundancy είναι ιδιαίτερα σημαντική σε επιχειρήσεις όπου οι σταθερές υποδομές είναι ευάλωτες σε φυσικές ή κυβερνοεπιθέσεις.

4. Redundant Command Posts (C2/C3 Centers)

Τα κέντρα διοίκησης και ελέγχου αποτελούν τον εγκέφαλο κάθε στρατιωτικής επιχείρησης. Για την προστασία τους, σχεδιάζονται εφεδρικά κέντρα επιχειρήσεων, είτε υπόγεια είτε κινητά, τα οποία μπορούν να ενεργοποιηθούν αμέσως μόλις το κύριο κέντρο πληγεί [109]. Με τη χρήση real-time replication κρίσιμων δεδομένων, τα εφεδρικά C2/C3 είναι σε θέση να συνεχίσουν αδιάλειπτα τη διοίκηση, εξασφαλίζοντας επιχειρησιακή συνέχεια ακόμη και υπό συνθήκες βαριάς προσβολής.

5. Dispersed & Synchronized Data Centers

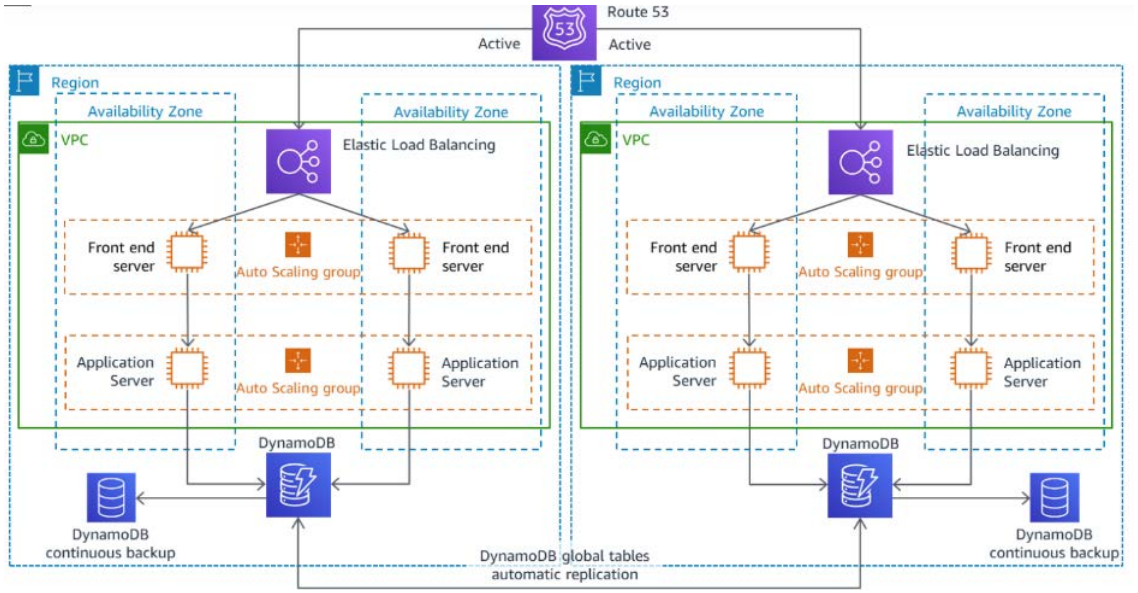
Σε στρατηγικό επίπεδο, η εφεδρεία υλοποιείται με διασπαρμένα data centers, τα οποία λειτουργούν σε active-active διάταξη. Αυτό σημαίνει ότι δύο ή περισσότερα κέντρα δεδομένων λειτουργούν ταυτόχρονα, με real-time synchronization, ώστε η απώλεια ενός από αυτά να μην έχει καμία επίδραση στη συνολική υπηρεσία. Ένα χαρακτηριστικό παράδειγμα είναι οι υποδομές του NATO, όπου κάθε στρατηγικό δίκτυο διαθέτει τουλάχιστον δύο data centers με συνεχή συγχρονισμό. Εκτός από την ανθεκτικότητα, η πρακτική αυτή βελτιώνει και την απόδοση, καθώς τα δεδομένα εξυπηρετούνται από τον κοντινότερο κόμβο.

Η στρατηγική της εφεδρείας συνδέεται άμεσα με την έννοια της διαθεσιμότητας (availability), η οποία εκφράζεται συνήθως με ποσοστά λειτουργίας σε ετήσια βάση. Στον χώρο των τηλεπικοινωνιών, τα «πεντάρια» (π.χ. 99.999%) αντιστοιχούν σε χρόνο εκτός λειτουργίας μόλις λίγων λεπτών ετησίως. Ωστόσο, για στρατιωτικές εφαρμογές οι απαιτήσεις είναι ακόμη αυστηρότερες, καθώς η απώλεια υπηρεσιών, ακόμη και για λίγα δευτερόλεπτα, μπορεί να οδηγήσει σε αποτυχία κρίσιμων επιχειρήσεων ή σε απώλεια ανθρώπινων ζωών.

5.4.3 Στρατηγικές backup & disaster recovery

Η προστασία των δεδομένων και η διατήρηση της επιχειρησιακής συνέχειας στα στρατιωτικά δίκτυα δεν μπορεί να βασίζεται αποκλειστικά σε μηχανισμούς πρόληψης επιθέσεων. Η πραγματικότητα του κυβερνοπολέμου και των φυσικών απειλών (π.χ. καταστροφές, παρεμβολές ηλεκτρονικού πολέμου) επιβάλλει την ανάπτυξη στιβαρών μηχανισμών αποκατάστασης [172], [192]. Οι στρατηγικές backup και disaster recovery (DR) λειτουργούν ως ο δεύτερος πυλώνας άμυνας, εξασφαλίζοντας ότι ακόμη και σε περίπτωση παραβίασης ή καταστροφής, τα κρίσιμα δεδομένα και οι βασικές υπηρεσίες θα μπορούν να αποκατασταθούν γρήγορα, με ελάχιστες απώλειες.

Η αναπαραγωγή δεδομένων (replication) αποτελεί τον ακρογωνιαίο λίθο της επιχειρησιακής συνέχειας σε στρατιωτικά και κρίσιμα πληροφοριακά συστήματα, καθώς εξασφαλίζει τη διατήρηση και τη διαθεσιμότητα των πληροφοριών ακόμη και σε περιπτώσεις αστοχίας ή επίθεσης. Διακρίνεται κυρίως σε συγχρονισμένη (synchronous) και ασύγχρονη (asynchronous) μορφή, ανάλογα με τον τρόπο και τον χρόνο αντιγραφής των δεδομένων.



Σχήμα 49- Διάταξη active

Στη Synchronous replication, τα δεδομένα αντιγράφονται σε πραγματικό χρόνο σε εφεδρικά data centers. Έτσι, το Recovery Point Objective (RPO) προσεγγίζει το μηδέν, κάτι που είναι κρίσιμο για C2/C3 υποδομές υψηλής προτεραιότητας. Μια απώλεια ακόμη και δευτερολέπτων δεδομένων θα μπορούσε να μεταφραστεί σε στρατηγική αστοχία. Ωστόσο, η απαίτηση για υψηλό εύρος ζώνης και χαμηλή καθυστέρηση το καθιστά δύσκολα εφαρμόσιμο σε γεωγραφικά διασκορπισμένα θέατρα επιχειρήσεων [202].

Αντίθετα, στην Asynchronous replication, η μετάδοση των δεδομένων γίνεται περιοδικά, με κάποια χρονική υστέρηση. Ενώ αυξάνει το ρίσκο απώλειας των τελευταίων συναλλαγών, είναι πιο

αποδοτική σε στρατηγικά δίκτυα μεγάλων αποστάσεων (π.χ. NATO inter-theater data centers). Έτσι επιτυγχάνεται ισορροπία μεταξύ κόστους, απόδοσης και αποδοχής κινδύνου [202].

Η στρατηγική απομόνωσης αντιγράφων ασφαλείας (air-gapping) θεωρείται από τις πιο ασφαλείς πρακτικές προστασίας. Τα αντίγραφα ασφαλείας αποθηκεύονται σε συστήματα που δεν διατηρούν μόνιμη σύνδεση με το κύριο δίκτυο, μειώνοντας δραστικά την πιθανότητα εξάπλωσης ransomware ή APTs. Στρατιωτικά, αυτό συχνά εφαρμόζεται με offline αποθήκευση σε υπόγειες εγκαταστάσεις ή ασφαλή vaults, έτοιμα να ενεργοποιηθούν σε περιπτώσεις κρίσης.

Συμπληρωματικά, η χρήση immutable backups και WORM (Write Once, Read Many) τεχνολογιών παρέχει έναν αδιάβλητο μηχανισμό ακεραιότητας. Ακόμη και αν ένας αντίπαλος αποκτήσει πρόσβαση, δεν είναι εφικτή η τροποποίηση ή διαγραφή των δεδομένων. Αυτό είναι κρίσιμο για κρίσιμα logs, όπως τα δεδομένα ISR ή τα C2 communications, που πρέπει να παραμένουν αδιάφθορα για forensic ανάλυση και ιχνηλασιμότητα.

Εξίσου σημαντικός πυλώνας της στρατηγικής ανθεκτικότητας είναι η τακτική επαλήθευση της αποτελεσματικότητας των σχεδίων αποκατάστασης καταστροφών(Disaster Recovery Drills). Η ύπαρξη ενός σχεδίου DR δεν επαρκεί χωρίς τακτική επαλήθευση. Οι ασκήσεις αυτές διακρίνονται σε table-top exercises όπου είναι θεωρητικές ασκήσεις προσομοίωσης κυβερνοεπιθέσεων ή φυσικών καταστροφών, για δοκιμή διαδικασιών και σε full-scale drills όπου γίνεται πλήρης ενεργοποίηση εφεδρικών data centers με στόχο τη μέτρηση πραγματικού RTO και RPO. Στο πλαίσιο του NATO, οργανώνονται επίσης διασυμμαχικές ασκήσεις που ελέγχουν την διαλειτουργικότητα πολυεθνικών δομών και να διασφαλίζεται ότι σε περίπτωση κρίσης οι μηχανισμοί ανάκαμψης θα λειτουργήσουν ομοιόμορφα.

Ο συνδυασμός replication, air-gapping, immutable αποθηκευτικών μέσων και περιοδικών drills δημιουργεί ένα πολυεπίπεδο πλέγμα άμυνας. Με αυτόν τον τρόπο αποφεύγεται η εξάρτηση από ένα μόνο σημείο αποτυχίας και διασφαλίζεται ότι οι στρατιωτικές υποδομές θα παραμείνουν λειτουργικές ακόμη και υπό συνθήκες ολικής προσβολής. Σε ένα περιβάλλον όπου ο χρόνος αντίδρασης και η ακεραιότητα δεδομένων ισοδυναμούν με επιχειρησιακή επιτυχία ή αποτυχία, οι στρατηγικές backup και DR αποκτούν καθοριστική σημασία [202].

5.4.4 Ασφάλεια και προστασία δεδομένων

Η ασφάλεια και η προστασία των δεδομένων σε στρατιωτικά περιβάλλοντα αποτελούν θεμελιώδη παράγοντα επιχειρησιακής ανθεκτικότητας, καθώς συνδέονται με την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας (Confidentiality – Integrity – Availability, CIA). Σε αντίθεση με τα εμπορικά δίκτυα, όπου οι παραβιάσεις μπορεί να επιφέρουν κυρίως οικονομικό ή reputational κόστος, στα στρατιωτικά δίκτυα η απώλεια ή παραποίηση δεδομένων μπορεί να οδηγήσει σε λανθασμένες αποφάσεις μάχης, αποτυχία αποστολών ή ακόμη και απώλειες ζωών.

Α. Ασφάλεια κατά τη μετάδοση

Η προστασία της πληροφορίας κατά τη μεταφορά της είναι καίρια, καθώς οι γραμμές επικοινωνίας αποτελούν το πιο ευάλωτο σημείο σε περιβάλλοντα υψηλής απειλής. Για την διασφάλιση της εμπιστευτικότητας χρησιμοποιούνται ισχυροί αλγόριθμοι κρυπτογράφησης, όπως η χρήση αλγορίθμων AES-256 ή ακόμη και πιστοποιημένων Type-1 συσκευών (σύμφωνα με τα πρότυπα ΝΑΤΟ/ΗΠΑ) εξασφαλίζει ανώτατο επίπεδο εμπιστευτικότητας [123]. Η χρήση στρατιωτικών VPN και HAIPE διασφαλίζουν end-to-end κρυπτογράφηση ακόμη και μέσω δορυφορικών συνδέσεων SATCOM, μειώνοντας την πιθανότητα υποκλοπής [126].

Παράλληλα, τεχνικές όπως το frequency hopping και spread spectrum καθιστούν τη συνεχή αλλαγή καναλιών και η διάχυση σήματος αποτρέπουν τόσο τον εντοπισμό όσο και την παρεμβολή (jamming) [160]. Επιπλέον, η εφαρμογή noise shaping δυσκολεύει την αναγνώριση του πραγματικού σήματος, αυξάνοντας το επίπεδο προστασίας [140]. Τέλος, τα σύγχρονα δίκτυα επιτηρούνται με αλγορίθμους τεχνητής νοημοσύνης(AI/ML) που ανιχνεύουν αποκλίσεις (π.χ. spoofing GPS, ασυνήθιστη κατανάλωση bandwidth) σε πραγματικό χρόνο [202].

Β. Ασφάλεια κατά την αποθήκευση

Η προστασία των δεδομένων συνεχίζεται και στο επίπεδο αποθήκευσης, όπου τα συστήματα συχνά αποτελούν στόχους φυσικής ή λογικής παραβίασης. Τα κρυπτογραφημένα file systems διασφαλίζουν ότι ακόμη και σε περίπτωση απώλειας εξοπλισμού τα δεδομένα παραμένουν μη αναγνώσιμα [203]. Παράλληλα, η διαβάθμιση πρόσβασης (RBAC/ABAC) εξασφαλίζει ότι οι χρήστες έχουν μόνο τα απαραίτητα δικαιώματα, περιορίζοντας τις πιθανότητες insider threats.

Για την αποτροπή πλήρους αποκάλυψης πληροφοριών, εφαρμόζονται τεχνικές fragmentation & dispersion όπου ο διαχωρισμός των δεδομένων σε επιμέρους τμήματα και η διασπορά τους σε διαφορετικά μέσα μειώνει δραστικά τον κίνδυνο αποκάλυψης του συνόλου [203]. Επιπρόσθετα, οι μηχανισμοί self-destruct & zeroization mechanisms σε περίπτωση φυσικής παραβίασης ή απώλειας συσκευής ενεργοποιούνται, καταστρέφοντας τα κλειδιά ή και τα ίδια τα δεδομένα. Σε αυτό το πλαίσιο, τα hardware Security Modules (HSMs) προσφέρουν εξειδικευμένο περιβάλλον για την ασφαλή διαχείριση κλειδιών, αποτρέποντας την εξαγωγή ή την αντιγραφή τους [201].

Γ. Ενισχυτικές τεχνολογίες

Συμπληρωματικά προς την κρυπτογράφηση και τον έλεγχο πρόσβασης, εφαρμόζονται τεχνολογίες που ενισχύουν την ακεραιότητα και την ιχνηλασιμότητα. Η αξιοποίηση blockchain-based logging δημιουργεί ένα αποκεντρωμένο και αμετάβλητο αρχείο καταγραφών που αποκαλύπτει κάθε προσπάθεια παραποίησης. Παράλληλα, το trusted timestamping εξασφαλίζει την ακριβή χρονοσήμανση γεγονότων, παρέχοντας αποδείξεις εγκυρότητας. Επιπλέον, η εφαρμογή tamper-evident storage κάνει άμεσα εμφανείς τις απόπειρες φυσικής ή λογικής παραβίασης.

Δ. Στρατηγική σημασία

Η εφαρμογή ενός πολυεπίπεδου πλαισίου ασφάλειας και προστασίας δεδομένων δεν είναι προαιρετική αλλά ζωτικής σημασίας για τις Ένοπλες Δυνάμεις. Σε περιβάλλοντα όπου η επιχειρησιακή συνέχεια είναι κρίσιμη, ο συνδυασμός κρυπτογράφησης, redundancy, τεχνητής νοημοσύνης και μηχανισμών αυτοκαταστροφής προσφέρει ένα δίκτυο ανθεκτικό σε κυβερνοεπιθέσεις, ηλεκτρονικό πόλεμο και φυσικές παραβιάσεις. Έτσι, διασφαλίζεται ότι τα δεδομένα διοίκησης, ελέγχου και ISR παραμένουν αξιόπιστα και διαθέσιμα, επιτρέποντας τη λήψη αποφάσεων με ακρίβεια και ταχύτητα.

5.4.5 Καταγραφή, έλεγχος και ακεραιότητα

Η καταγραφή και ο έλεγχος (logging & auditing) αποτελούν κρίσιμα στοιχεία για την επιχειρησιακή ασφάλεια και την αξιοπιστία των στρατιωτικών δικτύων. Η προστασία δεδομένων και η εφεδρεία δεν επαρκούν από μόνες τους· είναι απαραίτητο να υπάρχει συνεχής, αδιάβλητη και τεκμηριωμένη εικόνα όλων των ενεργειών, ώστε να εντοπίζονται εγκαίρως οι απειλές, να αποτρέπεται η παραποίηση και να διασφαλίζεται η επιχειρησιακή συνέχεια [203].

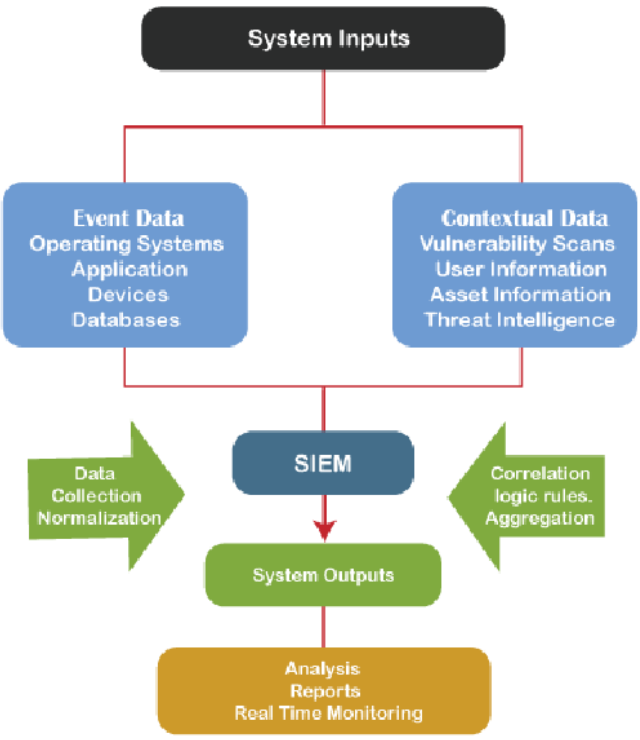
Α. Συστήματα Συγκέντρωσης και Ανάλυσης Καταγραφών

Η κεντρική συλλογή και ανάλυση καταγραφών είναι απαραίτητη για την έγκαιρη ανίχνευση και αντιμετώπιση απειλών. Τα SIEM (Security Information and Event Management) αποτελούν την «καρδιά» της διαχείρισης ασφάλειας, καθώς συγκεντρώνουν δεδομένα από πολλαπλές πηγές (firewalls, routers, servers, endpoints) και τα επεξεργάζονται με κανόνες συσχέτισης [205]. Με αυτόν τον τρόπο, μπορούν να εντοπίσουν μοτίβα που υποδεικνύουν επιθέσεις, όπως brute-force login, malware beaconing ή προσπάθειες εξαγωγής δεδομένων.

Η χρήση SIEM σε στρατιωτικά δίκτυα προσφέρει πλεονεκτήματα όπως:

- Κεντρική επιτήρηση σε πολλαπλά επίπεδα (C2, ISR, logistics).
- Real-time alerts που επιτρέπουν ταχεία αντίδραση.
- Διαλειτουργικότητα με IDS/IPS και SOAR για αυτοματοποιημένη απόκριση.
- Forensic δυνατότητες, καθώς όλα τα logs αποθηκεύονται για περαιτέρω ανάλυση σε περίπτωση περιστατικού.

Το Σχήμα 50 δείχνει τη ροή λειτουργίας ενός SIEM συστήματος, τα δεδομένα και καταγραφές (logs) από διάφορες πηγές, όπως firewalls, routers, servers, εφαρμογές και endpoints, συγκεντρώνονται σε ένα κεντρικό σημείο. Το SIEM εφαρμόζει μηχανισμούς συσχέτισης (correlation rules) και αλγορίθμους ανάλυσης για να εντοπίζει ύποπτα μοτίβα, όπως απόπειρες εισβολής ή ανωμαλίες κίνησης δικτύου. Τέλος, το αποτέλεσμα είναι η παραγωγή real-time alerts και αναφορών, τα οποία μπορούν να ενεργοποιήσουν μηχανισμούς απόκρισης (manual ή automated μέσω SOAR).



Σχήμα 50- Αρχιτεκτονική SIEM σε στρατιωτικό δίκτυο[205]

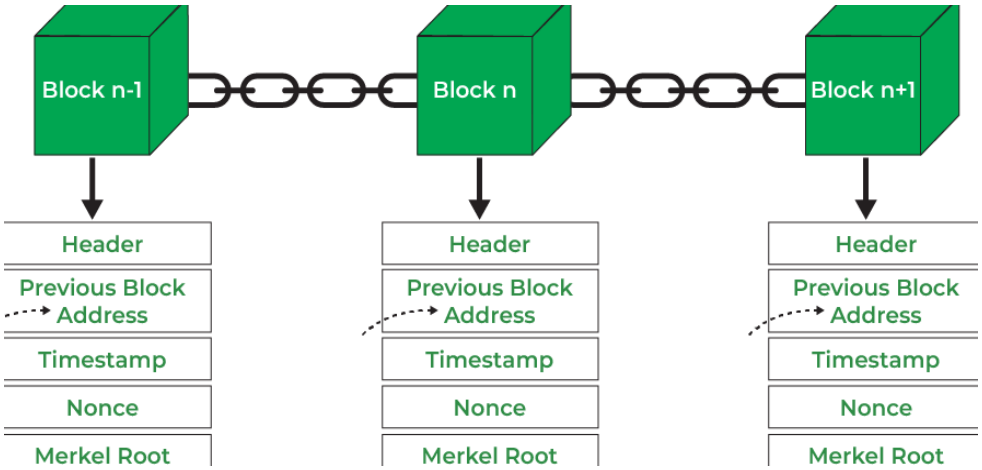
Β. Ακεραιότητα και Αδιάβλητη Καταγραφή

Η απλή αποθήκευση των logs δεν επαρκεί σε στρατιωτικά περιβάλλοντα απαιτείται εγγύηση ακεραιότητας και αδιάβλητης καταγραφής. Για τον σκοπό αυτό εφαρμόζονται μηχανισμοί που διασφαλίζουν ότι κάθε καταγραφή είναι αυθεντική, μη αλλοιώσιμη και επαληθεύσιμη ακόμη και μετά από μεγάλο χρονικό διάστημα.

Μια από τις βασικές τεχνικές είναι η χρήση append-only logs ,στα οποία οι εγγραφές αποθηκεύονται μόνο με προσθήκη, χωρίς δυνατότητα τροποποίησης ή διαγραφής, εξασφαλίζοντας διαφάνεια στη ροή γεγονότων. Παράλληλα εφαρμόζονται blockchain-style καταγραφή (hash chains) όπου κάθε νέο log ενσωματώνεται σε ένα block που συνδέεται κρυπτογραφικά με το προηγούμενο. Έτσι, οποιαδήποτε προσπάθεια αλλοίωσης γίνεται άμεσα εμφανής, αφού θα «σπάσει» η αλυσίδα. Αυτή η μέθοδος χρησιμοποιείται πιλοτικά σε στρατιωτικά data centers του NATO για forensics [206]. Επίσης, κρίσιμα επιχειρησιακά logs, όπως C2 και ISR, αποθηκεύονται σε WORM storage τα οποία δεν επιτρέπουν καμία αλλοίωση για προκαθορισμένο χρονικό διάστημα, ώστε να μπορούν να χρησιμοποιηθούν ως αξιόπιστα αποδεικτικά στοιχεία.

Το Σχήμα 51 παρουσιάζει τη λογική της αλυσίδας καταγραφών τύπου blockchain. Κάθε block περιέχει βασικά μεταδεδομένα (π.χ. header, timestamp, nonce, Merkle root) καθώς και τον hash του προηγούμενου block. Η σύνδεση αυτή δημιουργεί μια αλυσίδα (hash chain) που καθιστά άμεσα ανιχνεύσιμη κάθε παραποίηση. Αν αλλοιωθεί ένα block, η ασυνέπεια μεταφέρεται σε όλα τα επόμενα.

Το μοντέλο αυτό εξασφαλίζει ότι οι καταγραφές παραμένουν αδιάβλητες και μπορούν να χρησιμοποιηθούν ως αξιόπιστα forensic στοιχεία.



Σχήμα 51- Απεικόνιση καταγραφών τύπου blockchain[206]

Γ. Χρονισμός και Αυθεντικοποίηση Καταγραφών

Η αξιοπιστία των logs δεν εξαρτάται μόνο από την ύπαρξή τους, αλλά και από την ακριβή χρονοσήμανση και την αυθεντικοποίησή τους. Χωρίς αξιόπιστο χρόνο και επαλήθευση γνησιότητας, η χρήση τους σε στρατιωτικά περιβάλλοντα χάνει τη στρατηγική της αξία.

Για την επίτευξη ακριβούς χρονισμού, χρησιμοποιείται ο συνδυασμός GPS M-code και atomic clocks ο οποίος παρέχει υψηλή ακρίβεια στη χρονοσήμανση, κρίσιμη για την ανακατασκευή γεγονότων και την ταυτοποίηση ακολουθίας επιθέσεων. Η ακρίβεια αυτή είναι απαραίτητη σε C2/C3 περιβάλλοντα, όπου ακόμα και δευτερόλεπτα καθυστέρησης μπορεί να επηρεάσουν κρίσιμες αποφάσεις. Παράλληλα, κάθε αρχείο καταγραφής συνοδεύεται από ψηφιακές υπογραφές όπως HMACs ή PKI certificates, που επιβεβαιώνουν την προέλευσή του και αποκλείουν την πιθανότητα παραποίησης. Έτσι, τα logs καθίστανται αποδεκτά ως αποδεικτικά στοιχεία σε επιχειρησιακές ή νομικές διαδικασίες. Επιπλέον, ο πολυεπίπεδος συγχρονισμός χρόνου από διαφορετικές και ανεξάρτητες πηγές (GPS, NTP servers, atomic clocks) μειώνει τον κίνδυνο spoofing ή drift, ενισχύοντας την ανθεκτικότητα των συστημάτων. Αυτό το πολυεπίπεδο μοντέλο χρονισμού εξασφαλίζει ότι οι καταγραφές παραμένουν ακριβείς και αξιόπιστες ακόμη και σε συνθήκες έντονου ηλεκτρονικού πολέμου.

Δ. Στρατηγική Αξία για Στρατιωτικές Επιχειρήσεις

Η ύπαρξη ισχυρών μηχανισμών logging δεν αποτελεί απλώς τεχνικό εργαλείο αλλά κρίσιμο παράγοντα στρατηγικής αξίας. Η πλήρης ιχνηλασιμότητα (Traceability επιτρέπει στους διοικητές να έχουν σαφή εικόνα για το πώς εξελίχθηκαν τα γεγονότα, βελτιώνοντας τη διαδικασία λήψης αποφάσεων σε πραγματικό χρόνο. Σε περιβάλλοντα μάχης, η ικανότητα αναδρομής σε κάθε ενέργεια μπορεί να καθορίσει την επιτυχία ή την αποτυχία μιας αποστολής.

Παράλληλα, η απόδοση ευθυνών (Accountability) επιτυγχάνεται μέσω της τεκμηριωμένης αναδρομής σε περιστατικά κυβερνοεπιθέσεων ή λειτουργικών αστοχιών επιτρέπει την απόδοση ευθυνών σε άτομα ή συστήματα. Έτσι μειώνονται οι πιθανότητες εσωτερικών απειλών και ενισχύεται η πειθαρχία των εμπλεκομένων. Τα logs λειτουργούν ως αποδεικτικά στοιχεία σε περιπτώσεις στρατιωτικών δικαστηρίων ή συμμαχικών ερευνών. Η αδιάβλητη καταγραφή (π.χ. μέσω WORM ή blockchain logging) διασφαλίζει ότι τα δεδομένα μπορούν να χρησιμοποιηθούν ως αξιόπιστα στοιχεία για την απόδειξη παραβιάσεων.

Τέλος, η real-time ανάλυση των καταγραφών επιτρέπει την άμεση κατανόηση της κατάστασης και τον εντοπισμό κυβερνοεπιθέσεων τη στιγμή που εκδηλώνονται. Με αυτόν τον τρόπο οι στρατιωτικές δυνάμεις αποκτούν αυξημένη επιχειρησιακή επίγνωση, μειώνοντας τον χρόνο αντίδρασης και αυξάνοντας τις πιθανότητες επιτυχούς αντιμετώπισης.

Συνολικά, η καταγραφή και ο έλεγχος συμβάλλουν όχι μόνο στην τεχνική προστασία, αλλά και στη στρατηγική αποτροπή (cyber deterrence), καθώς ενισχύουν τη διαφάνεια, την αξιοπιστία και την εμπιστοσύνη σε πολυεθνικά στρατιωτικά δίκτυα.

ΚΕΦΑΛΑΙΟ 6

6 Καινοτομία & Μελλοντικές Τάσεις

6.1 AI και ML σε τακτικά στρατιωτικά δίκτυα

Η ραγδαία πρόοδος της Τεχνητής Νοημοσύνης (AI) και της Μηχανικής Μάθησης (ML) τα τελευταία χρόνια έχει μεταμορφώσει τον τρόπο με τον οποίο σχεδιάζονται και λειτουργούν τα τακτικά στρατιωτικά δίκτυα. Σε αντίθεση με τα παραδοσιακά δίκτυα που βασίζονται σε στατικούς αλγορίθμους και χειροκίνητη παραμετροποίηση, τα AI/ML συστήματα μπορούν να μαθαίνουν από το περιβάλλον τους και να προσαρμόζονται δυναμικά σε μεταβαλλόμενες συνθήκες.

Με αυτόν τον τρόπο, τα δίκτυα αποκτούν υψηλότερο βαθμό αυτονομίας, μειώνεται η ανάγκη συνεχούς ανθρώπινης παρέμβασης και ενισχύεται η ανθεκτικότητα σε ακραίες καταστάσεις, όπως επιθέσεις jamming, αιφνίδιες απώλειες κόμβων ή κυβερνοεπιθέσεις μεγάλης κλίμακας. Επιπλέον, τα AI/ML εργαλεία συμβάλλουν στη μείωση του χρόνου απόκρισης σε περιστατικά και ελαττώνουν τον γνωστικό φόρτο για τους χειριστές, επιτρέποντας σε στρατιώτες και επιτελείς να εστιάσουν σε στρατηγικές αποφάσεις υψηλότερου επιπέδου [207], [208].

6.1.1 Προσαρμοστική δρομολόγηση και διαχείριση κυκλοφορίας

Σε δίκτυα MANETs και Ad Hoc περιβάλλοντα, όπου οι κόμβοι χαρακτηρίζονται από υψηλή κινητικότητα και περιορισμένο φάσμα, η δρομολόγηση δεδομένων αποτελεί μια από τις σημαντικότερες προκλήσεις. Η συνεχής μεταβολή της τοπολογίας, οι φυσικοί φραγμοί και οι εχθρικές παρεμβολές δημιουργούν συνθήκες αστάθειας που συχνά οδηγούν σε απώλεια πακέτων ή διακοπή υπηρεσιών.

Η ενσωμάτωση αλγορίθμων Reinforcement Learning (RL) δίνει τη δυνατότητα στα δίκτυα να «μαθαίνουν» από την εμπειρία τους και να επιλέγουν δυναμικά τις βέλτιστες διαδρομές. Αντί να στηρίζονται σε στατικούς πίνακες δρομολόγησης, τα AI-ενισχυμένα πρωτόκολλα εξετάζουν σε πραγματικό χρόνο μετρικές όπως καθυστέρηση, απώλεια πακέτων, ισχύ σήματος και ενεργειακή κατάσταση κόμβων. Έτσι μπορούν να ανακατευθύνουν την κίνηση πριν εμφανιστεί συμφόρηση ή πριν αποκοπεί κάποιος κόμβος.

Τα βασικά οφέλη της προσέγγισης είναι:

- Μείωση καθυστέρησης (latency): Ιδιαίτερα κρίσιμη σε εφαρμογές C2 και τηλεχειρισμού UAVs.

- Αυξημένη διαθεσιμότητα: Το δίκτυο παραμένει λειτουργικό ακόμη και σε περιπτώσεις πολλαπλών αστοχιών.
- Ανθεκτικότητα σε επιθέσεις: Τα routing disruption ή jamming αντιμετωπίζονται με άμεση ενεργοποίηση εναλλακτικών διαδρομών.

Επιπλέον, η προσαρμοστική δρομολόγηση είναι καθοριστική σε swarm επιχειρήσεις UAVs ή δικτυωμένων οχημάτων μάχης, όπου δεκάδες ή εκατοντάδες κόμβοι πρέπει να διατηρούν συνεχή επικοινωνία χωρίς κεντρική υποδομή [207], [208]. Σε τέτοια σενάρια, οι AI-βασισμένοι μηχανισμοί επιτρέπουν στο δίκτυο να λειτουργεί ως ένας ενιαίος «ζωντανός οργανισμός», ικανός να διατηρεί την αποστολή ακόμα και σε συνθήκες έντονου ηλεκτρονικού πολέμου.

6.1.2 Ανίχνευση και απόκριση σε απειλές

Η χρήση AI/ML για την ανίχνευση και απόκριση σε απειλές διαφοροποιείται ριζικά από τα παραδοσιακά signature-based συστήματα ασφαλείας, τα οποία βασίζονται αποκλειστικά σε γνωστά patterns επιθέσεων. Με την υιοθέτηση supervised και unsupervised learning, τα μοντέλα αποκτούν τη δυνατότητα να αναλύσουν τη συμπεριφορά του δικτύου και να εντοπίζουν ανορθόδοξες ή ύποπτες δραστηριότητες που δεν έχουν προηγουμένως καταγραφεί.

Οι κύριες κατηγορίες ανωμαλιών που μπορούν να εντοπιστούν μέσω συστημάτων ανάλυσης και τεχνητής νοημοσύνης αφορούν διαφορετικά επίπεδα λειτουργίας των στρατιωτικών δικτύων. Μία από τις πιο συχνές είναι η data exfiltration δηλαδή ασυνήθιστη αύξηση εξερχόμενης κίνησης που μπορεί να υποδηλώνει διαρροή δεδομένων. Εξίσου σημαντική είναι η ανίχνευση spoofing διευθύνσεων (IP/MAC): προσπάθειες παραπλάνησης πρωτοκόλλων routing ή πλαστογράφηση ταυτότητας κόμβων. Άλλη χαρακτηριστική μορφή απειλής είναι οι DDoS επιθέσεις: ασυνήθιστα υψηλή κατανάλωση bandwidth ή επαναλαμβανόμενα αιτήματα. Τέλος, οι φυσικού επιπέδου ανωμαλίες: μεταβολές στη συχνότητα ή στην ισχύ εκπομπής που μπορεί να οφείλονται σε jamming ή προσπάθεια υποκλοπής.

Η πραγματική καινοτομία εντοπίζεται στη δυνατότητα αυτόματης απόκρισης. Τα AI/ML υποσυστήματα δεν περιορίζονται στην ανίχνευση, αλλά μπορούν να ενεργοποιούν δυναμικά μέτρα όπως την αλλαγή καναλιού ή συχνότητας για αποφυγή παρεμβολών, την ενεργοποίηση εφεδρικών διαδρομών (redundancy) ώστε να διασφαλίζεται η συνέχεια επικοινωνίας και την απομόνωση ύποπτου κόμβου για την αποτροπή περαιτέρω εξάπλωσης της απειλής.

Σε επιχειρησιακά σενάρια όπου κάθε δευτερόλεπτο είναι κρίσιμο, η δυνατότητα ενός δικτύου να αναγνωρίζει και να αποκρίνεται αυτόματα σε απειλές παρέχει ουσιαστικό στρατηγικό πλεονέκτημα [211], [212]. Ένα AI-ενισχυμένο δίκτυο λειτουργεί ως «ζωντανός οργανισμός», ικανός να

αυτοπροστατεύεται, να προσαρμόζει και να διατηρεί τη λειτουργικότητα του ακόμη και υπό έντονες κυβερνοεπιθέσεις ή ηλεκτρονικό πόλεμο.

6.1.3 Ενεργειακή βελτιστοποίηση

Στα τακτικά περιβάλλοντα, οι περισσότερες πλατφόρμες αιχμής – όπως UAVs, φορητοί αισθητήρες IoMT και κινητοί κόμβοι δικτύου – λειτουργούν με περιορισμένες ενεργειακές πηγές, οι οποίες συχνά δεν μπορούν να ανανεωθούν εύκολα κατά τη διάρκεια μιας αποστολής. Η διαχείριση της ενέργειας, επομένως, δεν αποτελεί μόνο τεχνικό ζήτημα, αλλά συνδέεται άμεσα με την επιχειρησιακή αντοχή, τη διαθεσιμότητα επικοινωνιών και την επιτυχία της αποστολής.

Η ενσωμάτωση AI/ML τεχνικών επιτρέπει τη μετάβαση από στατικές πολιτικές εξοικονόμησης ενέργειας σε προσαρμοστικές και προγνωστικές στρατηγικές. Μέσω των προγνωστικών μοντέλων κατανάλωσης (predictive energy models) αναλύονται τα πρότυπα χρήσης και προβλέπουν πότε η κατανάλωση ενδέχεται να κορυφωθεί, ώστε το σύστημα να προσαρμόσει εκ των προτέρων τη λειτουργία του. Η τεχνική energy-aware routing: η δρομολόγηση δεδομένων γίνεται με βάση το εναπομείναν ενεργειακό απόθεμα των κόμβων, ώστε να αποφεύγεται η υπερφόρτωση συγκεκριμένων μονάδων. Επίσης, το adaptive power control: η ισχύς εκπομπής προσαρμόζεται δυναμικά ανάλογα με την ποιότητα του καναλιού, μειώνοντας την κατανάλωση χωρίς να θυσιάζεται η αξιοπιστία.

Επιπλέον, το AI μπορεί να υποστηρίξει συνεργατικές στρατηγικές διαχείρισης. Για παράδειγμα, σε ένα σμήνος UAVs, οι κόμβοι με υψηλότερα αποθέματα ενέργειας μπορούν να αναλάβουν μεγαλύτερο φόρτο επικοινωνίας ή relay λειτουργίες, επιμηκύνοντας τον χρόνο ζωής του συνολικού δικτύου. Σε περιπτώσεις όπου υπάρχει δυνατότητα ενεργειακής συγκομιδής (π.χ. ηλιακή φόρτιση), το AI μπορεί να συγχρονίζει τις περιόδους αυξημένης κατανάλωσης με τις περιόδους αναπλήρωσης ενέργειας.

Η ενεργειακή βελτιστοποίηση μέσω AI/ML συμβάλλει στη δημιουργία δικτύων με παρατεταμένη διάρκεια ζωής, που παραμένουν επιχειρησιακά λειτουργικά ακόμη και σε περιβάλλοντα με περιορισμένες δυνατότητες ανεφοδιασμού. Αυτό μεταφράζεται σε μεγαλύτερη αυτονομία, ανθεκτικότητα και μείωση του ρίσκου απώλειας κρίσιμων επικοινωνιών στο πεδίο μάχης.

6.1.4 Real Time Decision Support

Η ενσωμάτωση συστημάτων Τεχνητής Νοημοσύνης στα πλαίσια C4ISR μεταβάλλει ριζικά τον κύκλο λήψης αποφάσεων. Παραδοσιακά, η συλλογή, η ανάλυση και η αξιοποίηση πληροφοριών γίνονταν σε διακριτά στάδια με σημαντικές χρονικές καθυστερήσεις. Αντίθετα, τα AI-driven decision support systems μπορούν να συγχωνεύσουν δεδομένα από πολλαπλές πηγές (sensor fusion), να τα επεξεργαστούν με predictive analytics και να προσφέρουν εξηγήσιμες (explainable AI – XAI) συστάσεις σε πραγματικό χρόνο.

Οι βασικές λειτουργίες των ευφυών συστημάτων διοίκησης και ελέγχου βασισμένων σε AI/ML περιλαμβάνουν μια σειρά μηχανισμούς που συνδυάζουν συλλογή και συγχώνευση δεδομένων UAV video, SIGINT, telemetry από IoMT κόμβους και δορυφορικά feeds συνδυάζονται ώστε να δημιουργηθεί μια ενοποιημένη εικόνα της επιχειρησιακής κατάστασης. Στην συνέχεια, μέσω προβλεπτικής ανάλυσης (predictive analytics), τα μοντέλα εντοπίζουν τάσεις ή πιθανές εξελίξεις, π.χ. μετακίνηση εχθρικών μονάδων ή πιθανή κατάρρευση ενός κόμβου επικοινωνίας. Το σύστημα είναι επίσης σε θέση να παράγει συγκεκριμένες προτάσεις δράσης actionable recommendations, για παράδειγμα το σύστημα προτείνει συγκεκριμένες ενέργειες, όπως ανακατεύθυνση σμήνους UAV, ενεργοποίηση εφεδρικού gateway ή απομόνωση ενός κόμβου που εμφανίζει ύποπτη συμπεριφορά. Τέλος η λειτουργία explainability: οι προτάσεις συνοδεύονται από δείκτες εμπιστοσύνης και αιτιολόγηση, ώστε οι χειριστές να γνωρίζουν το «γιατί» πίσω από μια σύσταση.

Το αποτέλεσμα είναι η σημαντική μείωση του decision latency – ο χρόνος λήψης κρίσιμων αποφάσεων μειώνεται από λεπτά ή ώρες σε λίγα δευτερόλεπτα. Αυτό προσφέρει στρατηγικό πλεονέκτημα, ιδιαίτερα σε περιβάλλοντα υψηλής αβεβαιότητας, όπου η έγκαιρη και τεκμηριωμένη απόφαση μπορεί να κρίνει την έκβαση μιας αποστολή [213].

6.1.5 Ενδεικτική Εφαρμογή: DAPRA OFFSET

Ένα χαρακτηριστικό παράδειγμα εφαρμογής AI/ML σε τακτικά δίκτυα είναι το πρόγραμμα DARPA OFFSET (OFFensive Swarm-Enabled Tactics), το οποίο επικεντρώνεται στον αυτόνομο έλεγχο σμηνών UAVs.



Σχήμα 52- Swarm drones σε πειραματικό πεδίο προγράμματος DAPRA OFFSET [214]

Μέσω τεχνικών swarm intelligence, δεκάδες UAVs συνεργάζονται αυτόνομα, μοιράζονται δεδομένα σε πραγματικό χρόνο και εκτελούν αποστολές με ελάχιστη ανθρώπινη παρέμβαση. Το παράδειγμα αυτό αποδεικνύει ότι οι swarm τεχνολογίες(βλέπε Σχήμα 52) έχουν περάσει από τη θεωρία στην πράξη, προσφέροντας ουσιαστικό επιχειρησιακό πλεονέκτημα.

6.2 Κβαντικές επικοινωνίες και Entanglement

Η ανάπτυξη των κβαντικών επικοινωνιών θεωρείται από τις πιο κρίσιμες τεχνολογικές εξελίξεις για την ασφάλεια των στρατιωτικών δικτύων. Σε αντίθεση με τις παραδοσιακές μεθόδους κρυπτογράφησης που βασίζονται στη μαθηματική πολυπλοκότητα (RSA, ECC), οι κβαντικές επικοινωνίες στηρίζονται σε θεμελιώδεις νόμους της φυσικής, όπως η αρχή της αβεβαιότητας του Heisenberg και η κβαντική εμπλοκή. Αυτό σημαίνει ότι η ασφάλεια είναι εγγενής και δεν μπορεί να παρακαμφθεί ούτε από τους ισχυρότερους μελλοντικούς κβαντικούς υπολογιστές [215].

6.2.1 Quantum Key Distribution(QKD)

Η Κβαντική Διανομή Κλειδιού (Quantum Key Distribution – QKD) αποτελεί σήμερα την πιο ώριμη και κατανοητή τεχνολογία στον χώρο των κβαντικών επικοινωνιών. Η θεμελιώδης διαφορά της σε σχέση με τα παραδοσιακά κρυπτογραφικά συστήματα είναι ότι η ασφάλεια δεν βασίζεται στη δυσκολία επίλυσης ενός μαθηματικού προβλήματος (όπως συμβαίνει με RSA ή ECC), αλλά σε θεμελιώδεις φυσικούς νόμους της κβαντικής μηχανικής.

Στην QKD, η δημιουργία ενός κοινού μυστικού κλειδιού επιτυγχάνεται μέσω της μετάδοσης κβαντικών bits(qubits), που συνήθως υλοποιούνται ως φωτόνια με διαφορετικές πολώσεις. Ο αποστολέας (Alice) και ο παραλήπτης (Bob) πραγματοποιούν μετρήσεις σε τυχαίες βάσεις. Αν τρίτος (Eve) επιχειρήσει να υποκλέψει τα φωτόνια, η μέτρησή του θα αλλοιώσει τις κβαντικές καταστάσεις (λόγω της αρχής της αβεβαιότητας του Heisenberg), με αποτέλεσμα να προκύψουν εμφανή σφάλματα στο κλειδί. Έτσι, τα δύο μέρη γνωρίζουν άμεσα εάν το κανάλι είναι ασφαλές ή αν έχει παραβιαστεί [216].

Δύο από τα πιο εμβληματικά πρωτόκολλα QKD είναι το BB84 (Bennett & Brassard, 1984): που αποτελεί το πρώτο πρακτικό πρωτόκολλο QKD. Χρησιμοποιεί τέσσερις διαφορετικές πολώσεις φωτονίων (δύο ορθογώνιες και δύο διαγώνιες), επιτρέποντας στον Bob και την Alice να συμφωνήσουν σε κλειδιά μόνο όταν οι βάσεις μέτρησης ταιριάζουν. Η ασφάλεια προκύπτει επειδή οποιαδήποτε υποκλοπή αλλοιώνει αναπόφευκτα τα δεδομένα και το E91 (Ekert, 1991) όπου βασίζεται στην κβαντική εμπλοκή (entanglement). Η Alice και ο Bob λαμβάνουν ζεύγη εμπλεκόμενων φωτονίων, οι μετρήσεις των οποίων παραμένουν συσχετισμένες ακόμη και αν τα σωματίδια βρίσκονται σε μεγάλη απόσταση.

Η ασφάλεια θεμελιώνεται μέσω της παραβίασης των ανισοτήτων Bell, που αποκλείει την ύπαρξη κρυφών μεταβλητών ή κλασικών μηχανισμών υποκλοπής.

Στο στρατιωτικό πεδίο, η QKD αποκτά στρατηγική αξία καθώς παρέχει επίπεδα ασφαλείας που υπερβαίνουν τις δυνατότητες κλασικής κρυπτογραφίας. Πρωτίστως εξασφαλίζει απόλυτη εμπιστευτικότητα στις επικοινωνίες C2, αφού τα κβαντικά κλειδιά δεν μπορούν να παραβιαστούν ακόμη και σε περιβάλλοντα ηλεκτρονικού πολέμου. Επιπλέον, υποστηρίζει ασφαλείς δορυφορικές επικοινωνίες (SATCOM) όπως απέδειξαν πειράματα όπως αυτά με τον κινεζικό δορυφόρο Micius απέδειξαν ότι η QKD είναι εφαρμόσιμη σε διαστημικά περιβάλλοντα μεγάλης εμβέλειας. Τέλος, η QKD προσφέρει προστασία έναντι κβαντικών υπολογιστών καθώς σε αντίθεση με την κλασική κρυπτογραφία που κινδυνεύει να καταστεί ανασφαλής, η QKD παραμένει ασφαλής ακόμη και απέναντι σε μελλοντικούς κβαντικούς υπολογιστές.

Η QKD, επομένως, δεν αποτελεί απλώς τεχνολογικό πείραμα αλλά μια κομβική καινοτομία με στρατηγικό χαρακτήρα, που μπορεί να καθορίσει την υπεροχή σε μελλοντικά δίκτυα μάχης και διαστημικές επιχειρήσεις.

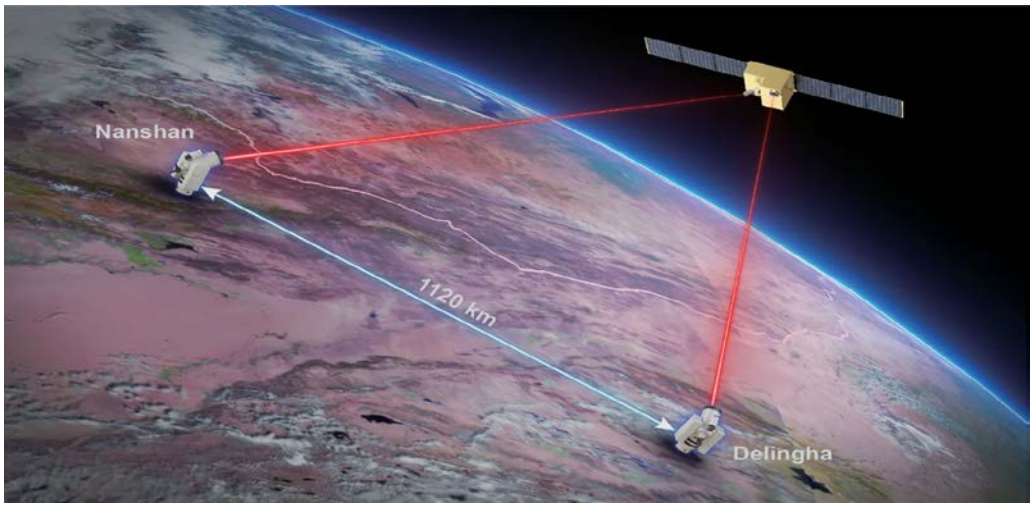
6.2.2 Κβαντική διεμπλοκή(Entanglement)

Το φαινόμενο της κβαντικής διεμπλοκής (quantum entanglement) αποτελεί μία από τις πιο ριζοσπαστικές και θεμελιώδεις έννοιες της κβαντικής φυσικής. Όταν δύο σωματίδια, όπως φωτόνια, δημιουργούνται σε εμπλεκόμενη κατάσταση, οι ιδιότητές τους παραμένουν απόλυτα συσχετισμένες ανεξαρτήτως απόστασης. Αυτό σημαίνει ότι μια μέτρηση στο ένα φωτόνιο καθορίζει ακαριαία την κατάσταση του άλλου, ακόμη και αν βρίσκονται σε διαφορετικές ηπείρους.

Η αρχή αυτή μπορεί να αξιοποιηθεί σε Entanglement-based QKD (όπως το πρωτόκολλο E91), όπου η ασφάλεια προκύπτει από τις θεμελιώδεις αρχές της κβαντικής φυσικής και όχι από την υπολογιστική πολυπλοκότητα. Επειδή η εμπλεκόμενη κατάσταση δεν μπορεί να αντιγραφεί (no-cloning theorem), οι επικοινωνίες είναι εγγενώς προστατευμένες από man-in-the-middle ή spoofing επιθέσεις [217].

Το πιο χαρακτηριστικό παράδειγμα προέρχεται από το πρόγραμμα QUESS (Quantum Experiments at Space Scale) της Κίνας. Ο δορυφόρος *Micius* πέτυχε για πρώτη φορά τη διανομή εμπλεκόμενων φωτονίων σε απόσταση άνω των 1.200 km, αποδεικνύοντας ότι η κβαντική εμπλοκή μπορεί να χρησιμοποιηθεί για ασφαλείς επικοινωνίες σε παγκόσμια κλίμακα. Το επίτευγμα αυτό αποτελεί ορόσημο, καθώς ανοίγει τον δρόμο για την ανάπτυξη ενός “κβαντικού internet”, με άμεσες εφαρμογές τόσο σε στρατηγικά στρατιωτικά δίκτυα όσο και σε πολυεθνικές συμμαχικές επικοινωνίες [217].

Η σημασία της κβαντικής εμπλοκής για τις ένοπλες δυνάμεις έγκειται στο ότι προσφέρει ασφαλή επικοινωνία χωρίς ενδιάμεσους κόμβους που θα μπορούσαν να υποκλαπούν, ανίχνευση οποιασδήποτε προσπάθειας υποκλοπής, καθώς η εμπλεκόμενη κατάσταση αλλοιώνεται και προοπτική παγκόσμιων δικτύων με ανθεκτικότητα σε μελλοντικές κβαντικές απειλές.



Σχήμα 53- Μετάδοση κβαντικής εμπλοκής μέσω του δορυφόρου Micius ανάμεσα στους σταθμούς Nanshan και Delingha [217]

6.2.3 Στρατιωτικές εφαρμογές και προγράμματα

Η γεωστρατηγική σημασία των κβαντικών επικοινωνιών έχει ήδη αναγνωριστεί από τις μεγάλες δυνάμεις και τους διεθνείς οργανισμούς, οι οποίοι επενδύουν σε ερευνητικά και επιχειρησιακά προγράμματα. Οι προσπάθειες αυτές αποδεικνύουν ότι η τεχνολογία δεν περιορίζεται πλέον σε θεωρητικά σχήματα ή πανεπιστημιακά εργαστήρια, αλλά μετατρέπεται σε εργαλείο στρατηγικής αποτροπής και επιχειρησιακής υπεροχής [218].

Η Κίνα πρωτοπορεί στον τομέα μέσω του προγράμματος QUESS(Quantum Ecxperiments at Space Scale) και του δορυφόρου Micius. Το εγχείρημα απέδειξε τη βιωσιμότητα δορυφορικών QKD και entanglement-based links σε αποστάσεις χιλιάδων χιλιομέτρων. Η επιτυχία του κατέστησε την Κίνα πρωτοπόρο στην κβαντική επικοινωνία, με άμεση εφαρμογή στην προστασία στρατηγικών δορυφορικών επικοινωνιών και C2 συστημάτων [217].

Στις Ηνωμένες Πολιτείες, η DARPA ηγείται του προγράμματος Quantum Networks το οποίο εστιάζει στην επιχειρησιακή χρήση QKD σε battlefield environments, όπου οι συνθήκες χαρακτηρίζονται από έντονο θόρυβο, παρεμβολές και κυβερνοεπιθέσεις. Το πρόγραμμα DARPA επιδιώκει τη δημιουργία τακτικών δικτύων με θεωρητικά «άθραυστη» κρυπτογράφηση, διατηρώντας λειτουργικότητα ακόμη και σε σενάρια έντονου κυβερνοπολέμου [219].

Η Ευρωπαϊκή Ένωση αναπτύσσει το δίκτυο EuroQCI (European Quantum Communication Infrastructure), το οποίο θα αποτελέσει το ασφαλές «quantum backbone» της ηπείρου. Η υποδομή

αυτή έχει διπλό χαρακτήρα: θα χρησιμοποιείται για πολιτικές επικοινωνίες υψηλής ασφάλειας αλλά και για στρατιωτικές εφαρμογές, ενισχύοντας τη στρατηγική αυτονομία της Ευρώπης.

Παράλληλα, το NATO μέσω του Οργανισμού Επιστήμης και Τεχνολογίας (STO) διερευνά την ενσωμάτωση QKD σε κρίσιμα δίκτυα C4ISR και SATCOM. Η βασική πρόκληση είναι η εξασφάλιση διαλειτουργικότητας μεταξύ των κρατών-μελών, ώστε οι πολυεθνικές αποστολές να λειτουργούν με κοινά πρότυπα ασφαλείας [216].

Η ανάπτυξη αυτών των προγραμμάτων δείχνει ότι οι κβαντικές επικοινωνίες εξελίσσονται σε νέο πεδίο γεωστρατηγικού ανταγωνισμού, αντίστοιχο με την πυρηνική και διαστημική κούρσα του 20ού αιώνα. Τα κράτη που θα αποκτήσουν επιχειρησιακά κβαντικά δίκτυα θα διαθέτουν ανυπέρβλητο πλεονέκτημα σε επίπεδο ασφάλειας επικοινωνιών, κυβερνοάμυνας και στρατηγικής αποτροπής.

6.2.4 Προκλήσεις και μελλοντικές κατευθύνσεις

Παρά την εντυπωσιακή πρόοδο που έχει σημειωθεί, η επιχειρησιακή ενσωμάτωση των κβαντικών επικοινωνιών σε στρατιωτικά δίκτυα παραμένει ιδιαίτερα προκλητική. Οι βασικές δυσκολίες εντοπίζονται σε τεχνικό, οργανωτικό και θεσμικό επίπεδο.

Στο τεχνικό επίπεδο,η μετάδοση φωτονίων επηρεάζεται από τον ατμοσφαιρικό θόρυβο, την απόσταση και την απορρόφηση σε οπτικές ίνες. Η απώλεια ακόμη και μικρού αριθμού qubits μπορεί να μειώσει δραματικά την αξιοπιστία του κλειδιού. Παράλληλα, ο εξοπλισμός (πηγές φωτονίων, ανιχνευτές, ψύξη υπεραγώγιμων υλικών) είναι ιδιαίτερα ακριβός και δύσκολος στη συντήρηση.

Η διαλειτουργικότητα αποτελεί μία ακόμη πρόκληση. Τα περισσότερα στρατιωτικά δίκτυα είναι σχεδιασμένα για κλασικές μορφές κρυπτογράφησης. Η εισαγωγή QKD απαιτεί την ανάπτυξη κοινών προτύπων και STANAGs (NATO Standardization Agreements), ώστε οι πολυεθνικές δυνάμεις να μπορούν να συνεργάζονται απρόσκοπτα.

Εξίσου σημαντικό ζήτημα είναι η ανάγκη ανάπτυξης νέων υποδομών. Για να επιτευχθεί παγκόσμια κάλυψη, απαιτείται η ανάπτυξη quantum repeaters και quantum memories. Οι συσκευές αυτές θα επιτρέψουν την ενίσχυση και αποθήκευση κβαντικών καταστάσεων σε μεγάλες αποστάσεις, δημιουργώντας έτσι ένα «κβαντικό backbone» σε ηπειρωτική ή ακόμη και διαπλανητική κλίμακα.

Κατά την μεταβατική περίοδο, η πλέον ρεαλιστική προσέγγιση είναι η ανάπτυξη υβριδικών αρχιτεκτονικών, όπου οι κβαντικές τεχνολογίες αναμένεται να συνδυαστούν με τις υφιστάμενες μεθόδους (π.χ. AES, IPsec). Ένα τέτοιο hybrid crypto μοντέλο θα προσφέρει επιχειρησιακή ευελιξία, επιτρέποντας τη σταδιακή μετάβαση από τα συμβατικά στα πλήρως κβαντικά δίκτυα.

Η μελλοντική έρευνα εστιάζει σε τρεις βασικούς άξονες: την κλιμάκωση (scalability): δημιουργία κβαντικών δικτύων μεγάλης κλίμακας που θα συνδέουν δορυφόρους, βάσεις και κινητές

μονάδες, την μείωση κόστους: ανάπτυξη πιο οικονομικών και αξιόπιστων υλικών και συσκευών και την θεσμική τυποποίηση: καθιέρωση διεθνών προτύπων που θα επιτρέψουν τη διαλειτουργικότητα και την ασφαλή χρήση σε πολυεθνικά περιβάλλοντα.

Στρατηγικά, τα κράτη και οι συμμαχίες που θα καταφέρουν να αποκτήσουν πρώιμη πρόσβαση σε πλήρως λειτουργικές κβαντικές υποδομές θα αποκτήσουν πλεονέκτημα ανάλογο με εκείνο που προσέφεραν οι πυρηνικές και διαστημικές τεχνολογίες τον 20ό αιώνα. Η κβαντική επικοινωνία δεν αποτελεί μόνο τεχνολογική καινοτομία, αλλά και μέσο αποτροπής στον 21ο αιώνα [217].

6.3 IoMT : Εξέλιξη και Πρόκληση

Το IoMT αποτελεί τη στρατιωτική εξέλιξη τουIoT, όπου εκατομμύρια αισθητήρες, συσκευές, οχήματα, UAVs, φορητά συστήματα και πλατφόρμες μάχης διασυνδέονται σε ένα ενιαίο δικτυοκεντρικό οικοσύστημα. Σε αντίθεση με το εμπορικό IoT, το IoMT λειτουργεί σε εξαιρετικά εχθρικά περιβάλλοντα (DIL – Disconnected, Intermittent, Limited), όπου η ασφάλεια, η αξιοπιστία και η ανθεκτικότητα έχουν πρωτεύουσα σημασία.

6.3.1 Αρχιτεκτονική και Λειτουργία

Το IoMT στηρίζεται σε μια πολυεπίπεδη αρχιτεκτονική, η οποία εξασφαλίζει τη συλλογή, μετάδοση και αξιοποίηση δεδομένων από το πεδίο μάχης. Η δομή αυτή οργανώνεται σε τρία βασικά επίπεδα.

Πρώτον το επίπεδο Αισθητήρων (Sensing Layer) που αποτελεί το «πρώτο μέτωπο» του IoMT, όπου λαμβάνει χώρα η συλλογή δεδομένων. Εδώ ανήκουν οι φορητοί αισθητήρες στρατιωτών (π.χ. βιομετρικοί, GPS), οι ενσωματωμένοι αισθητήρες σε οχήματα μάχης, τα UAVs/UGVs με κάμερες και ραντάρ, καθώς και σταθμοί επιτήρησης. Τα δεδομένα αυτά παρέχουν μια λεπτομερή και πολυδιάστατη εικόνα του επιχειρησιακού περιβάλλοντος. Δεύτερον το επίπεδο Δικτύωσης (Networking Layer) όπου εξασφαλίζει την αξιόπιστη μεταφορά των δεδομένων, ακόμα και σε απομονωμένα ή εχθρικά περιβάλλοντα. Εδώ εντάσσονται τεχνολογίες όπως MANETs, δορυφορικές επικοινωνίες (SATCOM), δίκτυα νέας γενιάς (5G/6G) και γνωστικά ραδιόφωνα (cognitive radios), τα οποία προσαρμόζονται δυναμικά σε παρεμβολές και μεταβαλλόμενες συνθήκες. Το επίπεδο αυτό είναι κρίσιμο για να διασφαλιστεί ότι τα δεδομένα φτάνουν χωρίς καθυστέρηση στα κέντρα διοίκησης [218]. Και τέλος, το επίπεδο Εφαρμογών (Application Layer): Πρόκειται για το επίπεδο όπου τα δεδομένα μετατρέπονται σε χρήσιμη πληροφορία. Εντάσσονται συστήματα C4ISR, εφαρμογές logistics για την εφοδιαστική αλυσίδα, συστήματα battlefield healthcare για υγειονομική υποστήριξη και real-time analytics που ενισχύουν τη λήψη αποφάσεων.

Η πολυεπίπεδη αυτή αρχιτεκτονική επιτρέπει την αδιάλειπτη ροή δεδομένων από το πεδίο μάχης προς τα κέντρα διοίκησης, ενισχύοντας τη situational awareness και μειώνοντας τον χρόνο λήψης κρίσιμων αποφάσεων. Ουσιαστικά, το IoMT λειτουργεί ως «νευρικό σύστημα» του στρατού, όπου οι αισθητήρες αποτελούν τα μάτια και τα αυτιά, τα δίκτυα το νευρικό δίκτυο και τα συστήματα C4ISR τον εγκέφαλο.

6.3.2 Ενδεικτικές εφαρμογές

Η εφαρμογή του IoMT εκτείνεται σε ένα ευρύ φάσμα στρατιωτικών επιχειρησιακών πεδίων, προσφέροντας δυνατότητες που ενισχύουν την αποτελεσματικότητα, την ασφάλεια και την επιχειρησιακή επίγνωση των δυνάμεων. Οι βασικές κατηγορίες εφαρμογών περιλαμβάνουν τη διασύνδεση προσωπικού, οχημάτων, αισθητήρων και υποδομών σε ένα ενιαίο δικτυοκεντρικό περιβάλλον.

Μία από τις πιο χαρακτηριστικές υλοποιήσεις είναι ο δικτυωμένος στρατιώτης (Networked Soldier). Ο σύγχρονος στρατιώτης μετατρέπεται σε «κινητό κόμβο πληροφορίας» χάρη στη χρήση wearables που καταγράφουν σε πραγματικό χρόνο ζωτικές παραμέτρους (καρδιακός παλμός, θερμοκρασία σώματος), την ακριβή θέση (GPS) αλλά και την κατάσταση του εξοπλισμού. Τα δεδομένα αυτά μεταδίδονται σε συστήματα C2, επιτρέποντας καλύτερη διαχείριση προσωπικού, προληπτική υγειονομική φροντίδα και βελτίωση της επιχειρησιακής επίγνωσης.

Αντίστοιχα, τα έξυπνα οχήματα μάχης: Τα οχήματα μάχης εξοπλίζονται με πολυάριθμους αισθητήρες (οπτικούς, θερμικούς, LIDAR) και AI modules που αναλύουν το περιβάλλον και επικοινωνούν με UAVs και σταθμούς διοίκησης. Έτσι, τα οχήματα μπορούν να ανταλλάσσουν δεδομένα απειλών, να λειτουργούν σε ημιαυτόνομη ή αυτόνομη λειτουργία και να βελτιώνουν τη συνεργασία μεταξύ χερσαίων και εναέριων δυνάμεων.

Η συνεργασία UAV/UGV συνιστά άλλη μία προηγμένη εφαρμογή του IoMT.Η χρήση σμηνών μη επανδρωμένων αεροσκαφών (UAVs) και επίγειων οχημάτων (UGVs) επιτρέπει τη δημιουργία συνεργατικών δικτύων επιτήρησης και μάχης. Τα σμήνη αυτά ανταλλάσσουν δεδομένα αισθητήρων, εντοπίζουν απειλές και μπορούν να εκτελέσουν επιθέσεις ακριβείας ή αποστολές αναγνώρισης με ελάχιστη ανθρώπινη παρέμβαση. Το IoMT αποτελεί τον βασικό μηχανισμό που επιτρέπει την επικοινωνία και τον συντονισμό τους.

Εξίσου σημαντική είναι η χρήση του IoMT στη διαχείριση logistics και εφοδιαστική αλυσίδα. Η εφαρμογή IoMT στα logistics δίνει τη δυνατότητα συνεχούς παρακολούθησης αποθεμάτων, καυσίμων, ανταλλακτικών και μεταφορών. Με αισθητήρες RFID, GPS trackers και predictive analytics, οι ένοπλες δυνάμεις αποκτούν πλήρη εικόνα της εφοδιαστικής αλυσίδας, μειώνοντας τον κίνδυνο ελλείψεων και βελτιστοποιώντας τη διανομή πόρων σε απομακρυσμένα μέτωπο.

Τέλος, στον τομέα της στρατιωτικής υγειονομικής υποστήριξης (Battlefield Healthcare) το IoMT αξιοποιεί biosensors, έξυπνων ιατρικών wearables και τηλεϊατρικής, είναι δυνατή η άμεση διάγνωση και παρακολούθηση της υγείας των στρατιωτών στο πεδίο μάχης. Τα δεδομένα μεταδίδονται σε κέντρα υγειονομικής υποστήριξης, όπου ιατρικό προσωπικό μπορεί να παρέμβει σε πραγματικό χρόνο ή να καθοδηγήσει πρώτες βοήθειες επί τόπου. Έτσι μειώνεται δραστικά ο χρόνος αντίδρασης σε ιατρικά περιστατικά.

6.3.3 Προκλήσεις και κίνδυνοι

Παρά τα σημαντικά πλεονεκτήματα που προσφέρει το *Internet of Military Things (IoMT)*, η εφαρμογή του σε τακτικά και στρατηγικά περιβάλλοντα συνοδεύεται από μια σειρά προκλήσεων που πρέπει να αντιμετωπιστούν ώστε να διασφαλιστεί η επιχειρησιακή αξιοπιστία. Η ασφάλεια και η κυβερνοάμυνα αποτελούν το σημαντικότερο ζήτημα, καθώς η ύπαρξη χιλιάδων ή και εκατομμυρίων διασυνδεδεμένων κόμβων αυξάνει δραματικά την επιφάνεια επίθεσης. Επιθέσεις όπως *spoofing*, *data exfiltration* ή κακόβουλες παρεμβολές μπορούν να οδηγήσουν σε παραπληροφόρηση, απώλεια εμπιστευτικότητας ή ακόμη και πλήρη επιχειρησιακή αποτυχία. Για τον λόγο αυτό απαιτούνται πολυεπίπεδα μέτρα άμυνας, όπως *end-to-end encryption*, *Zero Trust Architectures* και *anomaly detection*.

Εξίσου κρίσιμοι είναι οι ενεργειακοί περιορισμοί. Οι φορητοί αισθητήρες, τα UAVs και τα μικρού μεγέθους IoMT συστήματα διαθέτουν περιορισμένη αυτονομία, ενώ η συνεχής μετάδοση δεδομένων μπορεί να εξαντλήσει γρήγορα τις μπαταρίες, περιορίζοντας τον επιχειρησιακό χρόνο. Για την αντιμετώπιση αυτής της πρόκλησης αναπτύσσονται *energy-aware* πρωτόκολλα και τεχνικές ενεργειακής συγκομιδής, όπως ηλιακή ή *RF harvesting*, ώστε να αυξηθεί η διάρκεια των αποστολών χωρίς απώλεια αξιοπιστίας [220].

Ένα ακόμη σημαντικό ζήτημα είναι η διαλειτουργικότητα, καθώς οι διαφορετικοί κατασκευαστές και προμηθευτές χρησιμοποιούν συχνά μη συμβατά πρωτόκολλα. Σε πολυεθνικές επιχειρήσεις αυτό μπορεί να προκαλέσει σοβαρά προβλήματα συντονισμού και ασφάλειας. Η ανάπτυξη κοινών διεθνών προτύπων, όπως τα STANAGs του NATO, θεωρείται απαραίτητη για την απρόσκοπτη συνεργασία μεταξύ συμμαχικών δυνάμεων.

Εξίσου μεγάλη πρόκληση αποτελεί η διαχείριση δεδομένων. Ο τεράστιος όγκος πληροφοριών που παράγεται από το IoMT απαιτεί ισχυρές υποδομές *cloud* και *edge computing* καθώς και προηγμένα συστήματα *AI-based analytics*, ώστε να επιτυγχάνεται εξαγωγή χρήσιμης πληροφορίας σε πραγματικό χρόνο. Η δυσκολία δεν έγκειται μόνο στην αποθήκευση, αλλά κυρίως στο φιλτράρισμα και στην αξιολόγηση των κρίσιμων δεδομένων που πρέπει να φτάσουν εγκαίρως στον διοικητή.

Τέλος, δεν μπορούν να αγνοηθούν τα ηθικά και νομικά ζητήματα. Η εκτεταμένη παρακολούθηση στρατιωτών μέσω *biosensors* και φορητών συστημάτων εγείρει ανησυχίες σχετικά με

την ιδιωτικότητα, την ψυχολογική πίεση και τη λογοδοσία. Παράλληλα, η χρήση αυτόνομων IoMT πλατφορμών, όπως *UGVs* και σμήνη *UAVs*, θέτει ζητήματα ευθύνης σε περιπτώσεις σφαλμάτων ή απωλειών.

Συνολικά, οι προκλήσεις αυτές δείχνουν ότι το IoMT δεν αποτελεί απλώς τεχνολογικό εγχείρημα, αλλά απαιτεί ολιστική προσέγγιση που να συνδυάζει τεχνολογία, δόγματα επιχειρήσεων, διεθνή πρότυπα και ηθικό-νομικό πλαίσιο, ώστε να εξασφαλιστεί η ασφαλής και αποτελεσματική ενσωμάτωσή του στις σύγχρονες στρατιωτικές δομές.

6.3.4 Στρατηγική σημασία

Το IoMT μεταμορφώνει τον τρόπο διεξαγωγής στρατιωτικών επιχειρήσεων, καθώς επιτρέπει την πλήρη υλοποίηση της αρχής του network-centric warfare. Μέσω της συνεχούς ροής δεδομένων από αισθητήρες, UAVs, οχήματα μάχης και στρατιώτες, δημιουργείται μια ενιαία επιχειρησιακή εικόνα (common operational picture), στην οποία έχουν πρόσβαση όλοι οι εμπλεκόμενοι σε πραγματικό χρόνο.

Η στρατηγική σημασία του IoMT εκφράζεται σε πολλαπλά επιχειρησιακά επίπεδα, καθιστώντας το θεμέλιο της σύγχρονης δικτυοκεντρικής άμυνας. Πρωτίστως, ενισχύει την ενοποιημένη επίγνωση κατάστασης (situational awareness), παρέχοντας στους διοικητές μια ολοκληρωμένη και δυναμική εικόνα του πεδίου μάχης, γεγονός που μειώνει δραστικά την πιθανότητα λανθασμένων εκτιμήσεων και αποφάσεων. Εξίσου σημαντική είναι η μείωση του decision latency, καθώς η αξιοποίηση τεχνολογιών *AI/ML* σε συνδυασμό με τα δεδομένα του IoMT επιτρέπει τη λήψη αποφάσεων μέσα σε δευτερόλεπτα αντί για λεπτά ή ώρες — ένα στοιχείο καθοριστικής σημασίας σε ταχέως εξελισσόμενα επιχειρησιακά σενάρια. Επιπλέον, το IoMT συμβάλλει στη βελτίωση της διαλειτουργικότητας πολυεθνικών δυνάμεων, καθώς μέσα από την υιοθέτηση κοινών προτύπων και ασφαλών πρωτοκόλλων επιτρέπει τη συνεχή ανταλλαγή πληροφοριών μεταξύ των δυνάμεων του ΝΑΤΟ και των συμμάχων, χωρίς να δημιουργούνται κενά ασφαλείας. Τέλος, το IoMT υποστηρίζει την έννοια των Multi-Domain Operations (MDO), λειτουργώντας ως «ραχοκοκαλιά» που συνδέει τα επιχειρησιακά πεδία της ξηράς, του αέρα, της θάλασσας, του διαστήματος και του κυβερνοχώρου, καθιστώντας εφικτό τον πλήρη συντονισμό πολυχωρικών και διαλειτουργικών επιχειρήσεων.

Η στρατηγική αξία του IoMT είναι συγκρίσιμη με εκείνη που είχαν στο παρελθόν οι δορυφορικές επικοινωνίες και η ψηφιακή δικτύωση, οι οποίες αναβάθμισαν ριζικά την ισχύ και την αποτελεσματικότητα των στρατών. Σήμερα, το IoMT εξελίσσεται σε ένα νέο force multiplier, ικανό να προσφέρει σε όποιον το υιοθετήσει έγκαιρα ένα αποφασιστικό πλεονέκτημα στο πεδίο μάχης του 21ου αιώνα.

6.4 Τεχνολοηική σύγκλιση και ολοκληρωμένες πλατφόρμες

Η τεχνολογική σύγκλιση περιγράφει τη συνένωση κρίσιμων τεχνολογικών ρευμάτων —AI/ML, IoMT, 5G/6G, SATCOM, κυβερνοασφάλεια και προηγμένα C4ISR— σε ένα συνεκτικό, διαλειτουργικό οικοσύστημα. Στόχος είναι η δημιουργία ενός «στρατιωτικού νευρικού συστήματος» που συλλέγει, διακινεί και αξιοποιεί πληροφορία σε πραγματικό χρόνο, επιτρέποντας ταχύτερη, ασφαλέστερη λήψη αποφάσεων και ευέλικτη ανακατανομή πόρων σε πολυχώριες επιχειρήσεις.

6.4.1 Ορισμός και ανάγκη για σύγκλιση

Η τεχνολογική σύγκλιση αποτελεί θεμελιώδη παράγοντα στη μετάβαση των ενόπλων δυνάμεων προς ένα πλήρως δικτυοκεντρικό και πολυχώριο περιβάλλον επιχειρήσεων. Η σύγχρονη πραγματικότητα, όπου οι επιχειρήσεις εκτείνονται ταυτόχρονα σε ξηρά, θάλασσα, αέρα, διάστημα και κυβερνοχώρο, καθιστά ανεπαρκή την παραδοσιακή προσέγγιση της ανάπτυξης απομονωμένων τεχνολογιών. Όταν κάθε τομέας εξελίσσεται ανεξάρτητα, προκύπτουν προβλήματα κατακερματισμού, ασυμβατότητας και έλλειψης συντονισμού, τα οποία υπονομεύουν τη συνοχή των επιχειρήσεων και μειώνουν την επιχειρησιακή υπεροχή.

Η τεχνολογική σύγκλιση στοχεύει στη συνένωση κρίσιμων τεχνολογικών ρευμάτων —όπως η AI, το IoMT, τα δίκτυα 5G/6G, οι δορυφορικές επικοινωνίες (SATCOM) και οι υποδομές κυβερνοασφάλειας— μέσα σε ένα ενιαίο, διαλειτουργικό οικοσύστημα. Αυτή η ενοποίηση δεν αποτελεί απλώς τεχνική βελτίωση, αλλά μια δομική μετατόπιση στον τρόπο με τον οποίο οι στρατοί αντιλαμβάνονται, επεξεργάζονται και αξιοποιούν την πληροφορία στο πεδίο μάχης.

Μέσω αυτής της προσέγγισης επιτυγχάνεται ενοποίηση αισθητήρων και δεδομένων από UAVs, δορυφόρους, επίγειους κόμβους και IoMT συσκευές, τα οποία συνδυάζονται σε μία γεωχωρικά χαρτογραφημένη επιχειρησιακή εικόνα. Παράλληλα, η αξιοποίηση τεχνητής νοημοσύνης στην περιφέρεια του δικτύου (Edge AI) επιτρέπει την τοπική επεξεργασία δεδομένων και τη λήψη αποφάσεων σχεδόν σε πραγματικό χρόνο, μειώνοντας την εξάρτηση από απομακρυσμένα data centers. Επιπλέον, η καθιέρωση κοινών προτύπων και STANAGs του NATO εξασφαλίζει διαλειτουργικότητα και ασφαλή συνεργασία μεταξύ συμμαχικών δυνάμεων, ανεξαρτήτως προέλευσης εξοπλισμού ή τεχνολογίας.

Ένα χαρακτηριστικό παράδειγμα στρατιωτικής τεχνολογικής σύγκλισης αποτελεί το πρόγραμμα Joint All-Domain Command and Control (JADC2) των Ηνωμένων Πολιτειών. Το JADC2 στοχεύει στη σύνδεση όλων των τομέων επιχειρήσεων μέσω ενός κοινού δικτυοκεντρικού πλαισίου που επιτρέπει τη συλλογή, ανάλυση και ανταλλαγή δεδομένων σε πραγματικό χρόνο. Με αυτόν τον τρόπο, μειώνεται δραστικά ο χρόνος από την ανίχνευση της απειλής έως τη λήψη και εκτέλεση της απόφασης, ενώ επιτυγχάνεται πλήρης συγχρονισμός μεταξύ ετερογενών μονάδων.

Η στρατηγική σημασία της τεχνολογικής σύγκλισης έγκειται στη μετατόπιση της φιλοσοφίας από τη μεμονωμένη υπεροχή ανά domain προς την ολιστική υπεροχή, όπου η δύναμη προκύπτει από τη συνέργεια, την ταχύτητα και τη συνεχή ανταλλαγή πληροφορίας. Με αυτόν τον τρόπο, η τεχνολογική σύγκλιση δεν είναι απλώς μια τεχνική επιλογή, αλλά απαραίτητη προϋπόθεση για τη διατήρηση της στρατηγικής υπεροχής στο μέλλον των πολυχωρικών επιχειρήσεων.

6.4.2 Ολοκληρωμένες πλατφόρμες C4ISR

Τα σύγχρονα συστήματα C4ISR αποτελούν τον πυρήνα του ψηφιακού μετασχηματισμού των ενόπλων δυνάμεων. Η εξέλιξή τους από μεμονωμένα πληροφοριακά συστήματα σε ολοκληρωμένες πλατφόρμες (platforms-of-platforms) σηματοδοτεί τη μετάβαση σε ένα περιβάλλον όπου οι αισθητήρες, τα δίκτυα, οι υπολογιστικοί πόροι και τα αναλυτικά εργαλεία λειτουργούν συντονισμένα, παράγοντας πληροφορία υψηλής ακρίβειας και επιχειρησιακής αξίας σε πραγματικό χρόνο.

Ο μετασχηματισμός αυτός βασίζεται στη δυνατότητα των C4ISR να μετατρέπουν ωμές ροές δεδομένων (video, telemetry, SIGINT, SAR) σε actionable intelligence μέσω τεχνικών sensor fusion και AI-driven analytics. Με αυτόν τον τρόπο, ο διοικητής δεν λαμβάνει απλώς ακατέργαστα δεδομένα, αλλά μια ενοποιημένη, ερμηνευμένη και ιεραρχημένη εικόνα του πεδίου μάχης.

Η υποδομή λειτουργεί ως cloud-to-edge continuum στο οποίο η επεξεργασία δεδομένων κατανέμεται ιεραρχικά, με ελαφρά inference μοντέλα εκτελούνται στα edge nodes (π.χ. UAVs, τοπικοί σταθμοί, gateways) για αποφάσεις χαμηλού latency ενώ τα βαριά analytics και η εκπαίδευση μοντέλων πραγματοποιούνται σε regional ή strategic nodes, όπου υπάρχουν ισχυρότεροι υπολογιστικοί πόροι.Η αρχιτεκτονική βασίζεται σε microservices και API-based orchestration (π.χ. Kubernetes), ενώ τα κανάλια επικοινωνίας προστατεύονται με HAIPE/IPsec. Αυτή η διάρθρωση επιτρέπει multi-tier fusion: τοπική προεπεξεργασία → περιφερειακή συγκέντρωση → στρατηγική σύνθεση.

Οι κύριες λειτουργίες της πλατφόρμας περιλαμβάνουν fusion & Contextualization δηλαδή τον συνδυασμό δεδομένων οπτικών, IR, RF, θέσης και βιομετρικών σε ενιαίο geospatial layer με confidence metrics, ώστε ο διοικητής να βλέπει την ταυτότητα, πορεία, ρίσκο και πρόθεση κάθε αντικειμένου με εκτίμηση αξιοπιστίας. Επιπλέον λειτουργίες dynamic Resource Orchestration: Αυτόματος καταμερισμός πόρων μεταξύ domains (π.χ. ανακατεύθυνση UAV, ανακατανομή EW assets, αλλαγή QoS) βάσει επιχειρησιακών κανόνων και risk appetite. Η έννοια της resilience αποτυπώνεται στην ικανότητα διατήρησης επιχειρησιακής συνέχειας μέσω αυτόματης ανακατεύθυνσης ροών, failover μεταξύ SATCOM–MANET–LOS και graceful degradation σε περίπτωση απωλειών ή κυβερνοεπιθέσεων [221].

Η ασφάλεια και η διακυβέρνηση είναι άρρηκτα συνδεδεμένες με τις λειτουργίες των C4ISR πλατφορμών. Απαιτείται end-to-end κρυπτογράφηση, Key Management Infrastructure (KMI) και χρήση

HAIPE για ασφαλείς επικοινωνίες υψηλής διαβάθμισης. Για την ακεραιότητα των δεδομένων, εφαρμόζονται append-only logs (WORM ή blockchain-style) που διασφαλίζουν πλήρη ιχνηλασιμότητα και audit trails. Η διαλειτουργικότητα εξασφαλίζεται μέσω κοινών data models και προτύπων (π.χ. STANAG, FMN profiles), ενώ η governance περιλαμβάνει MLOps πρακτικές, signed models και πιστοποίηση αλγορίθμων.

Η αξιολόγηση των πλατφορμών C4ISR βασίζεται σε μετρήσιμα κριτήρια: decision latency(χρόνος από τη συλλογή δεδομένων έως τη λήψη απόφασης), MTTD/MTTR(χρόνος εντοπισμού και αποκατάστασης περιστατικών), action success rate(ποσοστό επιτυχούς εκτέλεσης αποφάσεων), fusion confidence(μέσο επίπεδο αξιοπιστίας σύνθεσης δεδομένων), system availability(ποσοστό διαθεσιμότητας κρίσιμων υπηρεσιών).

Συνολικά, οι ολοκληρωμένες πλατφόρμες C4ISR ενσωματώνουν τεχνητή νοημοσύνη, ασφάλεια, και κυβερνο-ανθεκτικότητα σε ένα ενιαίο πλαίσιο διοίκησης, ενισχύοντας την ταχύτητα, ακρίβεια και αποτελεσματικότητα των στρατιωτικών επιχειρήσεων.

6.4.3 Τεχνολογικές προϋποθέσεις για ολοκλήρωση

Η επιτυχής υλοποίηση της τεχνολογικής σύγκλισης και η μετάβαση από αποσπασματικά υποσυστήματα σε πλήρως ολοκληρωμένες πλατφόρμες απαιτεί την ταυτόχρονη ωρίμανση τεχνολογικών, οργανωτικών και επιχειρησιακών πυλώνων. Η σύγκλιση δεν μπορεί να επιτευχθεί μεμονωμένα· προϋποθέτει κοινά πρότυπα, ενιαίες αρχιτεκτονικές, ασφαλή δίκτυα και αξιόπιστους μηχανισμούς διακυβέρνησης.

Οι βασικοί άξονες προϋποθέσεων συνοψίζονται ως εξής:

1. Πρότυπα και Πρωτόκολλα

Η διαλειτουργικότητα αποτελεί ακρογωνιαίο λίθο για τη συνεργασία συμμαχικών δυνάμεων και προμηθευτών. Απαιτείται χρήση STANAGs του NATO, HAIPE για κρυπτογράφηση υψηλής διαβάθμισης, καθώς και προφίλ IPsec προσαρμοσμένα σε απαιτήσεις battlefield (χαμηλό latency, αυξημένο QoS). Επιπλέον, κοινά data models (π.χ. GeoJSON, XML/ASN.1 συμβατά με STANAG) και σταθερά API contracts διασφαλίζουν αξιόπιστη ανταλλαγή πληροφοριών μεταξύ ετερογενών συστημάτων.

2. Edge Computing με Δυνατότητες Μηχανικής Μάθησης (ML)

Η μεταφορά επεξεργαστικής ισχύος κοντά στην πηγή δεδομένων μειώνει καθυστερήσεις και αυξάνει την αυτονομία. Τα edge nodes πρέπει να υποστηρίζουν containerized microservices, ασφαλές caching, remote attestation για επιβεβαίωση ταυτότητας, και MLOps pipelines για συνεχή ενημέρωση

μοντέλων. Η χρήση signed models εξασφαλίζει την ακεραιότητα και την πιστοποίηση των αλγορίθμων [218].

3. Ιδιωτικά 5G/5G-Advanced και Μελλοντικά 6G Δίκτυα

Τα ιδιωτικά δίκτυα 5G (enterprise/private 5G) παρέχουν χαμηλό latency, υψηλή αξιοπιστία και network slicing, το οποίο επιτρέπει τη δημιουργία λογικών υποδικτύων για κρίσιμες ροές C2 ή ISR. Οι τεχνολογίες 5G-Advanced και μελλοντικά 6G θα ενισχύσουν τη φασματική απόδοση, την ασφάλεια και τη δυνατότητα διασύνδεσης πολλών εκατομμυρίων IoMT συσκευών [220].

4. Έξυπνη Διαχείριση Φάσματος (Spectrum Management)

Σε περιβάλλοντα έντονου ηλεκτρονικού πολέμου, η διαχείριση φάσματος πρέπει να είναι δυναμική και προσαρμοστική. Η χρήση cognitive radios και machine learning επιτρέπει real-time αναγνώριση παρεμβολών (jamming) και συμφόρησης, καθώς και αυτόματη ανακατανομή συχνοτήτων, ισχύος ή κατεύθυνσης εκπομπής (beamforming). Επιπλέον, απαιτείται σχεδιασμός για συνύπαρξη με πολιτικά δίκτυα σε περιβάλλοντα σύγκρουσης φάσματος [221].

5. Ασφάλεια by Design και Υποδομές Κλειδιών (KMI)

Η ασφάλεια πρέπει να ενσωματώνεται από τον σχεδιασμό (security-by-design). Αυτό περιλαμβάνει authenticated boot, signed firmware, WORM/blockchain-based logging για auditability και πλήρη Key Management Infrastructure (KMI). Παράλληλα, απαιτείται συμμόρφωση με πρότυπα πιστοποίησης όπως STANAGs, NIAP/CC ή εθνικά πλαίσια αξιολόγησης.

6. Ανθεκτικότητα και Ανάκαμψη (Resilience & Disaster Recovery)

Η σχεδίαση πρέπει να υποστηρίζει multi-path redundancy (MANET ↔ SATCOM ↔ line-of-sight), failover policies, immutable backups, καθώς και RPO/RTO στόχους ευθυγραμμισμένους με τις επιχειρησιακές απαιτήσεις. Η αυτόματη ανάκαμψη υπηρεσιών (self-healing systems) αποτελεί βασικό παράγοντα επιβιωσιμότητας.

7. Διακυβέρνηση Δεδομένων και Ποιότητας Fusion

Η αξιοπιστία της επιχειρησιακής εικόνας εξαρτάται από την ποιότητα των δεδομένων. Χρειάζονται μηχανισμοί provenance tracking, confidence scoring, και uncertainty modelling. Επιπλέον, η εφαρμογή Explainable AI (XAI) καθιστά τις αποφάσεις των μοντέλων διαφανείς και επαληθεύσιμες [221].

8. Ασφάλεια Εφοδιαστικής Αλυσίδας και Διακυβέρνηση

Η προστασία της αλυσίδας προμηθειών είναι κρίσιμη. Η υιοθέτηση Software Bill of Materials (SBOM), τακτικών vendor audits και πολιτικών change control διασφαλίζουν τη γνησιότητα των

προμηθειών. Παράλληλα, η ύπαρξη governance frameworks (RBAC, logging, auditing) προλαμβάνει αστοχίες και μη εξουσιοδοτημένες μεταβολές [219].

9. DevSecOps και Συνεχής Επικύρωση (Continuous Validation)

Η ανάπτυξη και συντήρηση των συστημάτων πρέπει να βασίζεται σε DevSecOps φιλοσοφία, με αυτοματοποιημένους ελέγχους ασφάλειας, red/blue team drills και σταδιακή ανάπτυξη (staged deployment) από εργαστηριακό σε επιχειρησιακό επίπεδο. Οι βασικοί δείκτες αξιολόγησης (KPIs) περιλαμβάνουν latency, availability, MTTR, detection rate και false positive rate [221].

Η σύγκλιση όλων αυτών των τεχνολογικών προϋποθέσεων δημιουργεί τη βάση για ένα ανθεκτικό, ευέλικτο και διαλειτουργικό οικοσύστημα μάχης, όπου η πληροφορία ρέει με ασφάλεια και ταχύτητα, υποστηρίζοντας τη λήψη αποφάσεων σε πολυχωρικά περιβάλλοντα επιχειρήσεων.

6.4.4 Τεχνολογικές προϋποθέσεις για ολοκλήρωση

Η τεχνολογική σύγκλιση δεν αποτελεί πλέον θεωρητική προσέγγιση, αλλά εφαρμόζεται ήδη σε μεγάλης κλίμακας στρατιωτικά προγράμματα και συμμαχικά δίκτυα. Τα ακόλουθα παραδείγματα αποτυπώνουν διαφορετικά μοντέλα υλοποίησης και δείχνουν πώς οι αρχές της ενοποίησης, της διαλειτουργικότητας και της ευελιξίας εφαρμόζονται στην πράξη.

Το NATO Federated Mission Networking (FMN) δεν πρόκειται για ένα συγκεκριμένο τεχνικό σύστημα, αλλά για πλαίσιο διαδικασιών, προτύπων και τεχνολογικών προφίλ που επιτρέπει σε ετερογενή εθνικά συστήματα να ανταλλάσσουν επιχειρησιακά δεδομένα με ασφάλεια και αξιοπιστία. Μέσω της υιοθέτησης κοινών data models, service registries και προτύπων επικοινωνίας, το FMN εξασφαλίζει τη συνέπεια του operational picture σε πολυεθνικές αποστολές, όπου η ταχύτητα πληροφορίας και η διαφάνεια είναι κρίσιμες. Επιπλέον, ενισχύει την ευελιξία των δυνάμεων, καθώς νέοι εταίροι μπορούν να ενσωματωθούν γρήγορα στο δίκτυο χωρίς εκτεταμένες τεχνικές αλλαγές.

Στο άλλο άκρο, το πρόγραμμα DARPA Mosaic Warfare επαναπροσδιορίζει τη φιλοσοφία του σχεδιασμού μάχης μέσα από μια ψηφιδωτή αρχιτεκτονική. Αντί για μεγάλα, μονολιθικά συστήματα, προτείνει τη χρήση μικρών, επαναχρησιμοποιήσιμων modules (sensors, effectors, communication nodes, compute units) που μπορούν να συνδυάζονται δυναμικά μέσω API-driven ορχήστρωσης. Η προσέγγιση αυτή επιτρέπει ταχεία αναδιάταξη δυνάμεων ανάλογα με την απειλή και το πεδίο επιχειρήσεων, αυξάνοντας δραματικά την ευελιξία και μειώνοντας το κόστος αντικατάστασης ή προσαρμογής συστημάτων. Επιπλέον, ενσωματώνει τεχνολογίες AI και machine learning για αυτόματη βελτιστοποίηση συνδυασμών αισθητήρων και εκτελεστικών συστημάτων σε πραγματικό χρόνο.

Συμπληρωματικά, το Israeli Digital Army Program αποτελεί χαρακτηριστικό παράδειγμα εθνικής στρατηγικής σύγκλισης τεχνολογιών. Συνδυάζει AI, ανάλυση μεγάλων δεδομένων, δίκτυα

χαμηλού latency και εκτεταμένη χρήση UAVs σε ένα ενιαίο πληροφοριακό οικοσύστημα. Εστιάζει στο human-machine teaming, όπου οι αποφάσεις λαμβάνονται σε συνεργασία ανθρώπου και συστήματος, με την τεχνητή νοημοσύνη να αναλαμβάνει προγνωστική ανάλυση και υποστήριξη αποφάσεων. Μέσω real-time καναλιών επικοινωνίας και συνεχούς επιτήρησης/ανάλυσης δεδομένων, το πρόγραμμα ενισχύει την ταχύτητα και ακρίβεια του κύκλου OODA (Observe–Orient–Decide–Act), προσφέροντας ουσιαστικό επιχειρησιακό πλεονέκτημα.

Συνολικά, τα παραπάνω παραδείγματα αναδεικνύουν τις πολλαπλές διαστάσεις της τεχνολογικής σύγκλισης: το FMN δίνει έμφαση στη διαλειτουργικότητα και τα κοινά πρότυπα, το Mosaic Warfare στη modular αρχιτεκτονική και την ευελιξία, ενώ το Israeli Digital Army στην επιχειρησιακή ενοποίηση και την εφαρμογή της τεχνητής νοημοσύνης στο πεδίο μάχης. Μαζί συνθέτουν έναν ρεαλιστικό οδικό χάρτη για τη μετάβαση προς τις πλήρως ολοκληρωμένες επιχειρήσεις του μέλλοντος [221].

ΚΕΦΑΛΑΙΟ 7

7 Συμπεράσματα & Προτάσεις

Η παρούσα διπλωματική εργασία επικεντρώθηκε στην επισκόπηση, ανάλυση και αξιολόγηση των τεχνολογιών, των πρωτοκόλλων και των αρχιτεκτονικών που συνθέτουν το σύγχρονο οικοσύστημα των στρατιωτικών τηλεπικοινωνιών. Μέσα από μια πολυεπίπεδη προσέγγιση που συνδύασε τη θεωρητική μελέτη, την τεχνολογική ανάλυση και τη σύνδεση με επιχειρησιακές εφαρμογές, επιδιώχθηκε η διαμόρφωση μιας ολοκληρωμένης εικόνας για το πώς η τεχνολογία των επικοινωνιών διαμορφώνει σήμερα την αμυντική ικανότητα και το στρατηγικό πλεονέκτημα των ενόπλων δυνάμεων. Το έργο αυτό απέδειξε ότι οι τηλεπικοινωνίες δεν αποτελούν πλέον ένα υποστηρικτικό εργαλείο των στρατιωτικών επιχειρήσεων, αλλά τον κεντρικό άξονα πάνω στον οποίο οικοδομούνται οι έννοιες της διαλειτουργικότητας, της ταχείας λήψης αποφάσεων και της επιχειρησιακής ανθεκτικότητας.

Η μελέτη της εξέλιξης των στρατιωτικών επικοινωνιών, όπως παρουσιάστηκε στα πρώτα κεφάλαια, κατέδειξε ότι η τεχνολογική πρόοδος αποτελεί τον κινητήριο μοχλό της επιχειρησιακής μεταμόρφωσης. Από τις πρώτες αναλογικές μορφές επικοινωνίας και τα ραδιοσυστήματα του 20ού αιώνα έως τα σύγχρονα δίκτυα IP, τα MANETs και τα συστήματα SATCOM, η επικοινωνία αποτέλεσε πάντοτε παράγοντα ισχύος, επιβιωσιμότητας και συντονισμού. Οι εξελίξεις στη ψηφιακή επεξεργασία σήματος, στη δικτυακή αρχιτεκτονική και στην κυβερνοασφάλεια οδήγησαν στη μετάβαση από τα κεντρικά, ιεραρχικά δίκτυα σε αποκεντρωμένες, ευέλικτες και προσαρμοστικές δομές, ικανές να λειτουργούν σε δυναμικά επιχειρησιακά περιβάλλοντα.

Στα κεφάλαια 4 και 5 αποδείχθηκε ότι η σύγχρονη στρατιωτική επικοινωνία βασίζεται σε ένα οικοσύστημα πρωτοκόλλων και προτύπων ειδικά σχεδιασμένων για ανθεκτικότητα, ασφάλεια και διαλειτουργικότητα. Οι τροποποιήσεις των πρωτοκόλλων TCP/IP, τα ad-hoc δίκτυα MANETs και οι μηχανισμοί ασφαλείας όπως το IPsec και το HAIPE αποτελούν θεμέλια για την προστασία της πληροφορίας και την εξασφάλιση αδιάλειπτης επικοινωνίας σε περιβάλλοντα με παρεμβολές ή περιορισμένη συνδεσιμότητα. Η έρευνα ανέδειξε ότι οι απαιτήσεις των στρατιωτικών δικτύων διαφοροποιούνται ριζικά από τις εμπορικές εφαρμογές: εκεί όπου ο ιδιωτικός τομέας επιδιώκει την αποδοτικότητα και το χαμηλό κόστος, οι ένοπλες δυνάμεις προτάσσουν την ασφάλεια, την επιβιωσιμότητα και τον έλεγχο.

Οι δορυφορικές επικοινωνίες (SATCOM), που αναλύθηκαν εκτενώς, αποτελούν βασικό πυλώνα της παγκόσμιας στρατιωτικής δικτύωσης. Η ανάπτυξη συστημάτων όπως τα MILSTAR, AEHF και WGS, σε συνδυασμό με την ενσωμάτωση τεχνολογιών LEO/MEO/GEO, έχει οδηγήσει στη δημιουργία ενός πολυεπίπεδου δικτύου που εξασφαλίζει επικοινωνία ακόμη και υπό συνθήκες πλήρους απομόνωσης

από το επίγειο δίκτυο. Η σύνδεση αυτών των συστημάτων με τις τεχνολογίες 5G και τις Non-Terrestrial Networks (NTNs) αποδεικνύει τη σταδιακή σύγκλιση του στρατιωτικού και του εμπορικού τεχνολογικού κόσμου, με στόχο τη δημιουργία ενιαίων, ευφυών δικτύων που προσφέρουν χαμηλή καθυστέρηση, υψηλή ασφάλεια και παγκόσμια διαθεσιμότητα.

Παράλληλα, η εργασία ανέδειξε ότι η ασφάλεια των επικοινωνιών αποτελεί το κρισιμότερο και πλέον απαιτητικό πεδίο των σύγχρονων επιχειρήσεων. Οι κυβερνοαπειλές, όπως το jamming, το spoofing, οι APT επιθέσεις και οι παραβιάσεις του IoMT, έχουν καταστήσει τον κυβερνοχώρο ισότιμο πεδίο πολέμου. Η αμυντική στρατηγική στον κυβερνοχώρο δεν περιορίζεται πλέον στην προστασία των συστημάτων αλλά επεκτείνεται στη διαρκή ανίχνευση, πρόληψη και προσαρμογή απέναντι στις εξελισσόμενες απειλές. Η προσέγγιση “Zero Trust”, οι τεχνικές πλεονασμού (redundancy), τα AI-based συστήματα ανίχνευσης ανωμαλιών και οι αρχιτεκτονικές “defence in depth” συνθέτουν το νέο πλαίσιο άμυνας, όπου η τεχνολογία και η ανθρώπινη επαγρύπνηση συνυπάρχουν.

Το πέμπτο και το έκτο κεφάλαιο ανέδειξαν τη σταδιακή μετάβαση προς τις γνωστικές, αυτόνομες και κβαντικά ασφαλείς επικοινωνίες. Οι εξελίξεις στην τεχνητή νοημοσύνη, στην υπολογιστική ισχύ στο άκρο του δικτύου (edge computing) και στην κβαντική κρυπτογραφία (Quantum Key Distribution) σηματοδοτούν τη γένεση μιας νέας εποχής στις στρατιωτικές επικοινωνίες, όπου τα δίκτυα δεν θα είναι απλώς εργαλεία μεταφοράς δεδομένων αλλά έξυπνα, αυτοπροσαρμοζόμενα οικοσυστήματα. Οι τεχνολογίες αυτές υπόσχονται σχεδόν απόλυτη εμπιστευτικότητα, αυτονομία και ταχύτητα στη λήψη αποφάσεων, καθιστώντας δυνατή την πλήρη ενοποίηση φυσικού, ψηφιακού και επιχειρησιακού πεδίου. Παράλληλα, όμως, εγείρουν ζητήματα διαχείρισης πολυπλοκότητας, συμβατότητας μεταξύ συστημάτων και ανάγκης για αυστηρές διαδικασίες πιστοποίησης.

Από τη συνολική ανάλυση προκύπτει ότι οι στρατιωτικές τηλεπικοινωνίες εξελίσσονται από τα ιεραρχικά και κεντρικά δίκτυα σε κατανεμημένες, δυναμικές και συνεργατικές αρχιτεκτονικές. Η έννοια του «δικτυοκεντρικού πολέμου» έχει μετατραπεί σε «δικτυοσυντονισμένο οικοσύστημα», όπου κάθε αισθητήρας, όχημα, UAV ή στρατιώτης αποτελεί κόμβο ενός ευφυούς πλέγματος πληροφορίας. Η επιτυχία σε αυτό το νέο περιβάλλον εξαρτάται από την ικανότητα των Ενόπλων Δυνάμεων να διασφαλίζουν ταυτόχρονα:

- διαλειτουργικότητα μεταξύ διαφορετικών τεχνολογιών και συστημάτων,
- επιχειρησιακή συνέχεια ακόμη και υπό επίθεση,
- και υψηλό επίπεδο κυβερνοανθεκτικότητας (cyber resilience).

Τα συμπεράσματα της εργασίας καταδεικνύουν τρεις θεμελιώδεις στρατηγικούς άξονες για το μέλλον των στρατιωτικών τηλεπικοινωνιών.

Πρώτον, η τυποποίηση και διαλειτουργικότητα αποτελούν απαραίτητη προϋπόθεση για την αποτελεσματικότητα των πολυεθνικών επιχειρήσεων. Η συνεχιζόμενη ανάπτυξη προτύπων, όπως τα NATO STANAGs και το Federated Mission Networking (FMN), είναι αναγκαία για να εξασφαλιστεί η ενιαία γλώσσα επικοινωνίας και η τεχνική συνεργασία μεταξύ συμμάχων. Η τυποποίηση δεν πρέπει να περιορίζεται στα φυσικά ή πρωτοκολλικά επίπεδα, αλλά να επεκτείνεται σε κοινά μοντέλα ασφάλειας, κρυπτογράφησης και ανταλλαγής δεδομένων.

Δεύτερον, η ενσωμάτωση της ασφάλειας εξ αρχής (secure by design) σε κάθε στάδιο ανάπτυξης συστημάτων είναι ζωτικής σημασίας. Οι απειλές εξελίσσονται ταχύτερα από τις άμυνες· συνεπώς, η ασφάλεια δεν μπορεί να αποτελεί προσθήκη εκ των υστέρων. Οι στρατιωτικοί οργανισμοί οφείλουν να επενδύσουν στην έρευνα και στην τεχνολογική καινοτομία σε τομείς όπως η τεχνητή νοημοσύνη για κυβερνοάμυνα, η κβαντική επικοινωνία, η χρήση blockchain για πιστοποίηση δεδομένων και η ανίχνευση ανωμαλιών σε πραγματικό χρόνο.

Τρίτον, ο ανθρώπινος παράγοντας παραμένει το κεντρικό στοιχείο επιτυχίας. Η τεχνολογία χωρίς εξειδικευμένο και εκπαιδευμένο προσωπικό δεν μπορεί να αποδώσει επιχειρησιακά οφέλη. Η εκπαίδευση στις αρχές της κυβερνοασφάλειας, της διαχείρισης κρίσεων, της τεχνητής νοημοσύνης και της ανάλυσης δεδομένων πρέπει να ενταχθεί οργανικά στη στρατιωτική κατάρτιση. Η ανάπτυξη ψηφιακής κουλτούρας ασφάλειας, που να διαπερνά όλα τα επίπεδα διοίκησης, είναι εξίσου κρίσιμη με την υλοποίηση των ίδιων των τεχνολογικών υποδομών.

Η εργασία αυτή κατέδειξε ότι το μέλλον των στρατιωτικών τηλεπικοινωνιών δεν θα καθοριστεί από μια μεμονωμένη καινοτομία, αλλά από τον συνδυασμό τεχνολογιών, υποδομών και ανθρώπινης τεχνογνωσίας μέσα σε ένα ευφυές, συνεργατικό και ασφαλές πλαίσιο λειτουργίας. Ο ρόλος των επικοινωνιών αναβαθμίζεται από τεχνικό υποσύστημα σε στρατηγικό πολλαπλασιαστή ισχύος, ικανό να επηρεάσει άμεσα την αποτελεσματικότητα, την επιβιωσιμότητα και την προσαρμοστικότητα των ενόπλων δυνάμεων.

Στο κατώφλι της νέας εποχής, όπου φυσικό, ψηφιακό και πληροφοριακό πεδίο συγκλίνουν, οι τηλεπικοινωνίες αναδεικνύονται ως το «νευρικό σύστημα» των στρατών του μέλλοντος. Η ικανότητα συλλογής, διαχείρισης και ασφαλούς μετάδοσης πληροφορίας σε πραγματικό χρόνο θα καθορίσει την επιτυχία κάθε επιχείρησης. Η μελλοντική έρευνα πρέπει να εστιάσει στην περαιτέρω σύζευξη των δικτύων 5G/6G με τις κβαντικές επικοινωνίες, στη δημιουργία αυτόνομων, αυτοθεραπευόμενων δικτύων και στη βελτίωση της συνεργασίας ανθρώπου–μηχανής.

Η παρούσα διπλωματική εργασία, μέσα από τη σύνθεση επιστημονικών πηγών και τεχνικών προτύπων, φιλοδοξεί να αποτελέσει ένα σημείο αναφοράς για τη συνέχιση της μελέτης και της ανάπτυξης του πεδίου. Η ασφάλεια, η καινοτομία και η διαλειτουργικότητα παραμένουν οι

ακρογωνιαίοι λίθοι πάνω στους οποίους θα οικοδομηθεί το επόμενο κεφάλαιο της στρατιωτικής επικοινωνίας – ένα κεφάλαιο όπου η πληροφορία θα είναι όχι απλώς μέσο, αλλά στρατηγικό όπλο.

Βιβλιογραφία

[1] F. Johnsen and K. S. Chan, "Military Communications," *IEEE Communications Magazine,* vol. 56, no. 10, October 2018.

[2] G. F. Elmasry, "A comparative review of commercial vs. tactical wireless networks," *IEEE Communications Magazine,* vol. 48, no. 10, October 2010.

[3] U. S. Gaire, "Application of Artificail Intelligence in the Military : An Overview," *Unity Journal,* vol. 4, no. 1, pp. 161-174, February 2023.

[4] D. Alberts, J. Garstka and F. Stein, "Network Centric Warfare Developing and Leveraging Information Superiority," *CCRP,* 1999.

[5] C. Chappe, The Optical Telegraph, Paris French: Academy of Sciences, 1795.

[6] R. Harris, Secret War : The Story of Enigma and the Codebreakers, London: Hutchinson, 1996.

[7] U.S. Department of Defense, MILSATCOM Overview, U.S. Department of Defense;, 2018.

[8] J. H. Van Boskirk, "Field Communications in World War I," *Military Review,* vol. 12, no. 3, 1932.

[9] NATO Standardization Agency, STANAG 5516- Tactical Data Exchange - Link 16, NATO Standardization Agency, 2014.

[10] J. Mitola, Cognitive Radio : An Integrated Agent Architecture for Software Defined Radio, Ph. D. dissertation, KTH Royal Institute of Technology, 2000.

[11] O. Younis, L. Kant, A. McAuley, K. Manousakis, D. Shallcross, K. Sinkar, K. Chang, K. Young, C. Graff and M. Patel, "Cognitive Tactical Network Models," *IEEE Communications Magazine,* vol. 48, no. 10, pp. 70-77, 2010.

[12] R. Bajracharya, R. Shrestha, S. A. Hassan, H. Jung και H. Shin, «5G and Beyond Private Military Communication : Trend, Requirements, Challenges and Enablers,» τόμ. 11, pp. 83996-84012, 2023.

[13] J. Nobre, D. Rosario, C. Both, E. Cerqueira and M. Gerla, "Toward Software-Defined Battlefield Networking : A Systematic Review of Military Software Defined Networks," *Future Internet,* vol. 10, no. 88, pp. 1-39, 2018.

[14] M. S. Blumberg, «The Integrated Tactical Network : Pivoting Back to Communications Superiority,» *Military Review,* pp. 104-113, May-June 2020.

[15] K. Katsaros, C. Bouras και A. Papazois , «Technological Advances in Military Communications System and Equipment,» *Military Communications Review,* τόμ. 6, αρ. 1, pp. 15-28, 2020.

[16] N. Boschetti, J. Sigholm, M. Wallen and G. Falco, "A Hybrid Space Architecture for Robust and Resilient Satellite Services," in *2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, 2023.

[17] M. Dillinger, K. Madani και N. Alonistioti, Software Defined Radio : Architectures, Systems and Functions, Hoboken, NJ, USA: John Wiley & Sons, 2003.

[18] J. Suryana and D. Candra, "Implementation of Link-16 based Tactical Data Link System Using Software-Defined Radio," in *2019 International Conference on Electrical Engineering and Informatics (ICEEI)*, Bandung, Indonesia, 2019.

[19] L. Concha Salor and V. Monzon Baeza, "Harnessing the potential of emerging technologies to break down barriers in tactical communications," *Telecom,* vol. 4, no. 4, pp. 709-731, October 2023.

[20] M. Sneps-Sneppe, On Cyber Threats in Military Communication Nets, Riga, Latvia: 2024 IEEE Workshop on Microwave Theory and Technology in Wireless Communications (MTTW), 2024, pp. 12-17.

[21] H. Pirayesh και H. Zeng, «Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey,» *IEEE Communications Surveys & Tutorials,* τόμ. 24, αρ. 2, pp. 767-809, 2022.

[22] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo, I. You and G. Pau, "Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone," *Sensors,* vol. 21, no. 6, p. 2057, March 2021.

[23] J. Chudzikiewicz, J. Furtak and Z. Zielinski, "Secure protocol for wireless communication within internet of military things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, Milan, Italy, 2015.

[24] N. Suri et al, "Peer-to-peer communications for tactical environments: Observations, requirements, and experiences," *IEEE Communications Magazine,* vol. 48, no. 0, pp. 60-69, October 2010.

[25] N. C. a. I. Agency, Federated Mission Networking (FMN) Spiral Specifications, Brussels, Belgium: NATO Communications and Information Agenc, 2020.

[26] V. Gkioulos, H. Gunleifsen and G. K. Weldehawaryat, "A Systematic Literature Review on Military Software Defined Networks," *Future Internet,* vol. 10, no. 9, p. 88, September 2018.

[27] P. H. J. Chong and N. A. Nordbotten, "Military Communications and Networks," *IEEE Communications Magazine,* vol. 61, no. 5, p. 158, May 2023.

[28] A. Mishra and T. Alexander, "Radio communications: components, systems, and networks [Series Editorial]," *IEEE Communications Magazine,* vol. 53, no. 6, pp. 42-143, June 2015.

[29] H. Wang, Y. Wang and J. Han, "A Security Architecture for Tactical Mobile Ad Hoc Networks," in *2009 Second International Workshop on Knowledge Discovery and Data Mining (WKDD)*, Moscow, Russia, 2009.

[30] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li and J. Wei, "Survey on Unmanned Aerial Vehicle Networks: A Cyber Physical System Perspective," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 2, pp. 1027-1070, 2020.

[31] M. Agiwal, A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 3, pp. 1617-1655, 2016.

[32] M. Shafi et al, "5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice," *IEEE Journal on Selected Areas in Communications,* vol. 35, no. 6, pp. 1201-1221, June 2017.

[33] F. Z. Yousaf, M. Bredel, S. Schaller και F. Schneider, «NFV and SDN—Key Technology Enablers for 5G Networks,» *IEEE Journal on Selected Areas in Communications,* τόμ. 35, αρ. 11, pp. 2468-2478, November 2017.

[34] M. Series, IMT Vision–Framework and overall objectives of the future development of IMT for 2020 and beyond, Recommendation ITU-R M.2083-0, 2015, pp. 1-21.

[35] Z. Wang, W. Pang, Z. Xiang and B. Wang, "5G in Military Applications: Challenges and Opportunities," in *2024 4th International Conference on Communication Technology and Information Technology (ICCTIT)*, Guangzhou, China, 2024.

[36] B. A. Hamilton, "Developing a Military First for AR and VR Training," 2025. [Online]. Available: https://www.boozallen.com/insights/defense/developing-a-military-first-for-ar-and-vr-training.html.

[37] A. Gupta and R. K. Jha, "A Survey of 5G Network: Architecture and Emerging Technologies," *IEEE Access,* vol. 3, pp. 1206-1232, 2015.

[38] H. Flinck, "Military use of 5G," *Eurescom Messages,* 2021.

[39] K. B. Adedeji, M. Abu-Mahfouz and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," *Journal of Sensor and Actuator Networks,* vol. 12, no. 4, p. 51, July 2023.

[40] W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network,* vol. 34, no. 3, pp. 34-142, May/June 2020.

[41] X. Lin, S. Rommer, S. Euler, E. A. Yavuz and R. S. Karlsson, "5G from Space: An Overview of 3GPP Non-Terrestrial Networks," *IEEE Communications Standards Magazine,* vol. 5, no. 4, pp. 147-153, December 2021.

[42] H. M. Al-Jawahry, D. Siri, T. Saravanan, A. K. Rai and D.G.V, "Secure and Scalable Quantum Key Distribution Protocol for Next-Generation Networks," in *2024 International Conference on IoT, Communication and Automation Technology (ICICAT)*, Gorakhpur, India, 2024.

[43] S. B. R. Tirmizi et al, "Hybrid Satellite–Terrestrial Networks toward 6G: Key Technologies and Open Issues," *Sensotd,* vol. 22, no. 21, 2022.

[44] J. Mitola, "The software radio architecture," *IEEE Communications Magazine,* vol. 33, no. 5, pp. 26-38, May 1995.

[45] J. H. Reed, Software Radio: A Modern Approach to Radio Engineering, Upper Saddle River, NJ, USA: Prentice Hall Professional, 2002.

[46] D. Advancement, "Software Defined Radio (SDR) – Military SDR Solutions," [Online]. Available: https://www.defenseadvancement.com/suppliers/software-defined-radio-sdr/.

[47] J. S. Gansler, W. Lucyshyn and J. Rigilano , The Joint Tactical Radio System: Lessons Learned and the Way Forward, College Park, MD, USA: University of Maryland, 2012.

[48] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications,* vol. 6, no. 4, pp. 13-18, August 1999.

[49] J. Li, C. Blake, D. S. De Couto, H. I. Lee and R. Morris, "Capacity of Ad Hoc Wireless Networks," in *ACM MobiCom (Proc. of the Annual International Conference on Mobile Computing and Networking)*, 2001.

[50] C. E. Perkins and E. M. Royer, "Ad-hoc-on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, USA, 1999.

[51] I. F. Akyildiz, X. Wang και W. Wang, «Wireless Mesh Networks : A Survey,» *Computer Networks,* τόμ. 47, αρ. 4, pp. 445-487, 2005.

[52] M. Conti and S. Giordano, "Multihop Ad Hoc Networking: The Theory," *IEEE Communications Magazine,* vol. 45, no. 7, pp. 78-86, April 2007.

[53] R. Jain and I. Kashyap, "Survey of Energy Aware Link Stable Routing Protocols in MANETS," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2018.

[54] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys & Tutorials,* vol. 11, no. 1, pp. 116-130, 2009.

[55] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks,* vol. 50, no. 13, pp. 2127-2159, 2006.

[56] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications,* vol. 23, no. 2, pp. 201-220, February 2005.

[57] J. Loo, J. Lloret Mauri and J. H. Ortiz, Mobile Ad Hoc Networks: Current Status and Future Trends, Boca Raton, FL, USA: CRC Press, 2011.

[58] "Cognitive Radio Network Applications – Battlefield Military Networks," in *Technical Presentation on Cognitive Radio Systems (SlideShare)*, 2020.

[59] S. M. Mishra, R. W. Brodersen and D. Cabric, "Implementation issues in spectrum sensing for cognitive radios," in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, 2004.

[60] Y. Shi, Y. E. Sagduyu, T. Erpek, K. Davaslioglu, LuZ. and J. H. Li, "Adversarial Deep Learning for Cognitive Radio Security: Jamming Attack and Defense Strategies," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, Kansas City, MO, USA, 2018.

[61] H. Sharma, N. Kumar and R. Tekchandani, "Mitigating Jamming Attack in 5G Heterogeneous Networks: A Federated Deep Reinforcement Learning Approach," *IEEE Transactions on Vehicular Technology,* vol. 72, no. 2, pp. 2439-2452, February 2023.

[62] M. Mozaffari, W. Saad, M. Bennis, Y.-. H. Nam and M. Debbah, "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 3, pp. 2334-2360, 2019.

[63] S. Hayat, E. Yanmaz and R. Muzaffar, "Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 4, pp. 2624-2661, 2016.

[64] Y. Zeng, Q. Wu and R. Zhang, "Accessing From the Sky: A Tutorial on UAV Communications for 5G and Beyond," *Proceedings of the IEEE,* vol. 107, no. 12, pp. 2327-2375, December 2019.

[65] M. Erdelj and E. Natalizio, "UAV-assisted disaster management: Applications and open issues," in *2016 International Conference on Computing, Networking and Communications (ICNC)*, Kauai, HI, USA, 2016.

[66] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine,* vol. 43, no. 9, pp. S23-S30, 2005.

[67] T. Clausen και P. Jacquet, «Optimized link state routing protocol (OLSR),» October 2003. [Ηλεκτρονικό]. Available: https://www.rfc-editor.org/rfc/rfc3626.

[68] Q. E. &. C. Inc., «Military Wireless Mesh Network Test Bed,» [Ηλεκτρονικό]. Available: https://quintech.com.

[69] S. Chen, X. Kaiping, H. Peilin and L. Hancheng, "A QoS Routing protocol in wireless mesh networks," in *2010 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, Chengdu, China, 2010.

[70] L. Buttyan and J.-P. Hubaux, Security and Cooperation in Wireless Networks, Cambridge, U.K.: Cambridge University Press, 2009.

[71] Y. Zeng, R. Zhang and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Communications Magazine,* vol. 54, no. 5, pp. 36-42, May 2016.

[72] H. M. M. Ali, A. H. Abdalla and X. Fernando, "Empowering Adaptive Geolocation-Based Routing for UAV Networks with GLAN," *Drones,* vol. 7, no. 6, pp. 1-19, June 2023.

[73] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri and A. Tuncer, "UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges," *IEEE Communications Magazine,* vol. 55, no. 3, pp. 22-28, March 2017.

[74] I. F. Akyildiz, D. Pompili and T. Melodia, "Challenges for efficient communication in underwater acoustic sensor networks," *ACM SIGBED Review,* vol. 1, no. 2, pp. 3-8, July 2004.

[75] T. E. Humphreys, Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing, Austin, TX, USA: University of Texas at Austin, 2012.

[76] Y. Sun, M. Yu, L. Wang, T. Li and M. Dong, "A Deep-Learning-Based GPS Signal Spoofing Detection Method for Small UAVs," *Drones,* vol. 9, no. 1, 2023.

[77] R. J. Hall, "An Internet of Drones," *IEEE Internet Computing,* vol. 20, no. 3, pp. 68-73, May-June 2016.

[78] C. Qiu, Y. Hu, Y. Chen and B. Zeng, "Unmanned Aerial Vehicles (UAV) Networking Algorithms: Communication, Control, and AI-Based Approaches," *Algorithms,* vol. 18, no. 5, 2023.

[79] A. Fotouhi and et al, "Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 4, pp. 3417-3442, 2019.

[80] M. Erdelj, M. Krol and E. Natalizio, "Wireless sensor networks and multi-UAV systems for natural disaster management," *Computer Networks,* pp. 72-86, September 2017.

[81] N. Ilcev, "Military Satellite Communication Network for Navy, Ground and Air Forces," 2019. [Online]. Available: https://www.researchgate.net/figure/Military-Satellite-Communication-Network-4_fig1_334750229.

[82] S. K. Sharma, S. Chatzinotas and . P.-D. Arapoglou, Satellite Communications in the 5G Era, London, U.K: Institution of Engineering and Technology (IET), 2018.

[83] A. D. Panagopoulos, P.-D. M. Arapoglou and P. G. Cottis, "Satellite communications at KU, KA, and V bands: Propagation impairments and mitigation techniques," *IEEE Communications Surveys & Tutorials,* vol. 6, no. 3, pp. 2-14, 2004.

[84] S. Kisseleff, E. Lagunas, T. S. Abdu, S. Chatzinotas and B. Ottersten, "Radio Resource Management Techniques for Multibeam Satellite Systems," *IEEE Communications Letters,* vol. 25, no. 8, pp. 2448-2452, August 2021.

[85] X. Lv and J. Jiao, "A Two-Step Handover Strategy for GEO/LEO Heterogeneous Satellite Networks," *Electronics,* vol. 11, no. 5, 2022.

[86] Joint Air Power Competence Centre, Space Operations – Jamming of Satellite Communications, Kalkar, Germany: JAPCC, 2020.

[87] A. Vanelli-Coralli, A. Guidotti, T. Foggi, G. Colavolpe and G. Montorsi, "5G and Beyond 5G Non-Terrestrial Networks: trends and research challenges," in *2020 IEEE 3rd 5G World Forum (5GWF)*, Bangalore, India, 2020.

[88] J. Postel, Transmission Control Protocol, IETF, 1981.

[89] U.S. Army Futures Command, The Integrated Tactical Network Whitepaper, 2021.

[90] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "Security in Wireless Ad Hoc Networks," *Communications of the ACM,* vol. 46, no. 5, pp. 46-55, 2002.

[91] S. Giordano, I. Stojmenovic and L. Blazevic, "Position based routing algorithms for ad hoc networks: A taxonomy," *IEEE Communications Magazine,* vol. 40, no. 7, pp. 128-134, 2002.

[92] NATO, STANAG 4691 - VHF/UHF Tactical Communications Standards, NATO Standardization Office, 2016.

[93] T. X. Brown, J. E. James and A. S. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," in *Proc. ACM MobiHoc*, 2006.

[94] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," in *ACM SIGCOMM*, 2003.

[95] K. Scott and S. Burleigh, Bundle Protocol Specification, IETF, 2007.

[96] C. Fu and S. Liew, "TCP Veno: TCP Enhancement for Transmission over Wireless Access Networks," *IEEE Journal on Selected Areas in Communications,* vol. 21, no. 2, pp. 216-228, 2003.

[97] U.S. DoD, Tactical Radio Communications Handbook, Department of Defense, 2021.

[98] S. Mascolo, C. Casetti, M. Gerla, M. Sanadidi and R. Wang, "TCP Westwood: Bandwidth Estimation for Enhanced Transport over Wireless Links," in *Proc. ACM MobiCom*, 2001.

[99] J. Iyengar and M. Thomson, QUIC: A UDP-Based Multiplexed and Secure Transport, IETF, 2021.

[100] E. M. Royer and C. K. Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *IEEE Personal Communications,* vol. 6, no. 2, pp. 46-55, 1999.

[101] I. Chlamtac, M. Conti and J. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," *Ad Hoc Networks,* vol. 1, no. 1, pp. 13-64, 2003.

[102] V. Kawadia and P. R. Kumar, "A Cautionary Perspective on Cross-Layer Design," *IEEE Wireless Communications,* vol. 12, no. 1, pp. 3-11, 2005.

[103] H. Zhai, X. Chen and Y. Fang, "Improving Transport Layer Performance in Wireless Networks by Cross-Layer Design," *IEEE Communications Magazine,* vol. 44, no. 1, pp. 123-129, 2006.

[104] J. Postel, User Datagram Protocol, IETF, 1980.

[105] Y. Liu, H. Zhang, Z. Chen and X. Fu, "AI-Driven Protocol Optimization in Tactical Networks," *IEEE Access,* pp. 12134-12147, 2021.

[106] L. Wood, W. Eddy, P. Holiday, J. McKim and E. Berg, "Delay-Tolerant Networking and the Internet Protocol Suite," *IEEE Communications Magazine,* vol. 45, no. 5, pp. 52-58, 2007.

[107] CCSDS, Space Communications Protocol Specification - Transport Protocol (SCPS-TP), CCSDS 714.0-B-2, 2006.

[108] H. Wang , Y. Liu and M. Li, "Mobile Ad-hoc Networking for Military Applications," *IEEE Communications Magazine,* vol. 58, no. 1, pp. 72-78, 2020.

[109] D. Alberts and R. Hayes, Understanding Command and Control, DoD CCRP (Command and Control Research Program), 2006.

[110] I. Bekmezci, O. K. Sahingoz and S. Temel, "Flying Ad-Hoc Networks (FANETs): A Survey," *Ad Hoc Networks,* vol. 11, no. 3, pp. 1254-1270, 2013.

[111] D. Djenouri, A. Bagula, A. Khelil and M. Balasingham, "Internet of Military Things: Perspectives and Challenges," *IEEE Access,* pp. 9881-9905, 2022.

[112] General Dynamics Mission Systems, "TACLANE-Nano (KG-175N) Datasheet," 2021. [Online].

[113] G. D. M. Systems, «TACLANE Family of Encryptors – Product Overview,» 2020. [Ηλεκτρονικό].

[114] NATO Communications and Information Agency, Cryptographic Modernization Strategy, Brussels, 2022.

[115] O. Bonaventure, C. Paasch and G. Detal, "Multipath TCP: From Theory to Deployment," in *Proc. IFIP Networking*, 2012.

[116] M. Conti, S. Giordano, M. May and A. Passarella, "Mobile Ad Hoc Networking: Overview and Challenges," *Ad Hoc Networks,* pp. 13-64, 2003.

[117] S. Corson and J. Macker , Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, IETF, 1999.

[118] C. Perkins, E. Belding-Royer and S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, IETF, 2003.

[119] S. Basagni, M. Conti, S. Giordano and I. Stojmenovic, Ad Hoc Networking, IEEE Press, 2004.

[120] A. Qayyum, L. Viennot and A. Laouiti, "Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks," in *Proc. HICSS*, 2002.

[121] A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. Boloni and D. Turgut, "Routing Protocols in Ad Hoc Networks: A Survey," *Computer Networks,* vol. 55, no. 3, pp. 3032-3080, 2011.

[122] S. Misra, R. Roy and A. Saha, "Military Applications of Internet of Things: A Review," *IEEE Systems Journal,* vol. 15, no. 1, pp. 14-126, 2021.

[123] S. Kent and K. Seo, Security Architecture for the Internet Protocol, IETF, 2005.

[124] W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 2017.

[125] U.S. DoD CIO, DoD Instruction 8500.01 – Cybersecurity, Department of Defense, 2020.

[126] NSA, Information Assurance Directorate: IPsec Guidance for Military Networks, National Security Agency, 2016.

[127] S. Kent, Encapsulating Security Payload (ESP), IETF, 2005.

[128] S. Kent, Authentication Header(AH), IETF, 2005.

[129] NATO Standardization Office, STANAG 5068 – Interoperability of IP Security Devices, 2010.

[130] NATO Communications and Information Agency, NATO Interoperability Standards and Profiles (NISP), Brussels, 2020.

[131] NSA, High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Specification (HAIPE IS), NSA, 2011.

[132] U.S. DoD, NSA/CSS Policy Manual 3-16: Control of COMSEC Material, U.S. Department of Defense, 2010.

[133] U.S. DoD, Electronic Key Management System (EKMS-1), U.S. Department of Defense, 2012.

[134] General Dynamics Mission System, HAIPE Technology Overview White Paper, General Dynamics Mission Systems, 2018.

[135] NATO, STANAG 4677 – Cryptographic Interoperability of Tactical Networks, NATO Standardization Office, 2014.

[136] U.S. DoD, Key Management Infrastructure (KMI) Overview, Key Management Infrastructure (KMI) Overview, 2018.

[137] General Dynamics Mission Systems, "TACLANE Family of Encryptors – Product Overview," 2020. [Online].

[138] K. Fall και R. Caceres, «Split TCP for Mobile Ad Hoc Networks,» σε *Proc.MILCOM*, 1998.

[139] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Management," in *Proc. IEEE Symposium on Security and Privacy*, 1996.

[140] G. Maral and M. Bousquet, Satellite Communications Systems: Systems, Techniques and Technology, Wiley, 2020.

[141] J. N. Pelton, Satellite Communications in the 5G Era, Springer, 2021.

[142] NATO Standardization Office, NATO STANAG 5066: Profile for HF Radio Data Communications, Brussels: NATO Standardization Office, 2021.

[143] N. S. Office, NATO SATCOM Policy and STANAGs, Brussels: NATO Standardization Office, 2020.

[144] GlobalSecurity.org, "Military Satellite Communications (MILSATCOM)," 2022. [Online]. Available: https://www.globalsecurity.org.

[145] B. Sklar, Digital Communications: Fundamentals and Applications, Prentice Hall, 2021.

[146] A. Molinaro, G. Araniti, A. Iera and F. Rinaldi, "Satellite Communications for Unmanned Aerial Systems: Survey and Future Perspectives," *Computer Networks,* pp. 107-125, 2020.

[147] U.S. DoD CIO, Hybrid SATCOM Networks Strategy, U.S. Department of Defense, 2022.

[148] F. Vallee, "The Role of LEO Constellations in Defence Communications," *Defence Studies Journal,* vol. 25, no. 2, pp. 122-140, 2021.

[149] D. G. Hull, "MILSTAR Communications System Overview," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 30, no. 1, pp. 135-145, 1994.

[150] U. A. Force, Advanced Extremely High Frequency (AEHF) System – Fact Sheet, U.S. Air Force, 2021.

[151] U. Navy, Mobile User Objective System (MUOS) – Official Program Overview, U.S. Navy, 2022.

[152] U. D. o. Defense, Wideband Global SATCOM (WGS) – Fact Sheet, U.S. Department of Defense, 2021.

[153] N. S. Office, "A Guide to STANAGs," 2020. [Online]. Available: https://www.nato.int.

[154] NATO, STANAG 4484 – SHF MILSATCOM Interoperability Requirements, NATO Standardization Office, 2019.

[155] NATO, STANAG 5040 – Interconnection Between National Tactical Communications and NATO NICS, NATO Standardization Office, 2019.

[156] NATO, STANAG 7085 – Standards for ISR Broadcast via Global Broadcast Service (GBS), NATO Standardization Office, 2018.

[157] N. STO, Military SATCOM Technologies and Applications, NATO Science and Technology Organization, 2021.

[158] E. D. Agency, Tactical Communications Beyond Line of Sight, European Defence Agency, 2020.

[159] G. D. M. Systems, Tactical SATCOM Terminals: Operational Resilience in the Field, General Dynamics Mission Systems, 2021.

[160] R. Poisel, Modern Communications Jamming Principles and Techniques, Artech House, 2011.

[161] T. Moltz, The Politics of Space Security, Stanford University Press, 2019.

[162] S. W. Ellingson, Radio Systems for Tactical Communications, Wiley, 2018.

[163] S. Farserotu, R. Prasad and L. Gavrilovska, "Mesh-based Satellite Networks for Tactical Resilience," *IEEE Communications Magazine,* vol. 60, no. 2, pp. 34-40, 2022.

[164] General Dynamics Mission Systems, TACLANE Next-Gen Secure Communications, General Dynamics Mission Systems, 2021.

[165] K. M. Kerns, D. Shepard, J. Bhatti and T. E. Humphreys, "Unmanned Aircraft Capture and Control via GPS Spoofing," *Journal of Field Robotics,* vol. 34, no. 4, pp. 617-636, 2014.

[166] D. A. Center), "Development of Array Receivers with Anti-Jamming and Anti-Spoofing Techniques," in *Proc. ION GNSS+*, Miami, 2019.

[167] A. Humayed, J. Lin, F. Li and B. Luo, "Cyber-Physical Systems Security — A Survey," *IEEE Internet of Things Journal,* vol. 4, no. 6, pp. 1802-1831, 2017.

[168] K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Crown, 2014.

[169] N. C. C. D. C. o. E. (. CCDCOE), Cybersecurity of Military IoT, Tallinn,Estonia: NATO CCDCOE, 2021.

[170] E. (. U. A. f. Cybersecurity), Threat Landscape for the Internet of Things, Athens,Greece: European Union Agency for Cybersecurity, 2022.

[171] A. Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, New York, NY, USA: Doubleday, 2019.

[172] U. D. o. D. (DoD), Department of Defense Strategy for Operating in Cyberspace, Washington, D.C, USA: U.S. Department of Defense, 2018.

[173] E. U. A. f. C. (ENISA), Threat Landscape for the Internet of Things, Athens,Greece: European Union Agency for Cybersecurity, 2022.

[174] N. I. o. S. a. T. (NIST), Zero Trust Architecture (SP 800-207), Gaithersburg,MD,USA: NIST, 2020.

[175] D. Ferraiolo, D. R. Kuhn and R. Chandramouli, Role-Based Access Control, Boston, MA, USA: Artech House, 2003.

[176] S. Team, "IoT layers architecture for connected military network environment," [Online].

[177] E. U. A. f. Cybersecurity(ENISA), Cybersecurity Training and Awareness in the EU, Athens,Greece: European Union Agency for Cybersecurity, 2021.

[178] R. Sommer and V. Paxson, "Outside the Closed World: On Using Machine Learning For Network Intrusion Detection," in *IEEE Symposium on Security and Privacy*, 2010.

[179] M. Lockheed, "Cyber Kill Chain Model," in *Lockheed Martin Corporation*, Bethesda, MD, USA, 2011.

[180] C. (. a. I. S. Agency), Zero Trust Maturity Model v2.0, Washington, DC, USA: Cybersecurity and Infrastructure Security Agency, 2023.

[181] N. S. Office, NATO Cyber Defence and STANAGs, Brussels, Belgium: NATO Standardization Office, 2020.

[182] P. Cornish, D. Livingstone, D. Clemente and C. Yorke, On Cyber Warfare, London, UK: Chatham House, 2010.

[183] N. (. I. o. S. a. Technology), IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A), Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020.

[184] T. Rid, Cyber War Wll Not Take place, Oxford, U.K.: Oxford University Press, 2013.

[185] United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, New York, NY, USA: United Nations, 2021.

[186] NATO, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge, U.K: Cambridge University Press, 2017.

[187] Cloudflare, "DDoS Threat Report, Q2 2023," Cloudflare, 2023. [Online]. Available: https://www.cloudflare.com/.

[188] F. Mandiant, "M-Trends 2022: Insights Into Today's Breach Trends," Mandiant, 2022. [Online]. Available: https://www.mandiant.com.

[189] MITRE, "Zero Day Exploit Reference," MITRE, [Online]. Available: https://attack.mitre.org/.

[190] CISA, Supply Chain Compromise: SolarWinds/SUNBURST, CISA Alerts, 2021.

[191] Verizon, "Data Breach Investigations Report (DBIR)," Verizon, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[192] N. CCDCOE, Cyber and Electronic Warfare in Multi-Domain Operations, Tallinn, Estonia: 2022, 2022.

[193] U. C. Command, About USCYBERCOM, U.S. Cyber Command, 2023.

[194] Mandiant, APT1: Exposing One of China's Cyber Espionage Units, Mandiant Report, 2013.

[195] N. CCDCOE, Annual Report 2022, Tallinn, Estonia: NATO CCDCOE, 2023.

[196] J. Healey, A Fierce Domain: Conflict in Cyberspace, 1986 to 2012, Cyber Conflict Studies Association, 2013.

[197] N. CCDCOE, Mutual Assistance and Information Sharing in Cyberspace, Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2020.

[198] P. Cornish, D. Livingstone, D. Clemente και C. Yorke, Cyber Security and the Strategic Impact of Cyber Attacks, Chatham House, 2010.

[199] VamosSandor, «A Stuxnet fertőzési mechanizmusa,» 2019.

[200] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 2018. [Online].

[201] N. D., «A photograph of a RQ-170 Sentinel at Andersen AFB in Guam on an unknown date.,» 2018.

[202] G. Gonzalez-Granadillo, R. Badonnel, I. Chrisment and M. Festor, "Security Information and Event Management (SIEM): A Review," *International Journal of Information Security,* vol. 20, no. 4, pp. 647-667, 2021.

[203] NIST, Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev.5), 2020.

[204] E. Chew και et al, Contingency Planning Guide for Federal Information Systems, NIST (National Institute of Standards and Technology), 2010.

[205] Splunk, SIEM Architecture for Defense Systems, 2021.

[206] H. Xu and et al, "Blockchain-based secure logging for military communication networks," *IEEE Access,* 2021.

[207] U. D. o. Defense, DoD Data, Analytics, and AI Adoption Strategy, U.S. Department of Defense, 2023.

[208] M. R. Endsley, «Toward a Theory of Situation Awareness in Dynamic Systems,» *Human Factors,* 1995.

[209] R. S. Sutton και A. G. Barto, Reinforcement Learning: An Introduction, 2018.

[210] J. A. Boyan και M. L. Littman, «Packet Routing in Dynamically Changing Networks: A Reinforcement Learning Approach,» σε *NeurIPS (Conference on Neural Information Processing Systems)*, 1994.

[211] V. Chandola , A. Banerjee και V. Kumar, «Anomaly Detection: A Survey,» *ACM Computing Surveys,* 2009.

[212] R. Sommer και V. Paxson, «Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,» σε *IEEE Symposium on Security and Privacy (IEEE S&P)*, 2010.

[213] DAPRA, Explainable Artificial Intelligence (XAI) Program Overview, Defense Advanced Research Projects Agency (DARPA), 2017.

[214] DARPA, OFFSET (OFFensive Swarm-Enabled Tactics) Program Overview, Defense Advanced Research Projects Agency (DARPA), 2017.

[215] S. Pirandola και et al, «Advances in Quantum Cryptography,» *Advances in Optics and Photonics,* 2020.

[216] A. K. Ekert, «Quantum Cryptography Based on Bell's Theorem,» *Physical Review Letters,* 1991.

[217] J. W. Pan και et al, «Satellite-based Entanglement Distribution over 1200km,» *Science,* 2017.

[218] N. S. a. T. Organization, Exploring Quantum-Safe Communications for NATO Networks, Brussels, Belgium: NATO Science and Technology Organization, 2023.

[219] DARPA, Quantum Network Challenge Overview, Washington, D.C.: U.S. Department of Defense, 2020.

[220] 3GPP, 5G Advanced and 6G Technologies for Defense Applications, 3rd Generation Partnership Project (3GPP), 2024.

[221] IEEE, «AI-Driven C4ISR and Network-Centric Warfare Systems Review,» *IEEE Access,* pp. 45780-45799, 2024.