ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEB INTELLIGENCE

Μελέτη των τεχνολογιών επικοινωνίας για περιπτώσεις εκτάκτων καταστάσεων και δικτύων δημόσιας ασφάλειας

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των:

ΑΛΕΞΑΝΔΡΟΥ ΚΑΡΥΠΙΔΗ ΤΟΥ ΝΙΚΟΛΑΟΥ
ΔΗΜΗΤΡΙΟΥ ΝΤΕΝΤΑ ΤΟΥ ΙΩΑΝΝΗ

Επιβλέπων : Δρ. Περικλής Χατζημίσιος
Καθηγητής, ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Φεβρουάριος 2023

Η σελίδα αυτή είναι σκόπιμα λευκή.

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEB INTELLIGENCE

Μελέτη των τεχνολογιών επικοινωνίας για περιπτώσεις εκτάκτων καταστάσεων και δικτύων δημόσιας ασφάλειας

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των:

ΑΛΕΞΑΝΔΡΟΥ ΚΑΡΥΠΙΔΗ ΤΟΥ ΝΙΚΟΛΑΟΥ
ΔΗΜΗΤΡΙΟΥ ΝΤΕΝΤΑ ΤΟΥ ΙΩΑΝΝΗ

Επιβλέπων : Δρ. Περικλής Χατζημίσιος
Καθηγητής ΔΙ.ΠΑ.Ε.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις Choose a date.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Όνομα Επώνυμο Choose an item. ΔΙ.ΠΑ.Ε.	Όνομα Επώνυμο Choose an item. ΔΙ.ΠΑ.Ε.	'Ονομα Επώνυμο Choose an item. ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Φεβρουάριος 2023

(Υπογραφή)

.....

Click here to enter text.

Click here to enter text.

Περίληψη

Η εμπέδωση του αισθήματος ασφαλείας στους πολίτες, η πρόληψη και άμεση επέμβαση σε ανθρωπογενείς και φυσικές καταστροφές, η διαχείριση και αποκατάσταση των συνεπειών που προκαλούν αυτές, η αναζήτηση και ανεύρεση επιζώντων και η διασφάλιση της λειτουργικής συνέχειας των κοινωνικών δομών μετά από τέτοιου είδους γεγονότα, είναι αρμοδιότητες που ανήκουν στον πυρήνα καθηκόντων του προσωπικού της δημόσιας ασφάλειας. Οι πρώτοι ανταποκριτές, ένα ιδιαίτερο κομμάτι του προσωπικού αυτού, συγκεντρώνει σε απόλυτο βαθμό τις λειτουργικές απαιτήσεις εκπλήρωσης των συγκεκριμένων αρμοδιοτήτων. Μια εκ των σημαντικότερων τέτοιων απαιτήσεων που συναρτά άμεσα την άρτια επιχειρησιακή ανταπόκριση των ομάδων αυτών, είναι η επικοινωνία. Η αδιάλειπτη, αποδοτική, διαλειτουργική και ασφαλής επικοινωνία των πρώτων ανταποκριτών, κρίνεται μείζονος σημασίας και σχετίζεται με τη δυνατότητά τους να σώζουν ζωές στο πεδίο. Η συμβολή της τεχνολογία στο ζήτημα της επικοινωνίας για τις υπηρεσίες αυτές είναι καθοριστικής σημασίας και τα πρότυπα που έχουν αναπτυχθεί υποστηρίζουν τις αντίστοιχες εφαρμογές. Ωστόσο και με δεδομένο ότι επιχειρείται σε παγκόσμια κλίμακα η μετάβαση στις πλήρως ευρυζωνικές τεχνολογίες, πραγματοποιήθηκε μια επισκόπηση των υφιστάμενων τεχνολογικών λύσεων, αλλά και αυτών που θα μας απασχολήσουν στο εγγύς μέλλον, στο πλαίσιο της επιλογής των βέλτιστων αρχιτεκτονικών και εφαρμογών για τις κρίσιμες επικοινωνίες.

Στην παρούσα εργασία πραγματοποιήθηκε εκτεταμένη και σε βάθος βιβλιογραφική επισκόπηση τόσο των τεχνολογικών απαιτήσεων των κρίσιμων επικοινωνιών, όσο και των πρωτοκόλλων και προτύπων που υποστηρίζουν αυτές και παρουσιάστηκαν οι υφιστάμενες λύσεις και αρχιτεκτονικές τους, καθώς και οι αντίστοιχες που εκτιμάται ότι θα μας απασχολήσουν στο μέλλον. Στο σημερινό τεχνολογικό περιβάλλον και με δεδομένη την επίσημη πρώτη του 5G από το 2020, άνοιξε ο δρόμος για το όραμα των πλήρως ευρυζωνικών επικοινωνιών, που παρέχουν όλα τα οφέλη των Κρίσιμης Αποστολής Υπηρεσιών (Mission Critical Services – MCX), φωνής, βίντεο και δεδομένων αναβαθμίζοντας ποιοτικά τις σημαντικότερες υπηρεσίες Κρίσιμης Αποστολής Επικοινωνιών Φωνής με το πάτημα ενός πλήκτρου (Mission Critical Push to Talk – MCPTT), που αποτελούν το επικοινωνιακό κύτταρο της δημόσιας ασφάλειας. Οι νέες αρχιτεκτονικές εμπλέκουν αποδοτικά ένα σύνολο καινοτόμων τεχνολογιών που σχετίζονται με εφαρμογές και συσκευές του διαδικτύου των Πραγμάτων (Internet of Things – IoT), νεφοϋπολογιστικής (cloud computing), υπολογιστικής στα άκρα και στο σύννεφο (edge/fog computing), τεχνητής νοημοσύνης (Artificial Intelligence), επαυξημένης και εικονικής πραγματικότητας (Augmented and Virtual Reality) και μηχανικής μάθησης (Machine Learning), αλλά και μια ομάδα περιφερειακών άρτιων τεχνολογικών δομών όπως τα μη επανδρωμένα ιπτάμενα συστήματα (Unmanned Aerial Systems – UASs) και τις επικοινωνίες με αξιοποίηση μη επίγειων ασύρματων δικτύων. Ο συνδυασμός πολλών εξ αυτών στην υλοποίηση δικτύων επικοινωνίας δημόσιας ασφάλειας, οποιουδήποτε εύρους κάλυψης, δημιουργεί πληθώρα προκλήσεων και ανοιχτών ζητημάτων, που η επιστημονική κοινότητα καλείται ν` αντιμετωπίσει.

Φαίνεται ότι η πενταετία 2023 – 2028 θα είναι καθοριστικής σημασίας για τη δημόσια ασφάλεια, καθώς θα ορίσει τον τρόπο με τον οποίο θα συντελεστεί αυτή η τεχνολογική μετεξέλιξη στα δίκτυα που χρησιμοποιούν οι επαγγελματίες. Παράλληλα, καταγράφεται παγκοσμίως μια τάση εξωστρέφειας των υπηρεσιών που παραδοσιακά και με αφορμή ζητήματα ασφαλείας και εμπιστευτικότητας ήταν επιφυλακτικές σε ανοιχτές πηγές. Ενθαρρύνονται οι πολίτες να διαδραματίσουν ενεργό ρόλο και να συνδράμουν τις υπηρεσίες, αναγνωρίζοντας τη δυναμική των μέσων κοινωνικής δικτύωσης, του πληθοπορισμού (crowdsourcing) και του εθελοντισμού. Επιπλέον, οι πλατφόρμες αυτές αντιμετωπίζονται ως φιλόξενος τόπος ανάδειξης και προβολής του έργου τους προς την κατεύθυνση δημιουργίας κλίματος εμπιστοσύνης απέναντι στους θεσμούς που αντιπροσωπεύουν. Ωστόσο, προκύπτει με κάθε βεβαιότητα ότι ο δρόμος προς την πλήρη ευρυζωνικότητα προϋποθέτει την ουσιαστική συμβολή του συνόλου των εμπλεκομένων, είτε αφορούν σε κρατικές υπηρεσίες, φορείς και ενώσεις, είτε σε οργανισμούς και πρωτοβουλίες που με οποιονδήποτε τρόπο σχετίζονται με την υλοποίηση και εξέλιξη των προτύπων επικοινωνίας. Ταυτόχρονα, η πολιτική βούληση, η ενιαία αντιμετώπιση σε επίπεδο κρατών και ηπείρων και η αντίστοιχη οικονομική στήριξη κρίνεται επιβεβλημένη. Απομένει να παρακολουθήσουμε τον τρόπο με τον οποίο όλες αυτές οι πρωτοβουλίες που κινούνται προς την ίδια κατεύθυνση θα συγκλίνουν προς κοινό όφελος.

Τέλος, επιχειρήθηκε μιας σημαντικής αξίας έρευνα για τις ανάγκες των πρώτων ανταποκριτών της χώρας μας σε επικοινωνιακό υλικό και λογισμικό, με την κατάρτιση κατάλληλου ερωτηματολογίου, η οποία φιλοδοξεί να πιστοποιήσει και προτεραιοποιήσει αυτές, ώστε να αποτελέσουν την αιτιολογική βάση στην αντίστοιχη πρόταση για τη χώρα μας.

Λέξεις Κλειδιά: «*Δίκτυα Δημόσιας Ασφάλειας, έκτακτες καταστάσεις, κρίσιμες επικοινωνίες, πρώτοι ανταποκριτές, 5G*»

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

Instilling a sense of security in citizens, preventing and intervening immediately in man-made and natural disasters, managing and restoring the consequences of such disasters, searching for and finding survivors, and ensuring the functional continuity of social structures after such events are core responsibilities of public security personnel. First responders, a particular part of these personnel, concentrate to the fullest extent on fulfilling these responsibilities. One of the most important requirements that directly relates to the perfect operational response of these teams is communication. The uninterrupted, efficient, interoperable, and secure communication of first responders is of major importance and is related to their ability to save lives in the field. The contribution of technology to the issue of communication for these services is crucial, and the standards that have been developed support the corresponding applications. However, given that a global transition to fully broadband technologies is being attempted, an overview of existing technological solutions and those that will be of concern in the near future has been carried out in the context of selecting the best architectures and applications for critical communications.

In this paper, an extensive and in-depth literature review of both the technological requirements of critical communications and the protocols and standards that support them was carried out. The existing solutions and their architectures were presented, as well as those that are expected to be of concern in the future. In today's technological environment, and given the official launch of 5G by 2020, the way has been paved for the vision of fully broadband communications, providing all the benefits of Mission Critical Services (MCX), voice, video, and data by qualitatively upgrading the most important Mission Critical Push to Talk (MCPTT) services, which are the communications cell of public safety. The new architectures efficiently integrate a set of innovative technologies related to the Internet of Things (IoT), cloud computing, edge/cloud computing, and artificial intelligence applications and devices, augmented and virtual reality (AR), and machine learning (ML), but also a group of peripheral technology structures such as unmanned aerial systems (UASs) and communications using non-terrestrial wireless networks. The combination of many of these in the implementation of public safety communication networks of any coverage range creates a multitude of challenges and open issues that the scientific community is called upon to address.

It appears that the five-year period from 2023 to 2028 will be critical for public safety as it will define how this technological evolution will occur in the networks used by practitioners. At the same time, there is a global trend towards outward-looking services that have traditionally been cautious about open sources on the occasion of security and confidentiality issues. Citizens are encouraged to play an active role and assist services, recognizing the potential of social media, crowdsourcing, and volunteering. In addition, these platforms are seen as a welcoming place to showcase and promote their work to build trust in the institutions they represent. However, it is clear that the road to full broadband requires a substantial contribution from all stakeholders, whether they are government departments, bodies and associations, or organizations and initiatives that are in any way related to the implementation and development of communication standards. At the same time, political will, a unified approach at the national and continental level, and

corresponding financial support are essential. It remains to be seen how all these initiatives moving in the same direction will converge for the common good.

Finally, an important research on the communication material and software needs of our country's first responders was attempted, with the preparation of an appropriate questionnaire that aspires to certify and prioritize them, in order to form the rationale for the corresponding proposal for our country.

Keywords: «*Public Safety Networks (PSNs), emergency situations, critical communications, First responders (FR), 5G»*

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1 Εισαγωγή 1

1.1 Η έννοια της ασφάλειας 1

1.2 Ζητήματα επικοινωνίας στη δημόσια ασφάλεια 4

1.2.1 Η πορεία μέχρι την πρόταση 5

1.3 Οργάνωση κειμένου 6

2 Δημόσια Ασφάλεια 8

2.1 Φυσικές καταστροφές 10

2.2 Ανθρωπογενείς καταστροφές 13

2.3 Ασύμμετρες απειλές 17

2.4 Διαχείριση του κινδύνου 20

2.5 Απαιτήσεις στις επικοινωνίες δημόσιας ασφάλειας 28

2.5.1 Γενικές - λειτουργικές απαιτήσεις 28

2.5.2 Τεχνολογικές απαιτήσεις 30

2.5.2.1 Στιβαρότητα, αξιοπιστία και βασικές προδιαγραφές 32

2.5.2.2 Απόλυτη ασφάλεια 34

2.5.2.3 Διαλειτουργικότητα 35

2.5.2.4 Απαιτήσεις υλικού και λογισμικού 36

2.5.2.5 Οικονομικές πτυχές 37

2.6 Η ιδιαίτερη κατηγορία των πρώτων ανταποκριτών 38

2.7 Πρώτοι ανταποκριτές στην Ελλάδα – Διεξαγωγή έρευνας 42

2.7.1 Ερωτηματολόγιο 42

2.7.2 Παρόμοιες έρευνες 43

3 Οργανισμοί και Ενώσεις 45

3.1 Διεθνείς Οργανισμοί 47

3.1.1 Διεθνής Ένωση Δημόσιας Ασφάλειας 47

3.1.2 Ένωση Υπαλλήλων Επικοινωνιών Δημόσιας Ασφάλειας 47

3.1.3 Πρωτοβουλία του Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών 47

3.1.4 Έργο Συνεργασίας Τρίτης Γενιάς 48

3.1.5 Αμερικανικό Εθνικό Ινστιτούτο Προτύπων 49

3.1.6 Διεθνής Ένωση Τηλεπικοινωνιών 49
3.1.7 Η Ένωση Κρίσιμων Επικοινωνιών 50
3.1.8 Πληροφοριακά Συστήματα Αντιμετώπισης και Διαχείρισης Κρίσεων 50
3.1.9 Ένωση Κινητών Δικτύων Επικοινωνίας Επόμενης Γενιάς 50
3.2 Ευρωπαϊκοί Οργανισμοί 51
3.2.1 Επικοινωνίες για τη Δημόσια Ασφάλεια στην Ευρώπη 51
3.2.2 Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων 52
3.2.3 Ευρωπαϊκή Ένωση Αριθμών Έκτακτης Ανάγκης 52
3.2.4 EURESCOM 52
4 Τεχνολογίες στις κρίσιμες επικοινωνίες 54
4.1 Land Mobile Radio System 58
4.2 Long Term Evolution 60
4.2.1 Ιστορικό 60
4.2.2 Βασικά στοιχεία αρχιτεκτονικής του LTE 62
4.2.3 Βασικά τεχνικά χαρακτηριστικά του LTE 67
4.2.4 Πλεονεκτήματα και μειονεκτήματα του LTE 67
4.3 4G 70
4.4 5G 73
4.4.1 Κύρια χαρακτηριστικά του 5G 74
4.4.2 Ενισχυμένη Κινητή Ευρυζωνικότητα 74
4.4.2.1 Μαζικό Διαδίκτυο των Πραγμάτων (massive IoT - mIoT) 75
4.4.2.2 Υπηρεσίες Κρίσιμης Αποστολής (Mission Critical Services - MCS) 75
4.4.2.3 Φάσμα και συχνότητες λειτουργίας του 5G 75
4.4.2.4 Αρχιτεκτονική Δικτύου 5G 76
4.4.2.5 Ιδεατοποίηση Λειτουργίας Δικτύου (Network Function Virtualization - NVF) 76
4.4.2.6 Δικτύωση καθορισμένη με λογισμικό (SDN) 77
4.4.2.7 Δίκτυο Πυρήνα 78
4.4.2.8 Δίκτυο Ραδιοπρόσβασης Επόμενης Γενιάς 80
4.4.3 Συγκριτικά χαρακτηριστικά του 5G, με το 4G και 3G 82
4.4.4 Το 5G στα Δίκτυα Δημόσιας Ασφάλειας 86
4.4.5 5G Μελέτες περίπτωσης 88
4.4.5.1 Δασοπυρόσβεση 88
4.4.5.2 Εκπαίδευση σε εικονικό περιβάλλον 89

4.4.5.3 Εντοπισμός στίγματος σε εσωτερικό χώρο με χρήση 5G και UAVs ... 90
4.5 Software Defined Radio ... 91
4.6 Cognitive Radio ... 95
4.7 Device to Device ... 99
4.8 M-MIMO ... 103
4.9 Millimetre wave (mmWave) ... 107
4.10 Internet of Things ... 111
4.10.1 Πρωτόκολλα δικτύωσης ... 115
4.10.2 Πρωτόκολλα επιπέδου εφαρμογής ... 120
4.11 Cloud, Fog, Edge Computing ... 123
4.11.1 Cloud Computing. ... 124
4.11.2 Edge Computing ... 127
4.11.3 Fog Computing. ... 129
4.12 Unmanned Aerial Vehicle ... 131
4.13 Optical Communications ... 137
4.13.1 Γενικά ... 137
4.13.2 Ο ρόλος των οπτικών επικοινωνιών στη δημόσια ασφάλεια ... 139
4.13.3 Το μέλλον των οπτικών επικοινωνιών ... 143
4.14 Φάσμα ραδιοσυχνοτήτων (spectrum) ... 143
5 Θέματα υλοποίησης ... 147
5.1 Επίπεδο Αντίληψης ... 149
5.1.1 Δεδομένα από αισθητήρες ... 149
5.1.2 Δεδομένα από συμμετοχή πολιτών ... 152
5.1.2.1 Μέσα κοινωνικής δικτύωσης ... 152
5.1.2.2 Ενιαίος αριθμός κλήσης έκτακτης ανάγκης ... 156
5.2 Επίπεδο δικτύου ... 161
5.2.1 Επίγεια δίκτυα ... 161
5.2.1.1 Επικοινωνίες στενής ζώνης (Narrowband) ... 162
5.2.1.2 Επικοινωνίες ευρείας ζώνης (wideband) ... 189
5.2.1.3 Πλήρως ευρυζωνικές επικοινωνίες (broadband) ... 195
5.2.2 Μη επίγεια δίκτυα ... 222
5.2.2.1 Δορυφορικά δίκτυα ... 222
5.2.2.2 Συστήματα Πλατφόρμας Μεγάλου Υψομέτρου ... 228

5.2.2.3 Συστήματα Πλατφόρμας Χαμηλού Υψομέτρου ... 238
5.3 Επίπεδο χρήστη ... 252
5.3.1 Εξοπλισμός ... 253
5.3.1.1 Έξυπνα κινητά τηλέφωνα (smartphones) ... 256
5.3.1.2 Φορητοί υπολογιστές – υπολογιστές ταμπλέτες (laptops - tablets) ... 258
5.3.1.3 Ενδυτά μέσα (wearables) ... 258
5.3.2 Υπηρεσίες (MCx) ... 262
5.3.2.1 Φωνητικές υπηρεσίες (MC-PTT) ... 263
5.3.2.2 Υπηρεσίες μετάδοσης εικόνων (MC-Video) ... 264
5.3.2.3 Υπηρεσίες μετάδοσης δεδομένων (MC-Data) ... 265
5.3.3 Εμπλεκόμενες τεχνολογίες ... 267
5.4 Επίπεδο Επεξεργασίας Δεδομένων ... 269
5.4.1 Διοίκηση και έλεγχος ... 269
5.4.2 Επίγνωση της κατάστασης ... 271
5.5 Επίπεδο εφαρμογών ... 273
5.5.1 Έλεγχος και ομαδοποίηση δεδομένων ... 274
5.5.1.1 Υπολογισμός αιχμής πολλαπλής πρόσβασης (MEC) ... 274
5.5.1.2 Συγχώνευση δεδομένων (Data Fusion) ... 275
5.5.2 Αξιολόγηση και αξιοποίηση πληροφοριών ... 276
5.5.2.1 Συστήματα διαχείρισης αρχείων (Records Management Systems - RMSs) ... 276
5.5.2.2 REST APIs ... 278
5.6 Ασφάλεια ... 280
5.6.1 Απειλές ... 281
5.6.2 Λύσεις ... 283
5.6.3 Ποιότητα Υπηρεσίας (QoS) ... 285
6 Βέλτιστες Πρακτικές ... 287
6.1 Τεχνολογίες, αρχιτεκτονικές και έργα διαφόρων χωρών ... 288
6.1.1 Ευρώπη ... 289
6.1.1.1 Βέλγιο ... 289
6.1.1.2 Ηνωμένο Βασίλειο ... 293
6.1.1.3 Γαλλία ... 296
6.1.1.4 Φινλανδία ... 299
6.1.2 Αμερική ... 303
6.1.2.1 Ηνωμένες Πολιτείες Αμερικής ... 303

6.1.3 Ασία – Ειρηνικός 303
6.1.3.1 Αυστραλία 303
6.1.3.2 Δημοκρατία Νότιας Κορέας 306
6.2 Συγκριτική αξιολόγηση – βέλτιστες πρακτικές 311
6.3 Σπουδαιότητα της προτυποποίησης 313
7 Επίλογος 316
7.1 Σύνοψη και συμπεράσματα 317
7.2 Μελλοντικές επεκτάσεις 319
Βιβλιογραφία 322

Πίνακας εικόνων

Εικόνα 1. Ιεραρχία των ανθρώπινων αναγκών κατά Maslow 1
Εικόνα 2. Είδη καταστροφών [14] 11
Εικόνα 3. Ποσοστιαία επί τις εκατό αποτύπωση των φυσικών καταστροφών και των συνεπειών τους, ανά ήπειρο (1ο εξάμηνο 2022) [16] 12
Εικόνα 4. Ποσοστιαία επί τις εκατό αποτύπωση των φυσικών καταστροφών και συνεπειών τους ανά είδος (1ο εξάμηνο 2022) [16].....13
Εικόνα 5. Συγκριτική μελέτη καταστροφών ανά είδος 2021 με εικοσαετία (2001-2020) [17]13
Εικόνα 6. Τεχνολογικές καταστροφές το διάστημα 1900-2022, συγκριτικά με τα αντίστοιχα των 50 τελευταίων ετών [13].....16
Εικόνα 7. Τεχνολογικές καταστροφές [21] 16
Εικόνα 8. Οι στόχοι και προτεραιότητες του προγράμματος - πλαισίου Sendai [9].....22
Εικόνα 9. Χρηματοδότηση της πολιτικής συνοχής της Ευρωπαϊκής Ένωσης για την πρόληψη και διαχείριση κινδύνων το 2014-2022 [34] 24
Εικόνα 10. Ταμείο συνοχής 2021 – 2027. Συνολικές δαπάνες [34].....24
Εικόνα 11. Ταμείο συνοχής 2021 – 2027. Δαπάνες ανά κράτος συμμετοχής [34] 25
Εικόνα 12. Κύκλος διαχείρισης καταστροφών.....26
Εικόνα 13. Παγκόσμιος δείκτης ανθρώπινης ανάπτυξης [36] 27
Εικόνα 14. Ιεραρχία των αναγκών των πρώτων ανταποκριτών [10] 38
Εικόνα 15. Εφαρμογές δημόσιας ασφάλειας [44] 39
Εικόνα 16. Αποτελέσματα έρευνας που διεξήχθη το 2020 στους πρώτους ανταποκριτές των Η.Π.Α. από το NIST [47] 44
Εικόνα 17. Συνοπτικός διαδραστικός χάρτης των οργανισμών που απασχολούνται με τη δημόσια ασφάλεια 46
Εικόνα 18. Επιθυμητά χαρακτηριστικά των δικτύων δημόσιας ασφάλειας [49], [50].....55
Εικόνα 19. Τεχνολογίες ενεργοποίησης των δικτύων δημόσιας ασφάλειας: (a)Land Mobile Radio System, (b)Long Term Evolution, (c)Software Defined Radio, (d)Cognitive Radio, (e)Device-to-Device, (f) Multiple Input Multiple Output, (g)Millimeter Wave, (i)Internet of Things, (j)Unmanned Air Vehicle [49] 56
Εικόνα 20. Τεχνολογίες και συσχετίσεις χρηστών δημόσιας ασφάλειας [53] 58
Εικόνα 21. Τυπική αρχιτεκτονική διάταξη δικτύου LMR για PSN [55].....59
Εικόνα 22. LTE Network Architecture [43].....62
Εικόνα 23. LTE functional architecture [57].....64
Εικόνα 24. 4G LTE ενοποίηση διαφορετικών τεχνολογικών προτύπων σε PSN [51].....72

Εικόνα 25. Χάρτης ανάπτυξης εμπορικών δικτύων 5G [70].....73
Εικόνα 26. Το όραμα του ITU για το 5G. ITU-R M.2083 [72].....74
Εικόνα 27. Προδιαγραφές της Διεθνούς Κινητής Τηλεπικοινωνίας (International Mobile Telecommunications IMT-2020) γνωστές και ως 5G [73].....75
Εικόνα 28. Οι ζώνες συχνοτήτων του 5G [74].....77
Εικόνα 29. NVF πλαίσιο [75].....77
Εικόνα 30. Αρχιτεκτονική SDN [75] 78
Εικόνα 31. Αρχιτεκτονική Πυρήνα Δικτύου 5G [75].....80
Εικόνα 32. NG-RAN κεντροποιημένο και κατανεμημένο σύστημα [77] 81
Εικόνα 33. Τα στάδια ολοκλήρωσης της 17ης έκδοσης. Πηγή: 3GPP [78].....81
Εικόνα 34. 5G Ζώνες λειτουργίας σε διαφορετικές χώρες. Πηγή: Devopedia [85].....84
Εικόνα 35. Ενεργειακή απόδοση ως συνάρτηση της (α) απόστασης μεταξύ κάθε RAN και της έξυπνης συσκευής του χρήστη και (β) αριθμό έξυπνων συσκευών [80].....84
Εικόνα 36. Λύσεις κάλυψης 5G NR για την παροχή απεριόριστης συνδεσιμότητας για τις επικοινωνίες MC δημόσιας ασφάλειας [69].....89
Εικόνα 37. NIST Κέντρο Δοκιμών Δημόσιας Ασφάλειας Καθηλωτικής Εμπειρίας [95].....90
Εικόνα 38. Σενάριο 3D αποτύπωσης θέσης σε εσωτερικό χώρο με τη χρήση UAVs [69].....91
Εικόνα 39. Διεπαφές διαλειτουργικότητας SDR [99] 93
Εικόνα 40. Το σύστημα των συστημάτων με υλοποίηση τεχνολογία SDR [99].....94
Εικόνα 41. Βασικοί ραδιομηχανισμοί για δίκτυο αντιμετώπισης καταστροφών [37] 97
Εικόνα 42. Αρχιτεκτονική CRN [105] 97
Εικόνα 43. Αρχιτεκτονική PSN βασισμένη σε D2D επικοινωνίες [124].....100
Εικόνα 44. Μοντέλο δικτύου που εξετάζει 3 διαφορετικά σενάρια D2D επικοινωνίας [125] 102
Εικόνα 45. Κατηγοριοποίηση επικοινωνιών D2D από την πλευρά του χρήστη [126] 102
Εικόνα 46. Τρισδιάστατη διαμόρφωση δέσμης σε M-MIMO 5G [130].....105
Εικόνα 47. Το 5G mmWave παρέχει σημαντική αύξηση χωρητικότητας με πρόσθετο φάσμα [134] 109
Εικόνα 48. mmWave συχνοτήτων κυμάτων που χρησιμοποιούνται από ορισμένες χώρες [134] 110
Εικόνα 49.Το ηλεκτρομαγνητικό φάσμα 5G mmWave και άλλων σημάτων ραδιοφώνου ...110
Εικόνα 50. Ετερογενές δίκτυο που περιλαμβάνει microcells, microcells WLANs, picocells σε 60GHz 111
Εικόνα 51. Επίπεδα αρχιτεκτονικής του IoT [51], [143].....113
Εικόνα 52. Σενάρια εφαρμογών IoT για τη δημόσια ασφάλεια [140] 114
Εικόνα 53. Οφέλη του IoT στη δημόσια ασφάλεια, ανάλογα με το επίπεδο ενοποίησης [146] 114

Εικόνα 54. Οι πόλεις μεγαλώνουν - Smart Cities [167] 123
Εικόνα 55. Διαφορετικοί τύποι νεφοϋπολογιστικής [168] 125
Εικόνα 56. Αρχιτεκτονική που εμπλέκει τη νεφελοϋπολογιστική [171] 126
Εικόνα 57. Παράδειγμα υπολογιστικής ακμής [175] 128
Εικόνα 58. Edge Computing [167] 128
Εικόνα 59. (α) Το cloudlet περιλαμβάνει υπολογιστική υποδομή εγγύτητας που μπορεί να αξιοποιηθεί από κινητές συσκευές (β) Βασικές διαφορές cloudlet και cloud computing [177]. 129
Εικόνα 60. Σύνδεση κόμβων fog computing σε μια έξυπνη πόλη [182] 130
Εικόνα 61. PSN με τη βοήθεια UAVs [44] 132
Εικόνα 62. Είδη των UAVs [44] 132
Εικόνα 63. Πεδίο εφαρμογής της τεχνολογίας επικοινωνίας με drones [187] 133
Εικόνα 64. Προκλήσεις υλοποίησης PSNs με εμπλοκή UAVs [50] 136
Εικόνα 65. Ενδεικτικά ζητήματα προκλήσεων υλοποίησης PSN με εμπλοκή UAVs: (a)Τοποθέτηση 3D [188] και (b)Σχεδιασμός τροχιάς [189]. 136
Εικόνα 66. Κατηγοριοποίηση UAVs με βάση τις εφαρμογές, το υψόμετρο και την υποδομή δικτύου [186]. 136
Εικόνα 67. Με κόκκινο οι συνδέσεις FSO Communication ανάμεσα στους σταθμούς, πηγή:NASA 138
Εικόνα 68. Υποθαλάσσιο δίκτυο αισθητήρων με χρήση οπτικών επικοινωνιών σε συνεργασία με επίγειο και δορυφορικό δίκτυο ραδιοεπικοινωνιών [201] 139
Εικόνα 69. Σενάρια χρήσης FSOC με στοιχεία από [200] 142
Εικόνα 70. Εννοιολογικός χάρτης των πέντε (5) επιπέδων των αρχιτεκτονικών των Δικτύων Δημόσιας Ασφάλειας και των στοιχείων που τα συνθέτουν 148
Εικόνα 71. Εφαρμογές επιπέδου αντίληψης [215] 149
Εικόνα 72. Ανάλυση βίντεο κάμερας ασφαλείας σε πραγματικό χρόνο [217] 150
Εικόνα 73. Διαφορετικοί τύποι αισθητήρων [218] 151
Εικόνα 74. Διαφορετικές κατηγορίες αισθητήρων [219] 151
Εικόνα 75. Περίπτωση μαζικών πυροβολισμών σε σχολείο - 5G MEC Network [220] 152
Εικόνα 76. Στατιστικά στοιχεία χρηστών των μέσων κοινωνικής δικτύωσης έως Ιανουάριο 2023 [222] 153
Εικόνα 77. Έξυπνο πλαίσιο δημόσιας ασφάλεια SPSF [221]. 154
Εικόνα 78. Στιγμιότυπο της πλατφόρμας Vizsafe’s Geoaware Network [230] 155
Εικόνα 79. Διαχείριση περιστατικών και επίγνωση της κατάστασης [230] 155
Εικόνα 80. Χάρτης αποτύπωσης αναφορών για ανθρώπους που χρειάζονατι βοήθεια – Σεισμός Αιτή [229] 156
Εικόνα 81. Περίπτωση μαζικών πυροβολισμών σε σχολείο [220] 156

Εικόνα 82. Αρμόδιοι φορείς παροχής υπηρεσιών έκτακτης ανάγκης [232] 157
Εικόνα 83. Ροή κλήσης στο 911 [240] 160
Εικόνα 84. Χειρισμός κλήσης από το κέντρο έκτακτης ανάγκης "911" [57].....161
Εικόνα 85. Επιλογή τεχνολογίας λειτουργίας του Project 25 [242].....164
Εικόνα 86. Αρχιτεκτονική του δικτύου P25 [57] 167
Εικόνα 87. Υπηρεσίες του P25 [244] 168
Εικόνα 88. P25: Δέκα κορυφαία οφέλη [245].....170
Εικόνα 89. Χώρες που χρησιμοποιούν την πλατφόρμα P25 για δίκτυα δημόσιας ασφάλειας 170
Εικόνα 90. Αρχιτεκτονική του δικτύου TETRA [59].....173
Εικόνα 91. Κύρια στοιχεία και διεπαφές δικτύου TETRA [252].....174
Εικόνα 92. Αποτελεσματικότητα TDMA στο TETRA [253] 175
Εικόνα 93. Αρχιτεκτονική προτύπου DMR [57].....178
Εικόνα 94. DMR αρχιτεκτονική συστήματος κορμού [258].....179
Εικόνα 95. Αξιοποίηση φάσματος - καναλιών ψηφιακής και αναλογικής λειτουργίας του DMR [261] 180
Εικόνα 96. Βελτίωση εύρους με DMR σε σύγκριση με αναλογικό [256].....180
Εικόνα 97. Βελτίωση εύρους με DMR σε σύγκριση με αναλογικό [261].....182
Εικόνα 98. Πρότυπο NXDN [267] 184
Εικόνα 99. Διαγραμματική απεικόνιση δυνατοτήτων dPMR 185
Εικόνα 100. Επιχειρησιακή εξέλιξη του TETRA [253] 191
Εικόνα 101. Συγκριτική αποτύπωση ρυθμού δεδομένων TETRA Release 1 και Release 2 [283] 191
Εικόνα 102. Περίπτωση χρήσης: Nødnett TEDS [285] 192
Εικόνα 103. Αντιστοίχιση προτύπων 3GPP και εκδόσεων TETRA [286].....193
Εικόνα 104. MESA Project [290].....194
Εικόνα 105. Μέγεθος της αγοράς για το TETRA, το διάστημα 2017-2027 [292].....194
Εικόνα 106. Πορεία από την αναλογική στην ψηφιακή τεχνολογία [46] 196
Εικόνα 107. FirstNet, υπηρεσίες εξυπηρέτησης ανά οικονομικό έτος.....198
Εικόνα 108. Αρχιτεκτονική LTE για το FirstNet [148].....199
Εικόνα 109. Βασικοί τομείς του δικτύου FirstNet 200
Εικόνα 110.Λύσεις ιδιωτικού δικτυου (PNS) [306].....201
Εικόνα 111. Αδειοδοτημένη ζώνη φάσματος του FirstNet [308] 202
Εικόνα 112. Compact Rapid Deployable (CRD) / Cell on Wheels (COW) -FirstNet 203
Εικόνα 113. (a) Flying COW, (b) SatCOLT, (c) FirstNet One 204
Εικόνα 114. Τεχνολογίες ενεργοποίησης 5G για το FirstNet [10].....205
Εικόνα 115. BroadMap [321].....208

Εικόνα 116. Από το BroadMap, στο BroadWay, στο BroadNet [322] 211
Εικόνα 117. Επιχειρησιακή κινητικότητα του έργου, από το BroadWay στο BroadNet [330] 211
Εικόνα 118. Αρχιτεκτονική SpiceNet [331].....212
Εικόνα 119. Αρχιτεκτονική (a)MCX, (b)X/BELLO, (c)MAESTRO.....215
Εικόνα 120. Αρχιτεκτονική του συστήματος RESPOND-A [332] 215
Εικόνα 121. Χώρες της ΕΕ που συμμετέχουν στο Respond-A Project.....216
Εικόνα 122. Οι Ζώνες δορυφορικών συχνοτήτων (πηγή: European Space Agency – ESA) .226
Εικόνα 123. Σύνδεση με το Δορυφόρο και αποστολή μηνύματος (πληροφορίες).....228
Εικόνα 124. HAPS στη στρατόσφαιρα 229
Εικόνα 125. Airbus HAPS Zephyr, 2022 229
Εικόνα 126. HAPS. Περιοχή παροχής υπηρεσίων. Πηγή: ITU Report F.2439-01 230
Εικόνα 127. Υψομετρικά όρια ενός HAPS 230
Εικόνα 128. Σενάριο Κάλυψης HAPS - Δυναμικός σχηματισμός ακτίνων εκπομπής.....231
Εικόνα 129. Οι τρεις τύποι των HAPS (Αερόστατο, Αερόπλοιο και Αεροσκάφος).....233
Εικόνα 130. ITU Περιοχές χάρτη 1,2,3 [372] 234
Εικόνα 131. Χρήση HAPS σε περιοχή με μερικώς κατεστραμμένη επικοινωνιακή υποδομή. LTE, 5G, NR, 3GPP, Rel,17 (NTN).....237
Εικόνα 132. Διαφορετικοί τύποι LAPs [383].....238
Εικόνα 133. Διάφορα είδη LAPs.....242
Εικόνα 134. Αερόστατο Skymesh- Χρήση και αρχιτεκτονική.....247
Εικόνα 135. Υποστήριξη επιχειρήσεων έρευνας και διάσωσης.....247
Εικόνα 136. Εγκατάσταση του συστήματος.....248
Εικόνα 137. Προβλεπόμενες περιοχές κάλυψης για ύψος 440m [390].....248
Εικόνα 138. Αρχιτεκτονική του συστήματος EBAN 249
Εικόνα 139. Αερόπλοιο Ζέπελιν 250
Εικόνα 140. Αερόπλοιο τύπου Eagle Owl της Γαλλικής εταιρείας CNIM 251
Εικόνα 141. Τυπικές απαιτήσεις ευρυζωνικής συσκευής MC [396].....253
Εικόνα 142. Διάφοροι τύποι ραδιοπομποδεκτών (α)P25 radiotης L3HARRIS, (β)TETRA radio της Hytera, (γ)TETRAPOL radio της Airbus και (δ)NXDN radio/analog της KENWOOD 254
Εικόνα 143. Πλήρες σύστημα P25 που παρέχει ραδιοπομποδέκτη, κονσόλα οχήματος και σύνδεσή του με tablet και smartphone από την L3HARRIS.....254
Εικόνα 144. Πλήρες σύστημα NXDN και DMR της KENWOOD.....255
Εικόνα 145. Σύστημα TETRA SmartOne της Hytera 255
Εικόνα 146. Εικονική επίσκεψη σε κέντρο ελέγχου FREQUENTIS 256
Εικόνα 147. Smartphone για PS της Bittium - Υπηρεσία MCPTT 257

Εικόνα 148. Smartphone για PS της Bittium - Υπηρεσία MCVideo 258
Εικόνα 149. Smartphone για PS της Bittium - Διασύνδεση του smartphone με laptop.....258
Εικόνα 150. Παραδείγματα ορισμένων φορητών συσκευών υγείας. (1)Αισθητήρας αυτιού (2)Φακοί επαφής (3)BioPatch (4)Έξυπνο ρολόι (5)Ζώνη καρδιακών παλμών (6)Βιομετρικό ρούχο (7)Παρακολούθηση δραστηριότητας [401].....261
Εικόνα 151. Body Camera (συσκευή, σημείο που φέρεται, εικόνα που δίνει) [403].....261
Εικόνα 152. Ένδυτα μέσα (wearables) [404], [405].....261
Εικόνα 153. Διαφορετικά είδη ένδυτων μέσων και αισθητήρων υγείας [401] 262
Εικόνα 154. Παραδείγματα ένδυτων μέσων για τη δημόσια ασφάλεια [398].....262
Εικόνα 155. 3GPP Releases for MCx [407].....263
Εικόνα 156. Έξυπνα κινητά και tablets για επικοινωνίες MCPTT στη δημόσια ασφάλεια [409] 264
Εικόνα 157. Υπηρεσίες μετάδοσης εικόνων [407].....265
Εικόνα 158. Υπηρεσίες μετάδοσης δεδομένων [407] 266
Εικόνα 159. Μοντέλο επικοινωνιών πολιτών και πρώτων ανταποκριτών με το κέντρο ελέγχου και διοίκησης [410] 266
Εικόνα 160. Αρχιτεκτονική του συστήματος επικοινωνίας PPDR [411].....267
Εικόνα 161. Ενδεικτικές κατηγορίες εφαρμογών για τη δημόσια ασφάλεια [412].....268
Εικόνα 162. Ο επαγγελματίας δημόσιας ασφάλειας του σήμερα και του μέλλοντος [140]...269
Εικόνα 163. Χαρακτηριστικά στιγμιότυπα κέντρου διοίκησης και ελέγχου και λειτουργικότητες αυτών – Hytera Command and Control center 271
Εικόνα 164. Στάδια μέχρι τη λήψη απόφασης σε ένα PSN.....272
Εικόνα 165. Επίγνωση της κατάστασης με αναδρομολόγηση δεδομένων θέσης, ταχύτητας, χώρου σε πραγματικό χρόνο και χρήση συστήματος 5G MEC [414].....273
Εικόνα 166. Τυπική αρχιτεκτονική ενός PSN [415] 274
Εικόνα 167. Κύρια χαρακτηριστικά των συστημάτων RMS [420].....278
Εικόνα 168. Παράδειγμα RMS συστήματος και στιγμιότυπο οθόνης – RIMS RMS [420] ..278
Εικόνα 169. Πηγές δεδομένων και υπηρεσίες του GeoServer REST API 280
Εικόνα 170. Διασυνδεδεμένες υπηρεσίες δημόσιας ασφάλειας στο πεδίο [423].....281
Εικόνα 171. Αρχιτεκτονική ασφαλείας για ασφάλεια δικτύου από άκρο σε άκρο [428].....284
Εικόνα 172. Κρίσιμες επικοινωνίες σε τέσσερις Ηπείρους.....289
Εικόνα 173. Σχηματική αναπαράσταση του δικτύου ASTRID TETRA (512 BS) 290
Εικόνα 174. Η κάλυψη του δικτύου ASTRID TETRA (523 B.S.) 292
Εικόνα 175. ESN χρήση smartphone από στελέχη της βρετανικής αστυνομίας [437] 293
Εικόνα 176. Δίκτυο υπηρεσιών έκτακτης ανάγκης της BT [437].....294
Εικόνα 177. Πρακτική χρήση του MOCN στο ESN [440] 296
Εικόνα 178. Γεωγραφική κάλυψη του δικτύου VIRVE (2020) 301

Εικόνα 179. Προγραμματισμός γεωργραφικής κάλυψης δικτύου VIVRE2 [447].....301
Εικόνα 180. VIVRE 2. Οδικός χάρτης του έργου [452] 303
Εικόνα 181. Πρόγραμμα Mobile Black Spot - Χρηματοδοτούμενοι σταθμοί βάσης. Φάση 5 [456] 304
Εικόνα 182. Η αρχιτεκτονική του SafeNet [462].....308
Εικόνα 183. Οι φάσεις ολοκλήρωσης του SafeNet [462] 309
Εικόνα 184. Κέντρο Daegu [464].....309
Εικόνα 185. Κέντρο Daegu - Θωρακισμένο δωμάτιο [464].....309
Εικόνα 186. Κέντρο Σεούλ [464] 310
Εικόνα 187. Το δένδρο της προτυποποίησης (ασύρματες επικοινωνίες 1990 - 2020) [51]...314

Πίνακας πινάκων

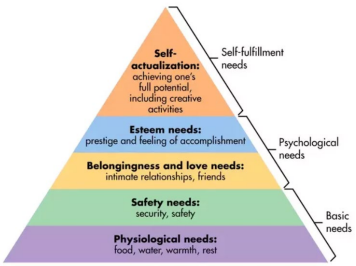
Πίνακας 1. Τεχνολογικά ορόσημα των εκδόσεων του 3GPP έως την 12η έκδοση 61
Πίνακας 2. Συγκριτικά στοιχεία τεχνολογικών εξελίξεων έως το LTE-A 61
Πίνακας 3. Κύρια τεχνολογικά χαρακτηριστικά του LTE 69
Πίνακας 4. 3GPP Releases σχετικά με το LTE [57].....70
Πίνακας 5. Δυνατότητες LTE-Advanced [67].....70
Πίνακας 6. Συγκριτικά στοιχεία των διαφορετικών γενιών δικτύων κινητής τηλεφωνίας [66] 72
Πίνακας 7. Χαρακτηριστικά Ποιότητας Υπηρεσιών QoS Κρίσιμης Αποστολής MC με βάση το πρότυπο 3GPP [69].....87
Πίνακας 8. Απαιτήσεις PSNs και είδη υπηρεσιών [91].....88
Πίνακας 9. Προγράμματα – έργα που σχετίζονται με το CR και το PPDR [37].....98
Πίνακας 10. Φορείς που εμπλέκονται στην αρχιτεκτονική IoT και σκοπός που επιτελείται [146] 122
Πίνακας 11. Συγκριτικά στοιχεία υπολογιστικής σύννεφου και άκρων [175].....128
Πίνακας 12. Προγράμματα της NASA με χρήση FSO επικοινωνιών.....138
Πίνακας 13. Ραδιοφάσμα δημόσιας ασφάλειας στις Η.Π.Α. 145
Πίνακας 14. Μη αδειοδοτημένη κατανομή φάσματος στις Η.Π.Α. 146
Πίνακας 15. Αδειοδοτημένη κατανομή φάσματος στις Η.Π.Α. [214] 146
Πίνακας 16. Συχνότητες κατά ITU.....146
Πίνακας 17. Χαρακτηριστικά που ικανοποιεί η συμβατική και επίγεια λειτουργία του P25 [243] 165
Πίνακας 18. Βασικές προδιαγραφές ραδιοδικτύου TETRA 174
Πίνακας 19. Τεχνικά χαρακτηριστικά προτύπων επικοινωνίας TETRA, TETRAPOL, DMR 189
Πίνακας 20. Ρυθμοί δεδομένων που υποστηρίζει το TEDS ανά εύρος καναλιών και διαμόρφωση [248].....191
Πίνακας 21. Τεχνικά χαρακτηριστικά προτύπων TETRA, TETRAPOL, TEDS, P25 [43] ...192
Πίνακας 22. Κατανομή φάσματος των 700 MHZ: Ζώνες 12, 13, 14, και 17 [148].....202
Πίνακας 23. Είδη αναπτυσσόμενων στοιχείων του δικτύου FirstNet 204
Πίνακας 24. Αξιολόγηση ασύρματων συστημάτων έκτακτης ανάγκης (Πεδία εφαρμογής και πηγές των έργων).....220
Πίνακας 25. Χαρακτηριστικά ασύρματων συστημάτων έκτακτης ανάγκης [52] 221
Πίνακας 26. Παράδειγμα γεωμετρικών χαρακτηριστικών της πλατφόρμας.....231

Πίνακας 27. HAPS τύποι και τεχνικές προκλήσεις [371] 233
Πίνακας 28. HAPS ζώνες συχνοτήτων.....233
Πίνακας 29. Συγκριτικά χαρακτηριστικά των Non Terrestrial Networks (Δορυφόροι και HAPS) 236
Πίνακας 30. Κατηγορίες (TCOM) αερόπλοιων 240
Πίνακας 31. Συγκριτικά χαρακτηριστικά LAPs.....242
Πίνακας 32. Χαρακτηριστικά των δικτύων δημόσιας ασφάλειας των χωρών: Νότιας Κορέας, Η.Π.Α., Φιλανδίας, Γαλλίας, Ηνωμένου Βασιλειου, Βελγίου και Αυστραλίας.....315

1 Εισαγωγή

1.1 Η έννοια της ασφάλειας

Ο όρος ασφάλεια, που είναι οικείος στο σύνολο των αναγνωστών, προέρχεται ετυμολογικά από το αρχαίο ελληνικό ρήμα «σφάλλω», που σημαίνει ρίχνω κάτω, κάνω κάποιον να πέσει. Ο συνδυασμός αυτού με το στερητικό α- προσδίδει στην ασφάλεια την κύρια έννοιά της, δηλαδή την κατάσταση στην οποία δεν υπάρχουν κίνδυνοι, όπου αισθάνεται κανείς ότι δεν απειλείται, ή την αποτροπή κινδύνου ή απειλής, την εξασφάλιση σιγουριάς και βεβαιότητας [1]. Από την αρχική λεξικολογική προσέγγιση έως τον όρο «δημόσια ασφάλεια» και το πλαίσιο που αυτός καθορίζει υπάρχουν πολλές ομοιότητες και συναφείς εννοιολογικοί προσδιορισμοί. Περαιτέρω δε, σε μία εκ των δημοφιλέστερων ιεραρχήσεων που επιχειρήθηκε το 1943 από τον Abraham Maslow στην ερευνητική του εργασία με τίτλο «A Theory of Human Motivation» [2], η οποία αποτελεί βασικό οδηγό όλων των μεταγενέστερων ερευνητών της κοινωνικής θεωρίας και των επιστημών της κοινωνιολογίας και ψυχολογίας, όρισε ότι η ασφάλεια αποτελεί μία από τις πέντε βασικές κατηγορίες αναγκών του ανθρώπου. Από την αρχική ιεράρχηση έως και τις μεταγενέστερες, πληρέστερες και αναθεωρημένες πλέον προσεγγίσεις της αναφερόμενης κατάταξης, προκύπτει ότι η ασφάλεια εξακολουθεί να βρίσκεται στη βάση της πυραμίδας των αναγκών του ανθρώπου (Εικόνα 1) και ν` αποτελεί τις κυρίες εξ αυτών [3].



Εικόνα 1. Ιεραρχία των ανθρώπινων αναγκών κατά Maslow

Ποια όμως θα μπορούσε να είναι η εμπλοκή της τεχνολογίας και των ραγδαίων εξελίξεων του χώρου στον αντίστοιχο της ασφάλειας; Σαφώς και δεν αναφερόμαστε σε πρωτοείσακτες συσχετίσεις και νεοφυείς σχέσεις, καθώς είναι αυτονόητο ότι από τα πρώτα κιόλας βήματά της, η τεχνολογία δεν θα μπορούσε παρά να εμπλακεί ενεργά στην προσπάθεια παροχής αυτής της βασικής ανάγκης. Η σχέση αυτή λοιπόν μετρά ήδη πολλές δεκαετίες και ταυτόχρονα αποτελεί έναν ζωντανό οργανισμό, διαρκώς εξελισσόμενο και ταχέως αναπτυσσόμενο, με ρυθμούς ταυτόσημους με αυτούς που λαμβάνουν χώρα οι όποιες τεχνολογικές εξελίξεις. Η ασφάλεια, η δημόσια ασφάλεια, η ασφάλεια κρίσιμων υποδομών, η πρόληψη και διαχείριση καταστροφών, καθώς και όποια άλλη μορφή της, αποτέλεσαν και εξακολουθούν ν` αποτελούν ένα από τα βασικά πεδία εφαρμογής των τεχνολογικών επιτευγμάτων κάθε εποχής. Οι ευκαιρίες υλοποίησης πληθώρας εφαρμογών συνδυαστικά με τη σημαντικότητα του οφέλους και της προστιθέμενης αξίας εγκαθίδρυσαν και διατηρούν επίκαιρη τη συγκεκριμένη αλληλεξάρτηση.

Πλείστες τεχνολογικές λύσεις χρησιμοποιούνται επί του παρόντος στη δημόσια ασφάλεια. Καίτοι κάποιες εξ αυτών καλύπτουν αποδοτικά ένα μέρος των απαιτήσεων, υφίστανται κατά περίπτωση σημαντικά προβλήματα και κενά που οφείλονται κατά μείζονα λόγο στο γεγονός ότι οι απαιτήσεις στοιχειοθετούν ένα διαρκώς μεταβαλλόμενο περιβάλλον, το οποίο γεννά νέες και σημαντικά μεγαλύτερες ανάγκες τόσο σε εύρος, όσο και σε ποιότητα.

Οι τεχνολογικές προσπάθειες, από όποια πλευρά και εάν ιδωθούν, κατατείνουν στη διερεύνηση τυχόν πρόσθετων, τρεχουσών και αναδυόμενων τεχνολογιών που θα μπορούσαν να χρησιμοποιηθούν για εφαρμογές δημόσιας ασφάλειας. Ο στόχος είναι προφανής και αφορά στην παροχή βοήθειας στο πλαίσιο των αναγκών δημόσιας ασφάλειας, όπως αυτή λεπτομερώς θα ορισθεί στη συνέχεια, για τη βελτίωση της αποτελεσματικότητας και των επιδόσεων των τεχνολογικών εφαρμογών, ώστε να είναι σε θέση να ανταποκριθούν άμεσα σε όποια περίπτωση απαιτηθεί.

Μέσα από την ενδελεχή μελέτη τεχνολογικών λύσεων, περιπτώσεων χρήσης, ολοκληρωμένων έργων, έργων που βρίσκονται σε πρώιμο ερευνητικό στάδιο, ή σε όψιμο στάδιο υλοποίησης εφαρμογών, αλλά και τη μελέτη των ιδιαίτερων χαρακτηριστικών των τεχνολογιών που διαφαίνεται ότι θα μας απασχολήσουν μελλοντικά, έγινε μια συνολική προσπάθεια να συντεθεί μία γενική δομή υλοποίησης των έργων που φιλοδοξούν να εμπλακούν ενεργά στις λύσεις των τεχνολογικών ερωτημάτων του τομέα αναφοράς. Η τριβή με την τεχνολογία που εφαρμόζεται ήδη στο πεδίο, η εξαντλητική μελέτη της τεχνολογίας που προετοιμάζεται να υποστηρίξει τις εφαρμογές του εγγύς μέλλοντος, αλλά και αυτής που επί του παρόντος συνιστά τάση των δεκαετιών που θ` ακολουθήσουν και μελετάται ως όραμα, οδήγησε σε αδιαμφισβήτητα συμπεράσματα που αφορούν σε βέλτιστες πρακτικές και

κύριες αρχιτεκτονικές για αποδοτικές λύσεις, όπως αυτές θα αποτυπωθούν λεπτομερώς στη συνέχεια.

Στα συμπεράσματα που θα ακολουθήσουν, οδηγηθήκαμε από τη συγκριτική μελέτη των τεχνολογικών λύσεων που εφαρμόζονται στο πεδίο και των έργων που υλοποιούνται από μεγάλους διεθνείς οργανισμούς και εθνικούς φορείς ανά τον κόσμο, οι οποίες αποτελούν σημεία αναφοράς του αντικειμένου και σε κάποιες περιπτώσεις λογίζονται ως state-of-the-art του κλάδου. Από την ενδιαφέρουσα αυτή πορεία προέκυψαν ξεκάθαρα δύο συμπεράσματα. Ότι υπάρχουν «τεχνολογικές ευκαιρίες» και ότι η τρέχουσα χρονική περίοδος αποτελεί τεχνολογικό σταυροδρόμι που θα σηματοδοτήσει κατά το πλείστον την πορεία βελτίωσης των παρεχόμενων υπηρεσιών στο αντικείμενο αναφοράς. Οι ευκαιρίες αυτές συνιστούν κενά που θα πρέπει να καλυφθούν ικανοποιητικά και λύσεις που θα εστιάσουν σε συγκεκριμένα τεχνολογικά ζητήματα. Ιδιαίτερο ενδιαφέρον στο σημείο αυτό παρουσιάζουν οι πρωτοβουλίες που έχουν αναληφθεί επί του ζητήματος από το σύνολο της επιστημονικής κοινότητας, από τους διεθνείς και εθνικούς φορείς και υπηρεσίες, αλλά και από τις εταιρίες που αποτελούν τους πρωταγωνιστές του χώρου. Σε κάθε περίπτωση και ανεξαρτήτως από την επιλογή της μεθόδου ανάπτυξης του κάθε έργου, ο σχεδιασμός του θα πρέπει οπωσδήποτε να λαμβάνει υπόψη του τις ακόλουθες θεματικές:

- Καταγραφή των απαιτήσεων και των ιδιαίτερων χαρακτηριστικών τους με παράλληλη αναγωγή αυτών στα αμιγώς τεχνολογικά ζητήματα και μεγέθη, στο πλαίσιο του ορισμού των αντικειμενικών στόχων.
- Καταγραφή προκλήσεων που αντιμετωπίζουν, ή θα αντιμετωπίσουν στο μέλλον οι υπηρεσίες δημόσιας ασφάλειας, των περιπτώσεων που απασχολούν σήμερα, ως και αυτών που διαφαίνεται ότι θ‘ απασχολήσουν μελλοντικά, στο πλαίσιο της αξιολόγησης των στοιχείων του προβλήματος.
- Διερεύνηση, αναγνώριση και ιεράρχηση υφιστάμενων τεχνολογιών για επίλυση των προκλήσεων, καθώς και των πλεονεκτημάτων και μειονεκτημάτων που χαρακτηρίζουν αυτές, στο πλαίσιο της ανάπτυξης και επικύρωση λύσεων.
- Έρευνα νέων τεχνολογιών για την κάλυψη των κενών και την επίλυση των προβλημάτων στις εφαρμογές δημόσιας ασφάλειας, στο ίδιο ως άνω πλαίσιο.
- Μελέτη δραστηριοτήτων, προϊόντων και υπηρεσιών για τη χρήση τεχνολογιών από φορείς δημόσιας ασφάλειας. Εμπλοκή, αλληλεπίδραση και συνεργασία όλων των φορέων δημόσιας ασφάλειας προς όφελος του αποδοτικότερου αποτελέσματος, στο πλαίσιο τόσο της ανάπτυξης λύσεων, όσο και του ευρύτερου προγραμματισμού.

Η προγενέστερη αναφορά σε «τεχνολογικό σταυροδρόμι» εξηγείται από το γεγονός ότι σήμερα, περισσότερο από κάθε άλλη χρονική στιγμή υφίστανται τεχνολογικές δυνατότητες

για όποια μελλοντική ανάπτυξης. Οι ειδικότεροι τεχνολογικοί τομείς στους οποίους αναφερόμαστε είναι:

- Τεχνητή νοημοσύνη, μηχανική μάθηση, ανάλυση μεγάλων δεδομένων
- Ασφάλεια λογισμικού
- Τεχνολογίες δικτύων επικοινωνίας (5G, 6G, WiFi, LiFi – Οπτική μετάδοση δεδομένων, κ.λπ.)
- Blockchain
- Ευφυής πραγματικότητα (Επαυξημένη πραγματικότητα, Εικονική πραγματικότητα)
- Μη επανδρωμένα ιπτάμενα οχήματα (Unmanned Aerial Vehicles - UAVs)
- Έξυπνα συστήματα επιτήρησης
- Νεφουπολογιστική – Υπολογογιστική αιχμής (Cloud, Fog, Edge Computing)
- Διαδίκτυο των πραγμάτων (Internet of Things – IoT) / Έξυπνες πόλεις

Η δική μας προσέγγιση αφορά στον τεχνολογικό τομέα των δικτύων επικοινωνίας, με την συνεργατική εμπλοκή των υπολοίπων τομέων, όπου αυτό καθίσταται ή δύναται να καταστεί αποδοτικό. Από την ευρύτερη οπτική της εμπλοκής της τεχνολογίας στην δημόσια ασφάλεια, οδηγούμαστε μεθοδικά στη δημιουργία δικτύων επικοινωνίας δημόσιας ασφάλειας, στις αναφερόμενες κρίσιμες επικοινωνίες, οι οποίες φιλοδοξούν να υποστηρίξουν αποδοτικά το έργο των ανθρώπων της δημόσιας ασφάλειας. Έχει αποδειχθεί ότι οι περισσότερες και σημαντικότερες απαιτήσεις και χαρακτηριστικότερες λειτουργικές διαδικασίες απασχολούν τους πρώτους ανταποκριτές. Μία δεξαμενή ανθρώπων που προέρχονται από το σύνολο των υπηρεσιών και φορέων που εμπλέκονται στη δημόσια ασφάλεια και συγκεντρώνουν επάνω τους πληθώρα χαρακτηριστικών και επιχειρησιακών απαιτήσεων. Διανύουμε την «Εποχή των πρώτων ανταποκριτών». Είναι οι άνθρωποι που διαχειρίζονται κρίσεις και καταστροφές στο πεδίο, αυτοί που επιχειρούν, που στέκονται δίπλα στους ανθρώπους που δοκιμάζονται. Είναι οι άνθρωποι που εκτελούν όσα προβλέπει ένα σχέδιο διαχείρισης κρίσεων και καταστροφών. Συνήθως είναι επαγγελματίες, αλλά και σε ορισμένες περιπτώσεις εθελοντές ή και προσωπικό Μη Κυβερνητικών Οργανώσεων (ΜΚΟ). Η επιτυχημένη διαχείριση κρίσεων και καταστροφών βασίζεται σε σημαντικό βαθμό στην πρώτη ανταπόκριση. Μια γρήγορη και επιτυχής αντίδραση μπορεί να οδηγήσει σε εκκένωση περιοχών, στην έγκαιρη οριοθέτηση μιας πυρκαγιάς, στην άμεση μεταφορά ενός ανθρώπου που κινδυνεύει στο νοσοκομείο, αλλά και στην προστασία ανθρώπων από τρομοκρατική επίθεση [4].

1.2 Ζητήματα επικοινωνίας στη δημόσια ασφάλεια

Η αποδοτική υλοποίηση των δικτύων κρίσιμων επικοινωνιών, η ανθεκτικότητά τους, η διασφάλιση την απρόσκοπτης και αδιάλειπτης επικοινωνίας των ανθρώπων της δημόσιας ασφάλειας ακόμη και σε εξαιρετικά ακραίες συνθήκες, όπου ενδεχομένως να έχουν

σημειωθεί καταστροφές στην υποδομή του δικτύου, η παροχή όλων των κρίσιμων δεδομένων στον ελάχιστο δυνατό χρόνο, με την ελάχιστη δυνατή προσπάθεια και τη μέγιστη ευχρηστία επί του πεδίου, υπό συνθήκες απόλυτης ασφάλειας των δεδομένων που διακινούνται καθίσταται ως η κύρια πρόκληση που καλούμαστε να αντιμετωπίσουμε. Ο πρώτος ανταποκριτής, η ναυαρχίδα των απαιτήσεων της δημόσιας ασφάλειας, πρέπει να έχει εύκολη πρόσβαση στην κρίσιμη πληροφορία, πρέπει να έχει σαφέστατη εικόνα των δεδομένων ζωτικής σημασίας που θα του παρέχουν ασφαλή εκτίμηση της κατάστασης του πεδίου στο οποίο καλείται να ενεργήσει, πρέπει να μην έχει εμπόδια στο να συνεργαστεί αποτελεσματικά με τους υπόλοιπους ανθρώπους της δημόσιας ασφάλειας, είτε δρουν δίπλα του, είτε συντονίζουν και λαμβάνουν αποφάσεις από κάποιο συντονιστικό κέντρο λίγα, ή πολλά μέτρα μακριά απ' αυτόν.

Ποιο είναι λοιπόν το πρόβλημα που ζητάει λύση και ποιες οι προκλήσεις που το συνοδεύουν; Η διερεύνηση των αντιλήψεων των πρώτων ανταποκριτών τόσο της Χώρας μας, όσο και ευρύτερα αναφορικά με τη χρήση τηλεπικοινωνιακού εξοπλισμού, με απώτερο στόχο την ανάδειξη των απαιτήσεων τους όπως αυτές προκύπτουν από τις υπηρεσιακές τους ανάγκες. Η έρευνα, καταγραφή και ταξινόμηση των τεχνολογιών αλλά και των αρχιτεκτονικών στις επικοινωνίες της δημόσιας ασφάλειας, που χρησιμοποιούν προηγμένες χώρες εντός και εκτός Ευρωπαϊκής Ένωσης με σκοπό την αναζήτηση των βέλτιστων πρακτικών. Η αποτύπωση των Ευρωπαϊκών προγραμμάτων που αφορούν στον τομέα της δημόσιας ασφάλειας καθώς επίσης και η ανάδειξη των τεχνολογικών τους αποτελεσμάτων, τόσο σε επίπεδο λογισμικού όσο και σε επίπεδο τεχνολογικού εξοπλισμού, με απώτερο στόχο την αξιοποίηση τους σε μια προτεινόμενη αρχιτεκτονική που θα βασίζεται στον συνδυασμό των δυνατοτήτων αξιοποίησης των βέλτιστων πρακτικών, των ιδιαίτερων χαρακτηριστικών της Χώρας μας και των λύσεων που θα μπορούσαν να υιοθετηθούν την τρέχουσα τεχνολογική χρονική στιγμή.

Η προταθείσα λύση έρχεται ως φυσικό αποτέλεσμα της συγκριτικής μελέτης των εξαιρετικών προσπαθειών και πρωτοβουλιών που λαμβάνουν χώρα στο συγκεκριμένο πεδίο έρευνας παγκοσμίως, και ιδιαίτερα πανευρωπαϊκά, αλλά και ως ρεαλιστική και οικονομικά αποδοτική προσέγγιση για τη Χώρα μας, η οποία φιλοδοξεί να συνεισφέρει αποδοτικά και με προοπτική στο ζήτημα.

1.2.1 Η πορεία μέχρι την πρόταση

Κρίθηκε σκόπιμο να μελετήσουμε το σύνολο του έργου των κύριων διεθνών οργανισμών που ασχολούνται με τις επικοινωνίες δημόσιας ασφάλειας τόσο ως κύρια δραστηριότητα, όσο ως δευτερεύουσα, υπό την προϋπόθεση ότι αποτελούν ρυθμιστικούς φορείς των τεχνολογικών εξελίξεων παγκοσμίως. Κρίθηκε σκόπιμο να μελετήσουμε το σύνολο των δομικών στοιχείων του οικοδομήματος που αναφέρεται στις επικοινωνίες δημόσιας ασφάλεια, ξεκινώντας από

τις πρώτες προσπάθειες που έγιναν με τα διαθέσιμα πενιχρά τεχνολογικά μέσα της εποχής των επικοινωνιών στενής ζώνης, πολλές δεκαετίες πίσω στο παρελθόν, ακολούθως τις στέρεες και πολυδοκιμασμένες λύσεις που αποτελούν τη θεμέλιο λίθο των κρίσιμων επικοινωνιών της εποχής του TETRA, P25, DMR, TETRAPOL, αλλά και τις μεταγενέστερες λύσεις της ευρυζωνικής επικοινωνίας και της ένταξης του LTE και 4G, έως την υιοθέτηση των λύσεων που περικλείονται στον όρο κρίσιμες υπηρεσίες (Mission Critical Services - MCX). Κρίθηκε σκόπιμο να μελετήσουμε ακόμη το σύνολο των έργων που υλοποιούνται και έχουν δοκιμαστεί σε διάφορες ευρωπαϊκές και όχι μόνο Χώρες (FirstNet, SafeNet, ESP, Vivre2, RRF, Astrid, κ.λπ.). Κρίθηκε σκόπιμο να μελετήσουμε διεξοδικά τα μεγάλης σημασίας έργα που υλοποιούν ερευνητικοί φορείς, ή εταιρίες ανά τον κόσμο και φιλοδοξούν να ανοίξουν το παράθυρο της επόμενης ημέρας στο τομέα των κρίσιμων επικοινωνιών. Μελετήσαμε τη βιβλιογραφία, παρακολουθήσαμε την πορεία των έργων μέσα από τις δημοσιεύσεις τους (white papers, reports, κ.λπ.), μέσα από τα διαδικτυακά σεμινάρια (webinars), που είχαν ως στόχο να συντονίσουν τις προσπάθειες, να εκπαιδεύσουν τους εμπλεκόμενους, να δοκιμάσουν τις λύσεις και να αποτιμήσουν το έργο, συμμετείχαμε σε μια σειρά σχετικών με το θέμα συνεδρίων, ώστε να εξοικειωθούμε τόσο με την τρέχουσα κατάσταση, όπως αυτή παρουσιάζεται από την παγκόσμια ερευνητική επιστημονική κοινότητα, τους οργανισμούς, τα πανεπιστήμια και τις εταιρείες, όσο και τις εξελίξεις σε παγκόσμιο επίπεδο. Μέσα από τη προπεριγραφείσα διαδικασία της εμπλοκής μας με το ζήτημα των επικοινωνιών στη δημόσια ασφάλεια έγιναν κτήμα μας οι κύριες τεχνολογικές εξελίξεις που μας επέτρεψαν να αποκτήσουμε μια καλή γνώση των δυνατοτήτων και προοπτικών που παρέχονται τεχνολογικά. Μάλιστα, κρίθηκε σκόπιμο να διεξάγουμε έρευνα σχετικά με τις απόψεις και αντιλήψεων των πρώτων ανταποκριτών της Χώρας μας, ως αντικειμενικό στιγμιότυπο ή σε κάθε περίπτωση ασφαλή γνώση των αναγκών τους επί του πεδίου, τόσο σε επίπεδο συσκευών, όσο και επίπεδο τηλεπικοινωνιακής κάλυψης.

1.3 Οργάνωση κειμένου

Οι θεμελιώδεις ορισμοί, το πλαίσιο που ορίζει τη δημόσια ασφάλεια, οι απαιτήσεις που προκύπτουν σε επίπεδο επικοινωνίας παρουσιάζονται στο Κεφάλαιο 2. Στο Κεφάλαιο 3 παραθέτουμε το σύνολο των κύριων Διεθνών και Ευρωπαϊκών Οργανισμών, Ενώσεων και πρωτοβουλιών που εμπλέκονται στην υλοποίηση λύσεων και έργων σχετικά με τις κρίσιμες επικοινωνίες. Στο Κεφάλαιο 4 γίνεται μια εκτενής αναφορά στις τεχνολογίες και τα πρότυπα που καθ` οιονδήποτε τρόπο εμπλέκονται ενεργά στις προταθείσες λύσεις. Στο Κεφάλαιο 5 αναφερθήκαμε στα ζητήματα υλοποίησης των δικτύων δημόσιας ασφάλειας και έγινε μια αποτύπωση των κύριων έργων που είναι αξιόλογα στον τομέα. Στο Κεφάλαιο 6 αποτυπώθηκε η πρακτική που χρησιμοποιούν κάποιες Χώρες ανά τον κόσμο, η συγκριτική μελέτη αυτών

και οι βέλτιστες πρακτικές στον τομέα. Κεφάλαιο 7 αποτυπώθηκαν με τον χαρακτήρα του επίλογου, η ενεστώσα κατάσταση των δικτύων δημόσιας ασφάλειας στη Χώρα μας και οι μελλοντικές προεκτάσεις.

2 *Δημόσια Ασφάλεια*

Η δημόσια ασφάλεια είναι η ικανότητα του κράτους να επιβάλει, μέσω των θεσμών, των οργάνων και των μηχανισμών του, το σεβασμό στην έννομη τάξη και να εμπεδώνει ταυτόχρονα στον κοινωνικό σχηματισμό ένα αίσθημα εμπιστοσύνης και σιγουριάς για την ασφαλή ενάσκηση των δικαιωμάτων του πολίτη και την απόλαυση των εννόμων αγαθών του [5]. Από τη συγκεκριμένη προσέγγιση γίνεται αντιληπτό ότι η δημόσια ασφάλεια συνιστά ένα αυτοτελές έννομο αγαθό, καθώς αποτελεί μια κοινωνική και ηθική αξία που λαμβάνει τη δική της οντότητα και συγκαταλέγεται εννοιολογικά στο «σωρό» των λοιπών κοινωνικών και ηθικών αξιών που έχουν ανάγκη προστασίας. Μάλιστα, η πρόοδος του πολιτισμού σε παγκόσμια κλίμακα έχει επιφέρει σε μεγάλο βαθμό σύγκλιση των κοινωνικών αξιών ώστε να είναι σήμερα αδιανόητη η μη προστασία της ζωής, της υγείας, της ιδιοκτησίας κ.λπ. από κάποια πολιτισμένη κοινωνία [6]. Για το έννομο αγαθό της δημόσια ασφάλειας η σύγκλιση είναι καθολική και χωρίς διαφοροποιήσεις από χώρα σε χώρα.

Η συγκεκριμένη κατηγοριοποίηση και η ένταξή της δημόσιας ασφάλειας στην ίδια λίστα με τα μείζονα αγαθά της ανθρώπινης ζωής και υγείας, αποτελεί την κύρια απόδειξη της σπουδαιότητάς της. Από μια προσεκτικότερη ματιά στα δομικά της στοιχεία προκύπτει ότι ως άμεσα συνυφασμένη με τη διατήρηση της έννομης τάξης και της εμπέδωσης αισθημάτων εμπιστοσύνης και σιγουριάς προς τους πολίτες, απειλείται από κάθε κατάσταση που μπορεί να δημιουργήσει συνθήκες αστάθειας, ανασφάλειας και αβεβαιότητας. Οι πηγές των απειλών που αντιμετωπίζει η δημόσια ασφάλεια κατηγοριοποιούνται σε δύο είδη. Στις ανθρωπογενείς απειλές και τις φυσικές – τεχνολογικές καταστροφές. Στις ανθρωπογενείς πηγές εντάσσονται οι τρομοκρατικές ενέργειες, το οργανωμένο έγκλημα, τα ιδιαιτέρως βίαια εγκλήματα, τα διασυνοριακά εγκλήματα, τα σοβαρά εγκλήματα στον κυβερνοχώρο, τα μεγάλα γεγονότα και εκδηλώσεις, οι πολεμικές συγκρούσεις, οι εκτεταμένες αντιδράσεις και εξεγέρσεις, καθώς και κάθε άλλο συμβάν που διαταράσσει την έννομη τάξη και επιφέρει σημαντικό αρνητικό

αντίκτυπο στον κοινωνικό ιστό. Στις φυσικές καταστροφές εντάσσονται οι σεισμοί, οι κατολισθήσεις, τα ακραία καιρικά φαινόμενα (*τυφώνας, πλημμύρα, ξηρασία, παγετός, ανεμοθύελλα, χιονοθύελλα, κ.αλ.*), οι ηφαιστειακές εκρήξεις, το τσουνάμι, οι φυσικές πυρκαγιές, οι πανδημίες κ.αλ.. Στις ανθρωπογενείς (τεχνολογικές) καταστροφές εντάσσονται περιπτώσεις που προκύπτουν από κακή ανθρώπινη χρήση της τεχνολογίας, όπως ατυχήματα μεταφοράς (*αεροπορικά, σιδηροδρομικά, θαλάσσια και οδικά*), κάθε είδους περιβαλλοντική καταστροφή (*βιομηχανικές εκρήξεις, χημικά και ραδιενεργά απόβλητα*), τα αποτελέσματα κλιματικών μεταβολών, οι πυρκαγιές που οφείλονται στον ανθρώπινο παράγοντα, οι μεγάλου μεγέθους βλάβες σε κρίσιμες υποδομές, κ.αλ..

Κάθε οργανωμένη κοινωνία έχει δέσμια υποχρέωση να προστατεύσει το έννομο αγαθό της δημόσιας ασφάλειας έναντι των πολιτών της. Οι δράσεις για την προστασία εντάσσονται σε ένα ευρύτερο σχέδιο εθνικών πολιτικών και στρατηγικών, το οποίο περιλαμβάνει μεθοδολογημένη προσέγγιση και σαφείς στόχους. Ο αποτελεσματικός σχεδιασμός σε κάθε περίπτωση περιλαμβάνει τη λεπτομερειακή περιγραφή του προβλήματος, την πρόβλεψη της απειλής, την αξιολόγηση των κινδύνων, τον σχεδιασμό, προγραμματισμό και εκδήλωση της κατάλληλης αντίδρασης και την αποτίμηση των δράσεων. Η ετοιμότητα του κοινωνικού μηχανισμού να προστατευθεί από τις φυσικές καταστροφές περιγράφεται με τον όρο *προσαρμογή* στον κίνδυνο, ενώ ως *διευθέτηση* νοείται η συνολική προσπάθεια για μείωση των αρνητικών επιπτώσεων [7]. Στην κατεύθυνση της οργανωμένης και συντονισμένης αυτής αντιμετώπισης λειτουργούν πολλοί διεθνείς και κρατικοί οργανισμοί, υπηρεσίες και φορείς.

Ωστόσο, για να προσεγγίσουμε σωστά το πλαίσιο των απαιτήσεων που δημιουργούνται για τη δημόσια ασφάλεια, οφείλουμε να εμβαθύνουμε στα δομικά στοιχεία των απειλών και των δυσμενών για τη δημόσια ασφάλεια συνθηκών που είναι πιθανό να δημιουργηθούν. Μάλιστα, η επικρατούσα πλέον φιλοσοφία με την οποία προσεγγίζουμε τα συγκεκριμένα ζητήματα έχει αποδεχθεί το εύρος των δυνατοτήτων αντιμετώπισης, καθώς σε ένα τόσο σύνθετο περιβάλλον κινδύνων και απειλών, όπως αυτό που βιώνουμε ως παγκόσμια πραγματικότητα, η αντίληψη της απόλυτης προστασίας έχει δώσει τη θέση της στην ενίσχυση της ανθεκτικότητας των υποδομών προκειμένου να διασφαλίζεται η ικανοποίηση του επιπέδου εξυπηρέτησης που απαιτείται να παρέχουν στην κοινωνία και την οικονομία [8]. Χαρακτηριστική επί του θέματος είναι η προσέγγιση του Γενικού Γραμματέα του Οργανισμού Ηνωμένων Εθνών κ. Αντόνιο Γκουτέρες (Antonio Guterres), ο οποίος προλογίζοντας την 6η ετήσια Έκθεση Παγκόσμιας Αξιολόγησης των Ηνωμένων Εθνών για τη μείωση του κινδύνου καταστροφών για το έτος 2022, αναφέρει ότι: «*Πρέπει να σημειωθεί επειγόντως πρόοδος στη μείωση του κινδύνου καταστροφών ως προϋπόθεση για την αειφόρο ανάπτυξη. […] Ενώ οι αποφάσεις πρέπει να βασίζονται στην επιστήμη, μπορούν να συμπληρωθούν από πλούσιες πηγές πληροφοριών, όπως η γηγενής και η παραδοσιακή γνώση, η οποία μπορεί να προσθέσει μια*

βαθύτερη κατανόηση των συγκεκριμένων προκλήσεων. […] Αν θέλουμε να ανταποκριθούμε στις προκλήσεις του εικοστού πρώτου αιώνα, χρειαζόμαστε συστημική σκέψη, συντονισμό και αντίδραση στον κίνδυνο καταστροφής. Έτσι μπορούμε να δημιουργήσουμε ένα πιο βιώσιμο, ανθεκτικό και δίκαιο μέλλον για όλους» [9].

2.1 Φυσικές καταστροφές

Ένα από τα εμβληματικά μηνύματα – συνθήματα του FirstNet αναφέρει: «*Να είσαι έτοιμος για τα πάντα, ακόμη και για το απρόσμενο*» [10]. Και όταν αναφερόμαστε στο απρόσμενο και ξαφνικό, αναφερόμαστε κυρίως σε φυσικές καταστροφές. Τι είναι όμως οι φυσικές καταστροφές και πως μπορούμε να τις αντιμετωπίσουμε;

Σύμφωνα με την υφιστάμενη εγχώρια νομοθεσία και συγκεκριμένα την υπ' αρίθμ: 1299/2003 Απόφαση του Υπουργού Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης (ΦΕΚ 423/Β/7-4-2003 – Σχέδιο με την κωδική ονομασία «ΞΕΝΟΚΡΑΤΗΣ»), η οποία αναθεωρήθηκε και συμπληρώθηκε με την υπ' αρίθμ: 3384/2006 Υπουργική Απόφαση(ΦΕΚ 776/Β/28-6-2006), καταστροφή είναι κάθε φυσικό φαινόμενο ή τεχνολογικό συμβάν στο χερσαίο, θαλάσσιο και εναέριο χώρο, ταχείας ή βραδείας εξέλιξης, το οποίο προκαλεί εκτεταμένες δυσμενείς επιπτώσεις στον άνθρωπο, καθώς και στο ανθρωπογενές ή φυσικό περιβάλλον. Επίσης, είναι η σοβαρή διατάραξη της λειτουργίας μια κοινότητας ή μιας κοινωνίας περιλαμβάνοντας ανθρώπινες, υλικές, οικονομικές ή περιβαλλοντικές απώλειες και επιπτώσεις, οι οποίες υπερβαίνουν την ικανότητα της πληγείσας κοινότητας να ανακάμψει χρησιμοποιώντας ίδια μέσα [11]. Επιπλέον, είναι μία ταχύτατη, στιγμιαία ή μεγάλη σύγκρουση του φυσικού περιβάλλοντος με το κοινωνικο - οικονομικό σύστημα που μπορεί ν' αποτελέσει απειλή στην κοινωνία ή κάποιο τμήμα της με σοβαρές ακούσιες επιπτώσεις [7]. Οι ορισμοί αυτοί, μαζί με πολλούς άλλους που υπάρχουν στη βιβλιογραφία, συνθέτουν την έννοια της καταστροφής σε απόλυτο βαθμό και αποτελούν την προσπάθεια των κατά περίπτωση μελετητών να προσεγγίσουν με τον καλύτερο δυνατό τρόπο τον συγκεκριμένο όρο. Η μελέτη της έννοιας επεκτείνεται στην κατηγοριοποίηση του κινδύνου, ώστε μέσω αυτής να οδηγηθούμε στην αποδοτικότερη διαχείριση. Η κατηγοριοποίηση μπορεί να ειδωθεί από διάφορες παραμέτρους, με πιο διαδεδομένη αυτή που αφορά στον τύπο του κινδύνου που προκαλείται. Μάλιστα, υφίσταται διεθνής βάση καταγραφής των περιστατικών που απασχολούν παγκοσμίως, η Βάση Δεδομένων Έκτακτης Ανάγκης (Emergency Events Database - EM-DAT) [12], η οποία αποτελεί δράση στο πλαίσιο λειτουργίας του Κέντρου Έρευνας για την Επιδημιολογία των Καταστροφών (Center for Research on the Epidemiology of Disasters - CRED), τον κατ' εξοχήν αξιόπιστο φορέα ολοκληρωμένης καταγραφής και κατηγοριοποίησης φυσικών καταστροφών [13], η οποία δημιουργήθηκε με την υποστήριξη του Παγκόσμιου Οργανισμού Υγείας και της Βελγικής Κυβέρνησης. Με βάσει τα δεδομένα

αυτού και συγκεκριμένα της έκθεσης που αφορά για την εικοσαετία 2000-2019 [14], οι κατηγορίες που συναντάμε είναι (Εικόνα 2):

α. Γεωφυσικές καταστροφές, στις οποίες εντάσσονται σεισμοί, κατολισθήσεις, ηφαιστειακή δραστηριότητα, κ.αλ.

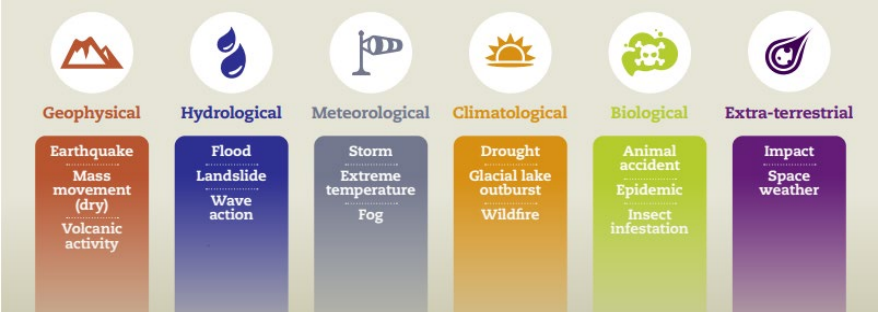
β. Υδρολογικές καταστροφές, στις οποίες εντάσσονται πλημμύρες, τσουνάμι, κ.αλ.

γ. Μετεωρολογικές καταστροφές, στις οποίες εντάσσονται τυφώνες, κάθε είδους ακραία καιρικά φαινόμενα, όπως έντονες βροχοπτώσεις, παρατεταμένη ξηρασία και καύσωνας, κ.αλ.

δ. Κλιματολογικές καταστροφές, στις οποίες εντάσσονται η ξηρασία, η απότομη και χωρίς συγκεκριμένη αιτία απελευθέρωση σημαντικότατων ποσοτήτων νερού από παγετώνες, η οποία έχει επικρατήσει να αναφέρεται με τον όρο Glacial Lake Outburst Flood (GLOF)

ε. Βιολογικές καταστροφές, στις οποίες εντάσσονται ατυχήματα του ζωικού βασιλείου, επιδημίες, επιδρομές εντόμων, κ.αλ.

στ. Εξωγήινες καταστροφές, στις οποίες εντάσσονται πτώσεις μετεωριτών, κ.αλ.

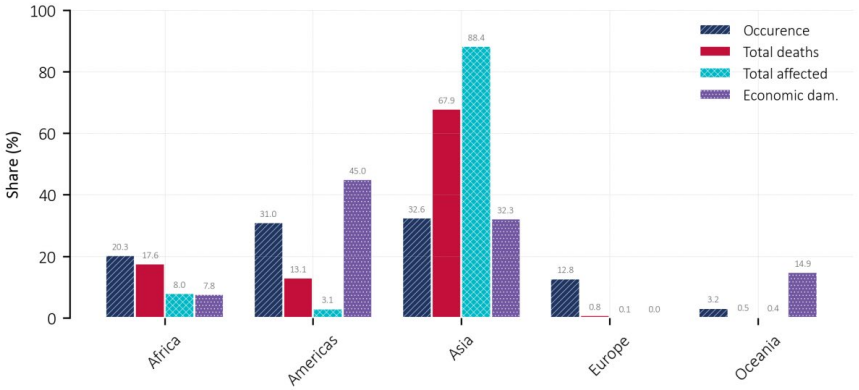


Εικόνα 2: Είδη καταστροφών **[14]**

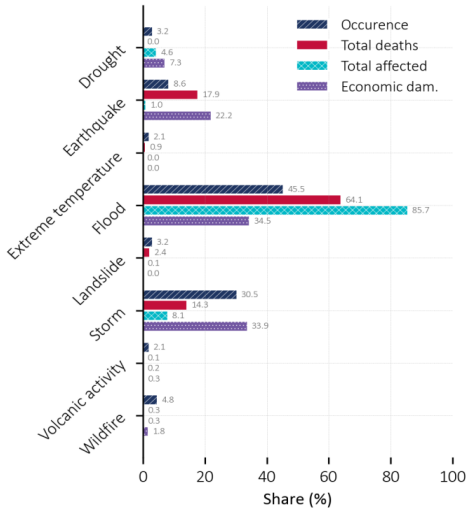
Για ν` αντιληφθούμε τα μεγέθη των συνεπειών από φυσικές καταστροφές, αρκεί να παραθέσουμε δειγματοληπτικά κάποια στατιστικά στοιχεία των τελευταίων ετών. Κατά το πρώτο εξάμηνο του 2022 (Εικόνα 3, Εικόνα 4) παρατηρούμε ότι οι χώρες της Ασίας αντιμετώπισαν τα περισσότερα περιστατικά και ακολούθως η Αμερική και η Αφρική. Το 2021, το EM-DAT ανέφερε 28 σεισμούς, έναντι του μέσου όρου των 27 σεισμών την εικοσαετία 2001-2020. Ωστόσο, ο αριθμός των θανάτων και τα άτομα που επλήγησαν από σεισμούς, καθώς και από τις παγκόσμιες οικονομικές ζημιές, ήταν χαμηλότερα το 2021 από τον μέσο όρο για τα τελευταία 20 χρόνια, γεγονός που οφείλεται στην απουσία μεγάλων σεισμών το 2021. Ωστόσο, ο σεισμός 7,2 Ρίχτερ στην Αϊτή, ο οποίος σημειώθηκε τον Αύγουστο του 2021, εξακολουθεί να βρίσκεται στην κορυφή της λίστα του EM-DAT για το 2021, ως η πιο θανατηφόρα καταστροφή με 2.575 θανάτους. Επιπλέον, ο σεισμός της Φουκουσίμα του Φεβρουαρίου του ίδιου έτους (μεγέθους 7,1) εμφανίζεται επίσης στην πρώτη δεκάδα των καταστροφών που προκάλεσαν τις μεγαλύτερες οικονομικές ζημίες,

καθώς το εκτιμώμενο οικονομικό κόστος ανέρχεται σε 7,7 δισεκατομμύρια δολάρια (US$). Η συνολική συγκριτική αποτύπωση των φυσικών καταστροφών του έτους 2021 έναντι της εικοσαετίας 2001-2020 εμφανίζεται στην Εικόνα 5 και καταδεικνύει ότι αυτό που είχε αρχίσει απότομα να συμβαίνει από το 1980 και έπειτα, ήτοι η αύξηση των περιστατικών καταστροφών, εξακολουθεί με τον ίδιο αμείωτο ρυθμό. Τραγική επιβεβαίωση της συγκεκριμένης αυξητικής τάσης, τόσο ως προς τα περιστατικά, όσο και ως προς την έντασή τους αποτελεί ο μόλις πρόσφατος σεισμός σε Τουρκία – Συρία, που συνέβη την 8-2-2023/03:30΄ και ήταν έντασης 7,8 της κλίμακας ρίχτερ. Επηρεάστηκαν απ` αυτόν περισσότερα από 24 εκατομμύρια άνθρωποι και ο πλήρης απολογισμός των θυμάτων και καταστροφών δεν έχει ολοκληρωθεί έως τη στιγμή συγγραφής της παρούσας εργασίας, αλλά σε κάθε περίπτωση ξεπερνά τους 43.858 νεκρούς και τους 114.926 τραυματίες, με την οικονομική ζημία να κυμαίνεται από 50 έως 80 δισεκατομμύρια δολάρια, καθώς καταστράφηκαν περίπου 6.500 κτήρια [15].

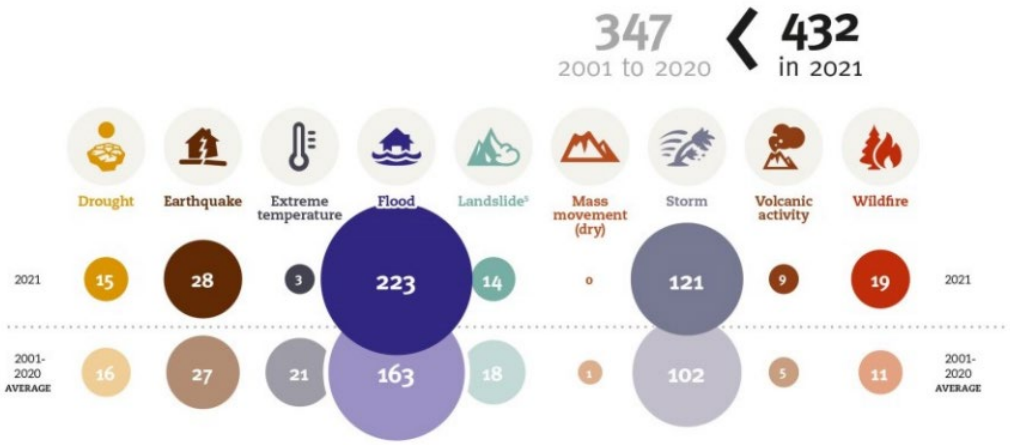
Η συγκεκριμένη διαπίστωση, μαζί με μια σειρά άλλους παράγοντες προκάλεσαν το αυξανόμενο ενδιαφέρον για την έρευνα των καταστροφών. Έτσι οδηγηθήκαμε σε διεθνείς δεσμεύσεις για τη μείωση του κινδύνου καταστροφών και τη βελτίωση της ανθεκτικότητας στις καταστροφές από πληθώρα οργανισμών, φορέων και κρατών, όπως αναφέρθηκε ήδη. Το σημαντικότατο βέβαια κέρδος από την ενεργοποίηση της παγκόσμιας κοινότητας αφορά στην παραδοχή ότι για την αντιμετώπιση των συνεπειών των καταστροφών, που είναι συχνά εκτεταμένες και πολυδιάστατες, καθίσταται αναγκαία μια διεπιστημονική προσέγγιση στην έρευνα. Η εμπλοκή της τεχνολογίας είναι μονόδρομος.



Εικόνα 3. Ποσοστιαία επί τις εκατό αποτύπωση των φυσικών καταστροφών και των συνεπειών τους, ανά ήπειρο (1ο εξάμηνο 2022) [16]



Εικόνα 4. Ποσοστιαία επί τις εκατό αποτύπωση των φυσικών καταστροφών και συνεπειών τους ανά είδος (1ο εξάμηνο 2022) [16]



Εικόνα 5. Συγκριτική μελέτη καταστροφών ανά είδος 2021 με εικοσαετία (2001-2020) [17]

Στο σημείο αυτό πρέπει ν' αναφερθεί ότι για να ενταχθεί οποιαδήποτε καταστροφή στα στατιστικά δεδομένα του EM-DAT θα πρέπει να ισχύουν μια των ακόλουθων προϋποθέσεων [13]:

- Να έχουν αναφερθεί δέκα (10) ή περισσότεροι νεκροί
- Να έχουν αναφερθεί εκατό (100) ή περισσότεροι άνθρωποι, ως πληγέντες
- Να έχει κηρυχθεί κατάσταση έκτακτης ανάγκης
- Να έχει ζητηθεί διεθνής βοήθεια

2.2 Ανθρωπογενείς καταστροφές

Ο Kofi Annan, πρώην Γενικός Γραμματέας των Ηνωμένων Εθνών, είχε κάποτε αναφέρει: *«Οι κοινότητες θα αντιμετωπίζουν πάντα φυσικούς κινδύνους, αλλά οι σημερινές καταστροφές προκαλούνται συχνά, ή επιδεινώνονται από την ανθρώπινη δραστηριότητα. Στο πιο δραματικό*

επίπεδο, οι ανθρώπινες δραστηριότητες αλλάζουν τη φυσική ισορροπία στη Γη, παρεμβαίνοντας όσο ποτέ άλλοτε στην ατμόσφαιρα, στους ωκεανούς, στους πάγους των πόλων της Γης, στις δασικές εκτάσεις και σε κάθε μορφής πυλώνα φυσικού πλούτου που κάνουν τον κόσμο μας βιώσιμο. Επιπλέον, βάζουμε τον εαυτό μας σε κίνδυνο και με λιγότερο ορατούς τρόπους. Ποτέ άλλοτε στην ανθρώπινη ιστορία δεν έχει καταγραφεί η συγκεκριμένη συγκέντρωση σε πόλεις που βρίσκονται σε ενεργές σεισμογενείς περιοχές. Εξαθλίωση και δημογραφικά προβλήματα έχουν οδηγήσει περισσότερους ανθρώπους από ποτέ να ζουν σε προβληματικές περιοχής, που παρουσιάζουν αυξημένο κίνδυνο πλημμύρων και κατολισθήσεων. Είτε αφορά σε κακή περιβαλλοντική διαχείριση, είτε σε έλλειψη ρυθμιστικού πλαισίου, αυξάνεται η διακινδύνευση και επιδεινώνονται οι επιπτώσεις καταστροφών» [18].

Η δεύτερη πολύ μεγάλη κατηγορία που συναντούμε είναι αυτή των ανθρωπογενών καταστροφών. Αφορούν σε καταστροφές που προκαλούνται από κινδύνους που προκαλεί ο άνθρωπος και τα δημιουργήματα ή οι ενέργειές του [7]. Και στην περίπτωση των ανθρωπογενών καταστροφών ο ρυθμός εμφάνισής τους είναι αυξητικός, ιδιαιτέρως κατά τις τελευταίες δεκαετίες [13]. Αυτό βέβαια αντικατοπτρίζει εν πολλοίς τη ραγδαία τεχνολογική ανάπτυξη σε όλα τα επίπεδα που υφίσταται ανθρώπινη παρέμβαση. Οι μεταφορές, η βιομηχανία και οι κατασκευές παρουσιάζουν τεράστιες διαφορές συγκριτικά με το παρελθόν. Επομένως, οι καταστροφές που καταγράφονται είναι περισσότερες σε αριθμό, αλλά και πιο επιζήμιες σε σχέση με τ‘ αρνητικά τους αποτελέσματα τόσο σε απώλεια ανθρώπινων ζωών, όσο και σε οικονομικές επιπτώσεις [13]. Στις ανθρωπογενείς καταστροφές εντάσσονται οι τεχνολογικές καταστροφές, οι αστικές καταστροφές και οι ένοπλες συρράξεις. Μια άλλη ξεχωριστή και ενδιαφέρουσα υποκατηγορία είναι ο συνδυασμός των φυσικών και ανθρωπογενών καταστροφών που έχει λάβει την ονομασία φυσικο-τεχνολογικές καταστροφές (NaTech) [19], χαρακτηριστικό παράδειγμα της οποία αποτελεί το πυρηνικό ατύχημα που προκλήθηκε το 2011 στην Ιαπωνία (πυρηνικός σταθμός Fukushima Daiichi), έπειτα από τσουνάμι από προηγηθείσα σεισμική δόνηση της τάξης των 9,1 ρίχτερ [20].

Από τα γραφήματα που παρουσιάζονται συνολικά στην Εικόνα 6, προκύπτει εύγλωττα ότι οι καταγεγραμμένες περιπτώσεις ανθρωπογενών καταστροφών, θανάτων και οικονομικών ζημιών που προκλήθηκαν απ‘ αυτές το χρονικό διάστημα από το 1900 έως σήμερα (2022), συγκριτικά με τα αντίστοιχα των πενήντα τελευταίων ετών, είναι σχεδόν ταυτόσημες, γεγονός που καταδεικνύει ότι η τεχνολογική εξέλιξη έφερε και τη δραματική αύξηση των τεχνολογικών καταστροφών, σε αριθμητικά δεδομένα και συνέπειες. Από τα ίδια διαγράμματα προκύπτει η ιδιαίτερα μεγάλη επιβάρυνση που προκαλείται στην οικονομία. Εδώ βέβαια κρύβεται μια μεγάλη αντίθεση, καθώς θα περίμενε κανείς ότι η πρόοδος που έχει σημειωθεί στην πρόβλεψη, έγκαιρη προειδοποίηση και αντιμέτωπη, με την ενεργό εμπλοκή

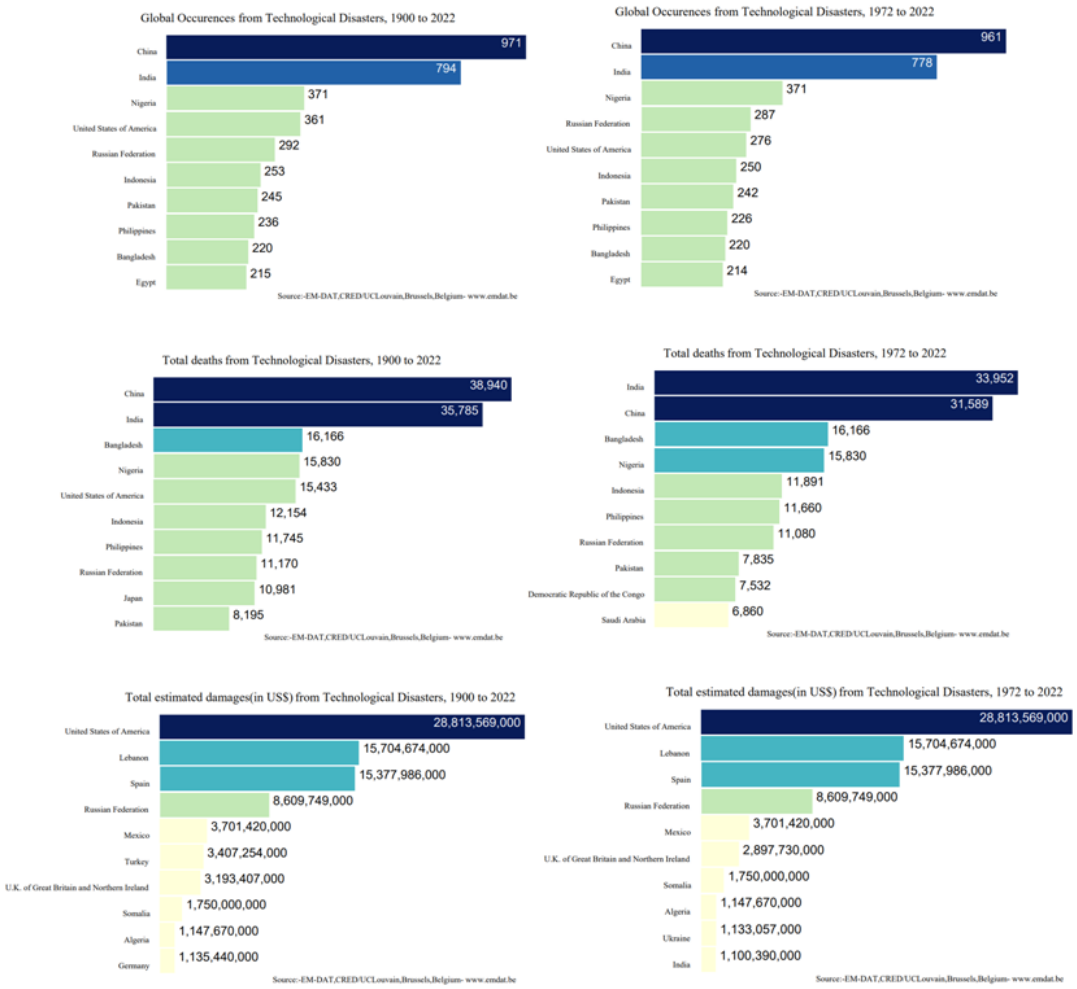
της τεχνολογίας, θα είχε ως αποτέλεσμα να αμβλυνθούν οι ζημιογόνοι δείκτες. Τουναντίον, ο αριθμός των πληγέντων και των ζημιών από καταστροφές ολοένα και αυξάνει.

Η αναφερόμενη κατηγοριοποίηση των ανθρωπογενών καταστροφών φυσικά και δεν είναι η μοναδική. Η ομαδοποίηση σε είδη καταστροφών που προκαλούνται από τον άνθρωπο μπορεί να ιδωθεί από διαφορετικές παραμέτρους. Είτε με βάση το έναυσμα της καταστροφής (αιφνίδια ή αργής εξέλιξης), είτε λαμβάνοντας υπόψη άλλα κριτήρια (βιομηχανικά ατυχήματα, ατυχήματα σε μεταφορές, άλλα ατυχήματα), ή την ένταση/μέγεθος των επιπτώσεων που προκάλεσαν (αγνοούμενοι, τραυματίες, πληγέντες, θάνατοι, κ.λπ.). Σε κάθε περίπτωση οι τεχνολογικές καταστροφές καταγράφουν μεγαλύτερη αύξηση σε λιγότερο αναπτυγμένες Χώρες [13].

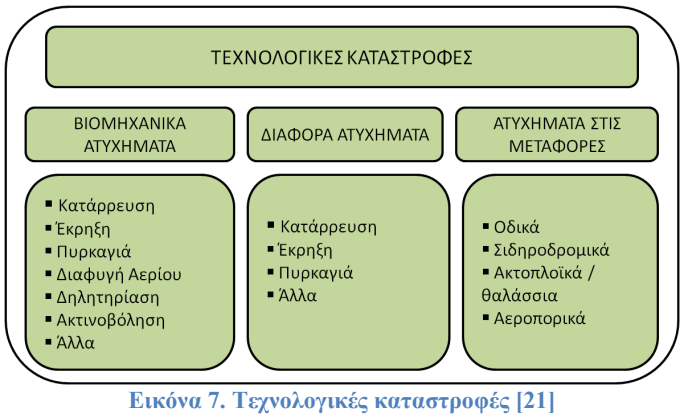
Μια από τις πιο ενδιαφέρουσες κατηγοριοποιήσεις που συναντούμε στη βιβλιογραφία για τις τεχνολογικές καταστροφές είναι η ακόλουθη [21]:

- Βιομηχανικά ατυχήματα
- Ατυχήματα στις μεταφορές
- Άλλα ατυχήματα

Στην Εικόνα 7 εξειδικεύονται ανά κατηγορία τα επιμέρους είδη των καταστροφών που κατηγοριοποιούνται σε κάθε μία από τις τρεις αυτές κατηγορίες. Στο πλαίσιο της παρούσας εργασίας δεν υφίσταται σκοπιμότητα να επεκταθούμε περαιτέρω στα είδη των ανθρωπογενών καταστροφών. Είναι αντιληπτό από τον οιονδήποτε ότι η βιομηχανική ανάπτυξη που καταγράφεται τα τελευταία πενήντα χρόνια στο σύνολο του πλανήτη είναι αλματώδης. Οι κίνδυνοι που προκύπτουν από τη δραστηριότητα του ανθρώπου δεν θα μπορούσε να μην επηρεάσει τον ίδιο. Παράλληλα, με τον ίδιο ρυθμό αυξήθηκαν οι μεταφορές ανθρώπων και αγαθών μεταξύ χωρών και ηπείρων, γεγονός που δημιούργησε ευνοϊκότερες συνθήκες για καταστροφές από μεταφορικά ατυχήματα, καθώς εμπλέκονται πλέον ενεργά εκατομμύρια άνθρωποι.



Εικόνα 6. Τεχνολογικές καταστροφές το διάστημα 1900-2022, συγκριτικά με τα αντίστοιχα των 50 τελευταίων ετών [13]



Εικόνα 7. Τεχνολογικές καταστροφές [21]

Οι ένοπλες συρράξεις, για τις οποίες έγινε λόγος παραπάνω, αποτελούν μια ξεχωριστή υποκατηγορία ανθρωπογενών καταστροφών. Προκαλούν αλυσιδωτές αντιδράσεις προβλημάτων και σύνθετες ανθρωπιστικές κρίσεις, τις λεγόμενες Σύνθετες Ανθρωπιστικές Καταστάσεις Έκτακτης Ανάγκης (Complex Humanitarian Emergencies - CHE), οι οποίες περιγράφονται ως αλληλουχία γεγονότων που καταλήγει σε ένα περίπλοκο σύνολο κοινωνικών, υγειονομικών, οικονομικών και συχνά πολιτικών συνθηκών, που συνήθως

οδηγούν σε μεγάλο ανθρώπινο πόνο και θάνατο και απαιτούν εξωτερικές βοήθεια και βοήθεια. Η σύνδεσή τους περιλαμβάνει ποικιλία γεγονότων όπως πόλεμος ή ένοπλη σύγκρουση, υπανάπτυξη, φτώχεια, υπερπληθυσμός, ανθρωπογενείς καταστροφές, κλιματική αλλαγή και καταστροφές όπως ξηρασία, πείνα και πλημμύρες [22]. Ενδεικτικά, το 2022, 274 εκατομμύρια άνθρωποι χρειάστηκαν ανθρωπιστική βοήθεια και προστασία, έναντι 235 εκατομμυρίων του έτους 2021. Η πανδημία του COVID-19, η κλιματική αλλαγή και οι συγκρούσεις είναι βασικοί παράγοντες της καταγραφείσας αύξησης. Στις αρχές του 2022, ο Οργανισμός Ηνωμένων Εθνών (Ο.Η.Ε.) ανακοίνωσε ότι η εισβολή της Ρωσίας στην Ουκρανία και άλλες συγκρούσεις είχαν οδηγήσει περισσότερους από 100 εκατομμύρια ανθρώπους να εγκαταλείψουν τα σπίτια τους, αριθμός που καταγράφεται πρώτη φορά. Βέβαια, τα αποτελέσματα τέτοιων καταστάσεων, ακόμη και όταν βρίσκονται σε φάση ύφεσης ή έχουν ολοκληρώσει τον καταστροφικό τους κύκλο, παραμένουν για δεκαετίες, μαζί με τις τεράστιες οικονομικές συνέπειες για τις εμπλεκόμενες χώρες.

2.3 Ασύμμετρες απειλές

Τι συμβαίνει όμως με τις καταστάσεις που «γεννούν» απειλή για τη δημόσια ασφάλεια και δεν εντάσσονται σε μια από τις κατηγορίες που ήδη αναφέρθηκαν; Στο σύγχρονο περιβάλλον ασφάλειας υπάρχουν τρία είδη απειλών για την εθνική ασφάλεια: οι παραδοσιακές διακρατικές συγκρούσεις, τα προβλήματα δημόσιας τάξης (τρομοκρατία οργανωμένο έγκλημα, εσωτερική παραβατικότητα διαφόρων μορφών) και οι φυσικές οι τεχνολογικές καταστροφές οι άλλες έκτακτες καταστάσεις [23]. Κάθε μορφής κατάσταση που οδηγεί σε καταστροφή ή κρίση και δεν πληροί τα κριτήρια των κατηγοριών στις οποίες ήδη αναφερθήκαμε, συνηθίζουμε να την εντάσσουμε σε μία ευρύτερη κατηγορία που ονομάζουμε «ασύμμετρες απειλές». Ως ασύμμετρη απειλή νοείται η εκδοχή του «δεν πολεμώ δίκαια» η οποία περιλαμβάνει από τη μία πλευρά τη χρήση του αιφνιδιασμού σε όλες του τις διαστάσεις και από την άλλη πλευρά τη χρήση όπλων με τρόπους που δεν προβλέπονται στη σχεδίαση και στα σενάρια των οργανωμένων κρατών [24]. Είναι γεγονός ότι ο όρος εμφανίστηκε τις δύο τελευταίες δεκαετίες και συνδέθηκε με τα ζητήματα εθνικής ασφάλειας και «ασύμμετρου πολέμου». Ωστόσο, ακόμη και εάν θεωρηθεί ότι χρησιμοποιείται καταχρηστικά, οι βασικές μορφές απειλών που εντάσσονται σ' αυτόν παράγουν αυξημένες συνθήκες διασάλευσης της δημόσιας ασφάλειας και όχι μόνο της εθνικής. Αξιοσημείωτο είναι ότι κατά το Γενικό Επιτελείο Εθνικής Άμυνας (Γ.Ε.ΕΘ.Α.), οι βασικότερες μορφές απειλών, που λογίζονται ως «ασύμμετρες» είναι:

- όπλα μαζικής καταστροφής
- διεθνής τρομοκρατία
- δράση ενόπλων ομάδων

- λαθρομετανάστευση
- οργανωμένο έγκλημα
- πληροφοριακός πόλεμος - κυβερνοπόλεμος
- ριζοσπαστικοποίηση – εθνικός ή θρησκευτικός φανατισμός
- διακίνηση ναρκωτικών
- απειλές συστημάτων που σχετίζονται με το διάστημα[1]

Από τα παραπάνω γίνεται αντιληπτό ότι εκτός των στοιχείων και προϋποθέσεων που εντάσσουν τις αναφερόμενες απειλές στην κατηγορία ασύμμετρων απειλών, βασικό κοινό χαρακτηριστικό που παρουσιάζουν όλες είναι η απουσία χωρικών ορίων, είτε αυτά ονομάζονται σύνορα κρατών, είτε διάκριση ηπείρων. Κάθε μία από τις περιπτώσεις αφορά σε διεθνές πρόβλημα, στο οποίο δεν υπάρχουν τοπικά όρια και οι προβληματική των αλληλεξαρτήσεων και εγκληματογόνων επιρροών μπορεί να εμπλέξει πολλές περιοχές, ανεξαρτήτως διοικητικής υπαγωγής.

Ένα άλλο αξιοπρόσεκτο χαρακτηριστικό των συγκεκριμένων απειλών εντοπίζεται στην ανυπαρξία συγκεκριμένου μοτίβου εγκληματικών ενεργειών (ακανόνιστο modus operandi), το οποίο όμως βάλει τα τρωτά σημεία των στόχων. Έχοντας ως βασική επιδίωξη να καταφέρει ένα ισχυρό πλήγμα στην αποφασιστικότητα του αντιπάλου, αλλά και των συντελεστών ισχύος κάθε οργανωμένης κοινωνικής δομής (φορείς, θεσμοί και υπηρεσίες κράτους υπεύθυνες στη διαφύλαξη της δημόσιας ασφάλειας), τέτοιες μέθοδοι ακολουθήθηκαν κατά κόρον από ασθενέστερες δυνάμεις εναντίον πολύ ισχυρότερων αντιπάλων, κυβερνήσεων κρατών, πολυεθνικών οντοτήτων και συλλογικών οργανισμών άμυνας και ασφάλειας. Οι συνέπειες που προκαλούνται είναι δυσανάλογες και πολλαπλάσιες, με μία λέξη «ασύμμετρες», τόσο σε ανθρώπινες ζωές, όσο και λοιπές επιπτώσεις σε σχέση με τα χρησιμοποιούμενα «όπλα» [24]. Παρά το γεγονός ότι η εθνική ασφάλεια αναφέρεται σε στρατιωτικό επίπεδο, τα περιστατικά δεν αφορούν μόνο στα πεδία των μαχών, αλλά πλήττουν κατά κύριο λόγο τις κοινωνίες σε όλες τις μορφές των δομών τους, καθώς επίσης και τις κρίσιμες υποδομές αυτών.

Πλείστα παραδείγματα των απειλών αυτών έχουν απασχολήσει και εξακολουθούν ν‘ απασχολούν παγκοσμίως. Κάποια χαρακτηριστικά εξ αυτών, τα οποία λόγω της κρισιμότητάς τους και των συνεπειών που προκάλεσαν αποτέλεσαν το έναυσμα για ανασχεδίαση των μέτρων αντιμετώπισης, αλλά και κάποια ιδιαιτέρως πρόσφατα, αναδεικνύουν αφενός ότι ο κίνδυνος είναι διαρκής και παρών, αφετέρου ότι ανάλογες ενέργειες μπορούν ν‘ αποβούν ιδιαιτέρως καταστροφικές και να δημιουργήσουν κλίμα ανασφάλειας, είναι:

[1] Γ.Ε.ΕΘ.Α., Διακλαδικός Κανονισμός 0-4/2006 Κοινή ορολογία ενόπλων δυνάμεων

- Βομβιστικές επιθέσεις στο μετρό του Παρισιού, την 25-07-1995 με θύματα 8 νεκρούς και 80 τραυματίες και την 03-12-1996 με θύματα 4 νεκρούς και περισσότερους από 180 τραυματίες.
- Οι τρομοκρατικές επιθέσεις της 11-09-2001 στους δίδυμους πύργους της Νέας Υόρκης, με ανθρώπινες απώλειες που υπολογίζονται σε 2.995, και τραυματίες που ξεπερνούν τους 25.000.
- Τρομοκρατική βομβιστική επίθεση την 12-10-2002 το Μπαλί της Ινδονησίας είχε ως αποτέλεσμα τον θάνατο 202 ανθρώπων και τον τραυματισμό περισσοτέρων από 200.
- Συντονισμένες βομβιστικές επιθέσεις της 11-3-2004 στον προαστιακό σιδηρόδρομο της Μαδρίτης με απολογισμό 191 νεκρούς και 1.800 τραυματίες.
- Ένοπλη επίθεση και ομηρία την 01/03-09-2004 σε σχολείο του Μπεσλάν της Βόρειας Οσσετίας της Ρωσίας οδήγησε στο θάνατο 334 ανθρώπους, ανάμεσα στους οποίους 186 παιδιά
- Βομβιστικές επιθέσεις της 07-07-2005 στο μετρό του Λονδίνου είχαν ως αποτέλεσμα τον θάνατο 56 ανθρώπων και τον τραυματισμό πλέον των 700.
- Δύο διαδοχικές δολοφονικές επιθέσεις, στο Όσλο και στο νησί Ουτόγια της Νορβηγίας την 22-07-2011, με αποτέλεσμα να σκοτωθούν 92 άνθρωποι και να τραυματιστούν 209.
- Βομβιστική επίθεση και ομηρία σε σχολείο του στρατού του Πακιστάν στην πόλη Πεσαβάρ την 16-12-2014 είχε ως αποτέλεσμα 141 νεκρούς, στην πλειονότητά τους παιδιά και έφηβοι
- Επίθεση κουκουλοφόρων την 07-01-2015 στα Γραφεία της σατυρικής εφημερίδας Charlie Hebdo με απολογισμό 12 νεκρούς και 11 τραυματίες και πολλαπλή βομβιστική επίθεση την 13-11-2015 στο θέατρο Μπατακλάν στο Παρίσι με 136 νεκρούς και πλέον των 352 τραυματιών.
- Τρομοκρατική βομβιστική επίθεση στη λεωφόρο Ιστικλάρ της Κωνσταντινούπολης την 13-11-2022, όπου έχασαν τη ζωή τους 6 άνθρωποι και τραυματίσθηκαν άλλοι 81. Η συγκεκριμένη επίθεση, δεν ήταν η μόνη στην Κωνσταντινούπολη, καθώς την 1-1-2017, 39 άνθρωποι έχασαν τη ζωή τους και άλλοι 79 τραυματίσθηκαν σε πυροβολισμούς από έναν οπλισμένο δράστη σε νυχτερινό κέντρο διασκέδασης, την 10-12-2016, πραγματοποιήθηκε διπλή επίθεση κοντά στο γήπεδο της ποδοσφαιρικής ομάδας Μπεσίκτας με θλιβερό απολογισμό 47 νεκρούς και 160 τραυματίες, ενώ τον θλιβερό κατάλογο συμπληρώνει και η τριπλή επίθεση αυτοκτονίας στο αεροδρόμιο Ατατούρκ την 28-6-2016, με 45 νεκρούς και 163 τραυματίες.

Ο πλήρης κατάλογος των περιπτώσεων αυτών είναι μακρύς και ο πλουραλισμός του είναι τέτοιος που αφορά στο σύνολο του Πλανήτη.

Τέλος, πλέον των όσων ήδη αναφέρθηκαν, υπάρχουν και πληθώρα περιστατικών που συνιστούν απειλή και τα οποία μπορούν να οδηγήσουν σε κατάσταση κρίσης, ή κρίσιμου περιστατικού, με αυξημένες απαιτήσεις σε όλα τα επίπεδα διαχείρισης. Χαρακτηριστικότερα εξ αυτών είναι οι βομβιστικές ενέργειες, οι επιθέσεις σε χώρους εστίασης, οι αεροπειρατείες, οι απαγωγές, οι οποιεσδήποτε καταστάσεις ομηρίας, οι δολοφονίες και τραυματισμοί και οι παράνομες εκδηλώσεις εκφοβισμού. Αυτού του είδους οι τρομοκρατικές ή ποινικά κολάσιμες ενέργειες έχουν ως αποτέλεσμα τη δημιουργία απρόβλεπτων καταστάσεων, ιδιαιτέρως εύθραυστων που εξελίσσονται με ταχύτητα, με κίνδυνο να ξεφύγουν από κάθε έλεγχο και να δημιουργήσουν απαιτήσεις λήψης προληπτικών και κατασταλτικών μέτρων αποκατάστασης, θεραπείας και ελέγχου, καθώς και ενέργειες διαχείρισης συνεπειών και απωλειών για την αποφυγή της κλιμάκωσης ή τον περιορισμό της έντασης και έκτασης αυτής.

2.4 Διαχείριση του κινδύνου

Η εξήγηση που δίνει ο άνθρωπος στις φυσικές και ανθρωπογενείς καταστροφές έχει διαφοροποιηθεί στο πέρασμα των χρόνων. Από την εποχή που οι άνθρωποι αντιμετώπιζαν τα φυσικά φαινόμενα ως θεομηνία, θεϊκή οργή ή τιμωρία, έως την πλήρη αντίληψη και την επιστημονική εξήγηση αυτών έχουν καταγραφεί σημαντικότατες εξελίξεις. Παράλληλα και για τους ίδιους λόγους διαφοροποιήθηκε και μετεξελίχθηκε ο τρόπος αντιμετώπισής τους. Μία χαρακτηριστική καμπή της αναφερόμενης μετεξέλιξης θεωρείται ο σεισμός της Λισσαβόνας της 1ης Νοεμβρίου 1755, ο οποίος, όπως χαρακτηριστικά γράφει ο Π. Αναγνωστόπουλος «προκάλεσε ισχυρότατους διανοητικούς μετασεισμούς σε όλη την Ευρώπη» [25].

Πως όμως έχει μοντελοποιηθεί ο τρόπος αντιμετώπισης των φυσικών και ανθρωπογενών καταστροφών, στις οποίες αναφερθήκαμε συνοπτικά στα προηγούμενα κεφάλαια; Η συνολική προσπάθεια που αφορά στη βελτίωση της ετοιμότητας, στη συνετή διαχείριση των φυσικών περιβαλλοντικών πηγών, στη στάθμιση των αιτιών και μείωση των επιφανειών τρωτότητας για τις φυσικές καταστροφές, απαντά στον ενιαίο πλέον παγκόσμια αποδεκτό και αναγνωρίσιμο τίτλο Μείωση Κινδύνου Καταστροφών (Disaster Risk Reduction –DRR). Υπό τον τίτλο αυτό έχουν καταγραφεί συνεργατικές στρατηγικές πέρα από τοπικά, περιφερειακά ή εθνικά όρια. Οι τρομακτικές κοινωνικές και οικονομικές συνέπειες των φυσικών καταστροφών είναι αυτές που έδειξαν ότι η συνεργασία είναι η μόνη οδός δια της οποίας θα έρθει το επιθυμητό αποτέλεσμα. Συνεπώς, ο σχεδιασμός χωρίς χωρικά πλαίσια οδήγησε στην ανάγκη λήψης πρωτοβουλιών από τη διεθνή κοινότητα. Αξίζει στο σημείο αυτό να

παρατεθούν επιγραμματικά κομβικής σημασίας πρωτοβουλίες που σκιαγραφούν την στρατηγική αντιμετώπισης παγκοσμίως:

α)Τις δεκαετίες 1960, 1970 και 1980 ο Ο.Η.Ε. στο πλαίσιο των μέτρων που λαμβάνει για την ανακούφιση των πληγέντων από φυσικές καταστροφές, δραστηριοποιήθηκε στην έρευνα για την αξιοποίηση της τεχνολογίας, στη μάχη για την έγκαιρη ενημέρωση, πρόληψη και αντιμετώπιση των κινδύνων και επιπτώσεων από φυσικές καταστροφές. Έτσι, το 1971 δημιουργήθηκε το Γραφείο Αρωγής των Ηνωμένων Εθνών σε Καταστροφές (United Nations Disaster Relief Office - UNDRO).

β)Το 1987, στο πλαίσιο Γενικής Συνέλευσης των Ηνωμένων Εθνών, ορίσθηκε η δεκαετία 1990 - 1999 ως διεθνής δεκαετία για τη μείωση των φυσικών καταστροφών. Πλέον της αναγνώρισης της σημασίας για τη μείωση των επιπτώσεων από φυσικές καταστροφές, αποφασίζεται να δοθεί ιδιαίτερη προσοχή στην προώθηση της συνεργασίας σε παγκόσμιο επίπεδο.

γ)Χαρακτηριστικό της προσπάθειας για ευαισθητοποίηση και προώθηση της παγκόσμιας κουλτούρας για τη μείωση των καταστροφών είναι ότι το 1989, στο πλαίσιο Γενικής Συνέλευσης των Ηνωμένων Εθνών, ορίσθηκε η 13^{η} Οκτωβρίου ως διεθνής ημέρα για τη μείωση του κινδύνου καταστροφών. Σήμερα η ημέρα αυτή έχει ορισθεί ως η δεύτερη Τετάρτη του μηνός Οκτωβρίου κάθε έτους.

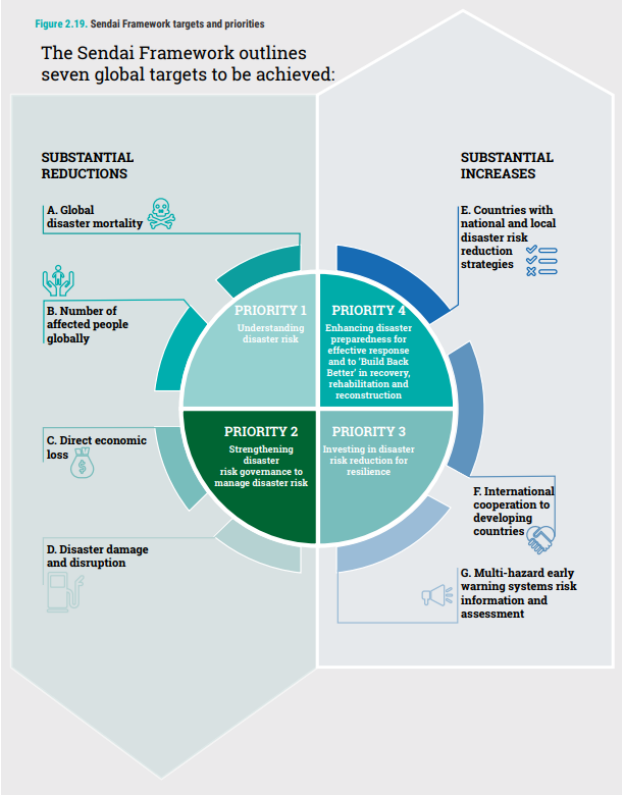
δ)Στο ίδιο πλαίσιο ευαισθητοποίησης εντάσσεται το βραβείο των Ηνωμένων Εθνών Sasakawa που θεσπίστηκε το 1986 από τον Πρόεδρο του Nippon Foundation, κ. Ryoichi Sasakawa για την αναγνώριση της αριστείας στη μείωση του κινδύνου καταστροφών. Το έτος 2022 το βραβείο απονεμήθηκε στη μη κερδοσκοπική οργάνωση Κοινωνία Βιώσιμης, Οικολογικής και Περιβαλλοντικής Ανάπτυξης (Sustainable, Ecological and Environmental Development Society - SEEDS) που δραστηριοποιείται στον τομέα της μείωσης του κινδύνου καταστροφών και της κλιματικής αλλαγής [26]

ε)Τον Μάιο του 1994 στη Γιοκοχάμα της Ιαπωνίας πραγματοποιήθηκε παγκόσμια διάσκεψη για τη μείωση των φυσικών καταστροφών Διεθνής Δεκαετία για τη Μείωση των Φυσικών Καταστροφών (International Decade for Natural Disaster Reduction - IDNDR) και συντάχθηκε συμφωνία όλων των μελών για συνεργασία. Το έγγραφο αυτό όρισε τη στρατηγική, τις δράσεις και τις συνολικές κατευθυντήριες γραμμές για την πρόληψη, την ετοιμότητα και τον μετριασμό των φυσικών καταστροφών [27]

στ)Τον Ιανουάριο του 2005 στο Κόμπε, Χόγκο της Ιαπωνίας πραγματοποιήθηκε η δεύτερη παγκόσμια διάσκεψη των Ηνωμένων Εθνών για τη μείωση των φυσικών καταστροφών και υιοθετήθηκε ένα πλαίσιο δράσης για το διάστημα 2005 – 2015 [28], που είχε ως στόχο την οικοδόμηση της ανθεκτικότητας των εθνών και των κοινοτήτων στις καταστροφές, με τις προσπάθειες να κατατείνουν στη μείωση της τρωτότητας και του

κινδύνου. Επισημάνθηκαν κενά και προκλήσεις στους τομείς της διακυβέρνησης, του προσδιορισμού, αξιολόγησης και έγκαιρης προειδοποίησης κινδύνου, της εκπαίδευσης, της μείωσης των παραγόντων που προκαλούν τον κίνδυνο και της ετοιμότητας.

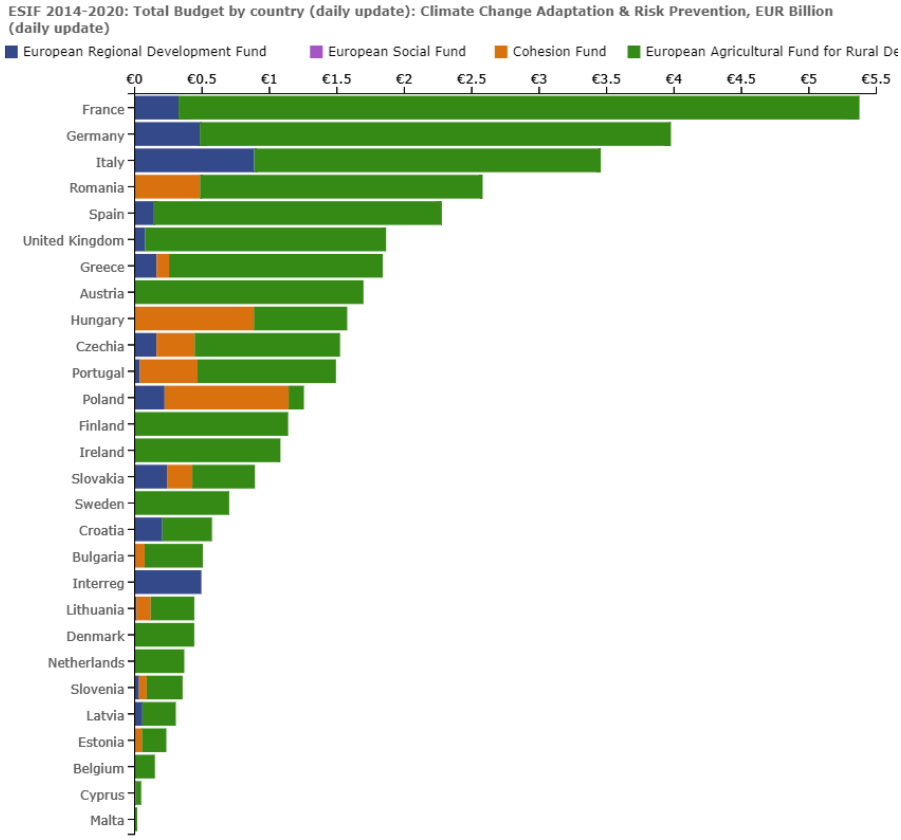
ζ)Τον Μάρτιο του 2015 στο Σεντάι της Ιαπωνίας πραγματοποιήθηκε η τρίτη παγκόσμια διάσκεψη των Ηνωμένων Εθνών για τη μείωση των φυσικών καταστροφών και εγκρίθηκε το πρόγραμμα - πλαίσιο για τα έτη 2015 – 2030 [29] . Μάλιστα, οι εργασίες προετοιμασίας είχαν ξεκινήσει ήδη από το 2012. Το συγκεκριμένο πρόγραμμα αποτελεί συμπλήρωμα της συμφωνίας της Γιοκοχάμα και συνάμα αξιολόγηση των πεπραγμένων της συμφωνίας του Κόμπε, Χόγκο. Επισημάνθηκαν εκ νέου στρατηγικοί πυλώνες προτεραιοτήτων και συγκεκριμένα κατανόηση του κινδύνου, ενίσχυση της διακυβέρνησης, αύξηση των επενδύσεων για την ανθεκτικότητα και ενίσχυση της ετοιμότητας, της αποτελεσματικής αντιμετώπισης και της καλύτερης ανοικοδόμησης και αποκατάστασης (Εικόνα 8). Στο πλαίσιο εφαρμογής των κατευθυντήριων στρατηγικών υλοποιήθηκαν και εξακολουθούν να υλοποιούνται διάφορες δράσεις σε όλο το φάσμα των ξεχωριστών αντικειμένων που συνθέτουν τη συμφωνία. Συγκεκριμένα παραδείγματα αποτελούν το «Στρατηγικό πλαίσιο 2016 - 2021» [30], το «Στρατηγικό πλαίσιο 2022 - 2025» [31], καθώς και το γεγονός ότι μέσω του Γραφείο Ηνωμένων Εθνών για τη μείωση του κινδύνου καταστροφών (United Nations Office for Disaster Risk Reduction - UNDRR) εκδίδεται κάθε δύο χρόνια παγκόσμια έκθεση αξιολόγησης των Ηνωμένων Εθνών (Global Assessment Report - GAR) [9].



Εικόνα 8. Οι στόχοι και προτεραιότητες του προγράμματος - πλαισίου Sendai [9]

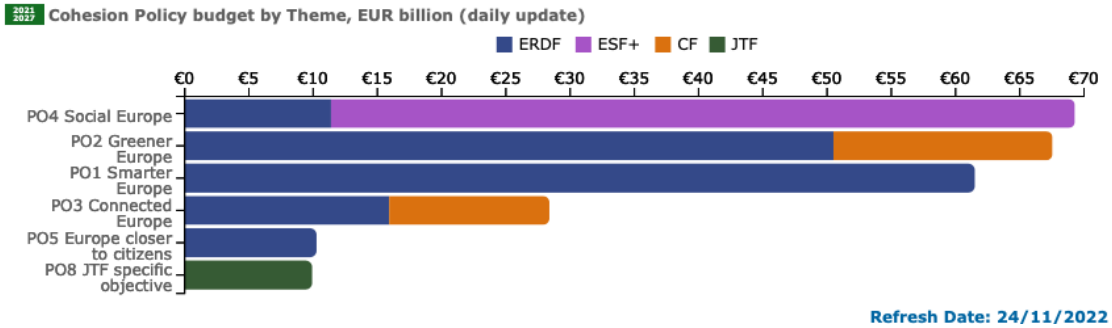
η)Αντίστοιχα, η Ευρωπαϊκή Ένωση έχει λάβει τις δικές της πρωτοβουλίες επί του ζητήματος. Το 1987 θεσπίστηκε το μόνιμο δίκτυο εθνικών αντιπρόσωπων για την προώθηση της συνεργασίας των κρατών μελών σε θέματα πολιτικής προστασίας, το οποίο λειτουργούσε ως φορέας ανταλλαγής πληροφοριών και εξέταζε πρωτοβουλίες του τομέα της πολιτικής προστασίας. Από τότε πραγματοποιήθηκε πλήθος σχετικών δράσεων, οι οποίες αρκετά αργότερα και συγκεκριμένα το 2001 ιδρύθηκε ο Μηχανισμός Πολιτικής Προστασίας της Ευρωπαϊκής Ένωσης [32], δια του οποίου προωθείται η συνεργασία μεταξύ των κρατών μελών, αλλά και έξι ακόμη κρατών, που δεν είναι μέλη και υπέγραψαν τη σχετική συμφωνία (Ισλανδία, Νορβηγία, Σερβία, Βόρεια Μακεδονία, Μαυροβούνιο και Τουρκία). Ο Μηχανισμός επικαιροποιήθηκε και βελτιώθηκε το 2007 [33]. Στο πλαίσιο λειτουργίας του συγκεκριμένου φορέα έχει γίνει πολύ δουλειά και έχουν αναληφθεί πρωτοβουλίες που φιλοδοξούν να υποστηρίξουν και συμπληρώσουν τις προσπάθειες πρόληψης και ετοιμότητας των κρατών μελών και των συμμετεχόντων κρατών, εστιάζοντας σε τομείς όπου μια κοινή ευρωπαϊκή προσέγγιση είναι πιο αποτελεσματική από τις χωριστές εθνικές δράσεις. Οι προσπάθειες αυτές περιλαμβάνουν την εκτίμηση των κινδύνων, την ενθάρρυνση της έρευνας για την προώθηση της ανθεκτικότητας σε καταστροφές και την ενίσχυση των εργαλείων έγκαιρης προειδοποίησης, δια της εντάξεων των τεχνολογικών εξελίξεων. Η αξιολόγηση των κινδύνων και η ικανότητα στη διαχείρισή τους πραγματοποιείται από τα συμμετέχοντα κράτη κάθε τρία έτη, ενώ τα συμπεράσματα τίθενται υπόψη της αναφερόμενης επιτροπής ώστε ακολούθως να ληφθούν αποφάσεις. Τα προγράμματα στοχεύουν να στηρίξουν πρωτίστως τη διασυνοριακή και διακρατική συνεργασία, καθώς ο εγγενής χαρακτήρας των καταστροφών είναι διασυνοριακός. Στην κατεύθυνση αυτή προωθείται η υλοποίηση στρατηγικών έργων και η συνεργασία σε όλους τους τομείς, τα επίπεδα διακυβέρνησης και τα ενδιαφερόμενα μέρη.

Η βασική πηγή χρηματοδότησης που φιλοδοξεί να υλοποιήσει τον αναφερόμενο σχεδιασμό αντλείται από τα Ευρωπαϊκά Διαρθρωτικά και Επενδυτικά Ταμεία (Ε.Δ.Ε.Τ.). Χαρακτηριστικό είναι ότι την περίοδο 2014-2020, κατανεμήθηκαν στα κράτη μέλη συνολικά περισσότερα από 26 δισεκατομμύρια ευρώ από τη χρηματοδότηση των Ε.Δ.Ε.Τ. για επενδύσεις στην προσαρμογή στην κλιματική αλλαγή και την πρόληψη και διαχείριση κινδύνων (Εικόνα 9) [34]. Η συγκεκριμένη οικονομική πολιτική, η οποία καταδεικνύει τη σοβαρότητα με την οποία αντιμετωπίζει η Ευρωπαϊκή Ένωση το ζήτημα έχει την ίδια ακριβώς συνέχεια στη νέα χρηματοδοτική περίοδο του 2021 – 2027. Συγκεκριμένα, θα δαπανηθούν συνολικά 350 δισεκατομμύρια ευρώ και αυτά θα επιμεριστούν σε πέντε διακριτούς στόχους – πυλώνες του ευρύτερου σχεδιασμού της πολιτικής συνοχής της Ευρωπαϊκής Ένωσης, ανά θεματική σύμφωνα με την αποτύπωση που προκύπτει στην Εικόνα 11 και ανά κράτος συμμετοχής, σύμφωνα με την αποτύπωση που προκύπτει στην Εικόνα 10.

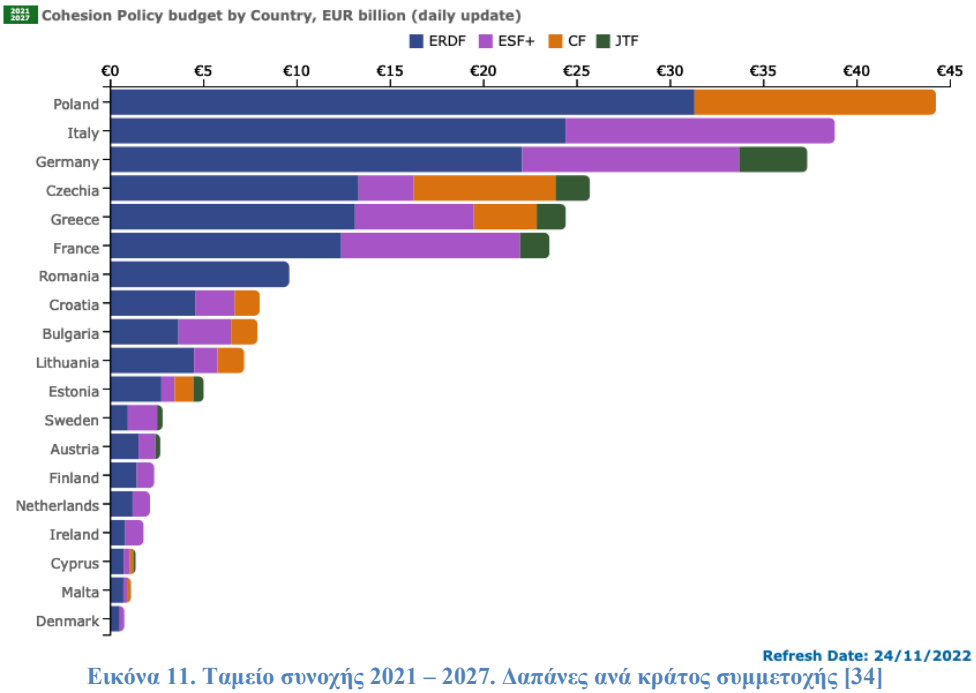


Εικόνα 9. Χρηματοδότηση της πολιτικής συνοχής της Ευρωπαϊκής Ένωσης για την πρόληψη και διαχείριση κινδύνων το 2014-2022 [34]

θ)Στην πολιτική που χάραξε η Ευρωπαϊκή Ένωση, η Χώρα μας συμμετέχει στον Μηχανισμό Πολιτικής Προστασίας, καθώς και σε πληθώρα δράσεων και έργων που σχετίζονται με την αντιμετώπιση των κινδύνων από καταστροφές. Η συμμετοχή αυτή έχει θεσμοθετηθεί νομικά με την εφαρμογή των διατάξεων του Ν. 4662/2020 (ΦΕΚ Α΄ 27/7-7-2020), ενώ με τις διατάξεις του Π.Δ/τος 70/2021 (ΦΕΚ Α΄ 161/9-9-2021) συστήθηκε Υπουργείο Κλιματικής Κρίσης και Πολιτικής Προστασίας, ως μια από τις σημειολογικά σημαντικές κινήσεις της σπουδαιότητας με την οποία αντιμετωπίζεται πλέον το θέμα.



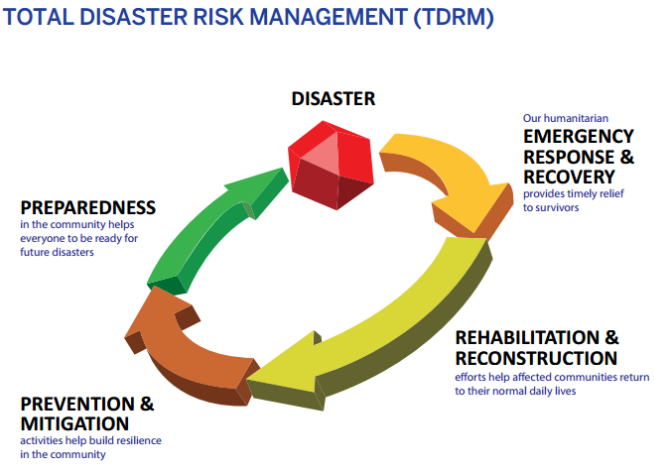
Εικόνα 10. Ταμείο συνοχής 2021 – 2027. Συνολικές δαπάνες [34]



Εικόνα 11. Ταμείο συνοχής 2021 – 2027. Δαπάνες ανά κράτος συμμετοχής [34]

Τι περιλαμβάνει λοιπόν ο όρος διαχείριση καταστροφών; Στο ερώτημα αυτό το δίκτυο ανάπτυξης των Ηνωμένων Εθνών με τίτλο Αναπτυξιακό πρόγραμμα των Ηνωμένων Εθνών (United Nations Development Program - UNDP) που δραστηριοποιείται σε πλέον των 170 χωρών παγκοσμίως για την εξάλειψη της φτώχειας, τη μείωση των ανισοτήτων και του αποκλεισμού και την οικοδόμηση ανθεκτικότητας, ώστε οι χώρες να μπορούν να διατηρήσουν την πρόοδο, απαντά ότι η «διαχείριση καταστροφών» αφορά στο σύνολο των τακτικών και διαχειριστικών αποφάσεων, καθώς και επιχειρησιακών δραστηριοτήτων για τα διάφορα στάδια μιας καταστροφής σε όλα τα επίπεδα. Κάποιες από τις βασικές στοχεύσεις που εντάσσονται στο πλαίσιο του όρου αυτού είναι η δυνατότητα πρόληψης, η μείωση ή αποφυγή των ζημιών που προκαλούνται, η ταχεία και αποτελεσματική ανάκαμψη, η οποία ξεκινά αμέσως μόλις η καταστροφή λαμβάνει χώρα, καθώς και η διασφάλιση άμεσης βοήθειας. Οι στόχοι αυτοί εντάσσονται σε συγκεκριμένες δράσεις και σχεδιαστικά πλάνα που λαμβάνουν διάφορους φορμαλισμούς. Ο σπουδαιότερος και δημοφιλέστερος εξ αυτών, που συναντούμε ευρέως στη βιβλιογραφία, αναφέρεται στον κύκλο διαχείρισης των καταστροφών [19] [21], αν και υφίστανται διαφοροποιήσεις σχετικά με τις φάσεις ή τα μέρη στα οποία κατακερματίζεται. Η άποψη των [21] θεωρεί τον κύκλο τεσσάρων φάσεων που αναπτύχθηκε για την Πρόληψη, Προετοιμασία, Αντίδραση, Ανάρρωση που είναι πλέον γνωστή με το ακρωνύμιο PPRR (Prevention, Preparation, Response, Recovery) (Εικόνα 12):

- Πρόληψη και μετριασμός (Prevention and Mitigation)
- Προετοιμασία / Ετοιμότητα (Preparedness)
- Απόκριση (Response)
- Αποκατάσταση (Recovery, rehabilitation and reconstruction)



Εικόνα 12. Κύκλος διαχείρισης καταστροφών

Ενδιαφέρον βέβαια παρουσιάζει και η θεώρηση του [7], σύμφωνα με την οποία υφίστανται τρείς φάσεις:

- Της ανάπτυξης και σχεδιασμού που προηγείται της καταστροφής
- Των επιπτώσεων, που λαμβάνει ώρα κατά τη διάρκεια και αμέσως μετά το καταστροφικό γεγονός
- Της απόκρισης και δράσης, που έπεται της καταστροφής

Μια ακόμη σημαντική προσέγγιση του θέματος, στην ίδια φιλοσοφία και άμεσα επηρεασμένη από τον κύκλο διαχείρισης έργων της Ευρωπαϊκής Ένωσης από την δεκαετία του 1990 προέρχεται από την Αυστραλιανή αναπτυξιακή εταιρία TorqAid που έκανε την εμφάνισή της το 1992 και έκτοτε έχει εδραιωθεί ως μια από τις σημαντικότερες ανθρωπιστικές και αναπτυξιακές εταιρίες παγκοσμίως που προσφέρει υπηρεσίες εκπαίδευσης και έρευνας. Σύμφωνα με τη συγκεκριμένη προσέγγιση, οι κύριοι στόχοι για τη διαχείριση των καταστροφών, αφορούν:

(1)Στη μείωση ή αποφυγή απωλειών από κινδύνους.
(2)Στην εξασφάλιση άμεσης βοήθειας στα θύματα.
(3)Στην επίτευξη ταχείας και αποτελεσματικής ανάκαμψης / αποκατάστασης.

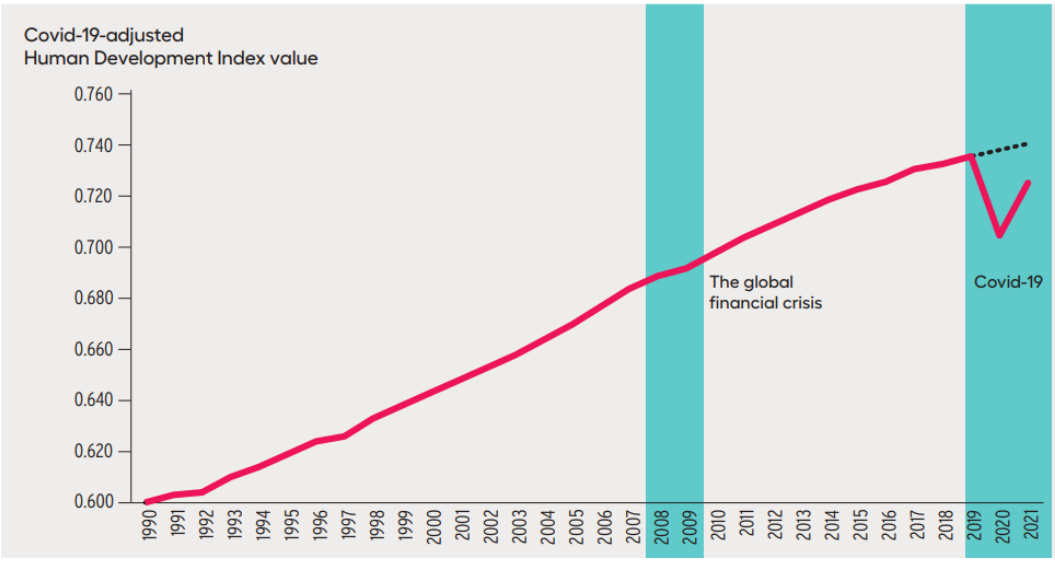
Εμπλοκή στην επαναλαμβανόμενη αυτή διαδικασία της προσπάθειας επίτευξης των ως άνω στοχεύσεων έχει το σύνολο της κοινωνίας, από τον απλό πολίτη έως τους κυβερνώντες, αλλά και τις επιχειρήσεις. Το βέλτιστο αποτέλεσμα επιτυγχάνεται όταν σε κάθε επανάληψη λαμβάνουν χώρα βελτιωμένες ενέργειες σε σχέση με τις θεματικές της ετοιμότητας, των προειδοποιήσεων και της πρόληψης.

Όπως είναι λογικό, η διαχείριση των κρίσεων που εμπεριέχουν τα στοιχεία της εγκληματικής συμπεριφοράς, τρομοκρατίας ή θεωρούνται ασύμμετρες απειλές, όπως διεξοδικά αναφέρθηκε, είναι σημαντικά διαφορετική από την αντίστοιχη της διαχείρισης των φυσικών και τεχνολογικών καταστροφών. Οι ανθρώπινες αυτές παραβατικές συμπεριφορές έχουν

απέναντί τους οργανωμένες υπηρεσίες με συγκεκριμένα σχέδια αντεγκληματικών δράσεων, για τα οποία δεν απαιτείται ιδιαίτερη ανάλυση, καθώς δεν εξυπηρετεί τους σκοπούς της παρούσας εργασίας. Σε κάθε περίπτωση, η γενικότερη φιλοσοφία σχεδιασμού της λύσης είναι παρόμοια με τον τρόπο αντιμετώπισης των καταστροφών, καθώς απαιτείται σειριακά να υλοποιηθούν ενέργειες που σχετίζονται με την πρόληψη, τον μετριασμό, την ετοιμότητα, τις επιπτώσεις, την απόκριση και την ανάκαμψη.

Είναι σημαντικό ν‘ αναφερθεί ότι όλες οι καταστάσεις που ήδη περιγράφηκαν εκτενώς, είτε αφορούν σε φυσικές ή ανθρωπογενείς καταστροφές, είτε σε ασύμμετρες απειλές, είτε σε όποια άλλης μορφής απειλή σε βάρος της ανθρώπινης ζωής και των περιουσιών του ανθρώπου, πλήττουν καίρια το αίσθημα της ασφάλειας, στην σπουδαιότητα του οποίου αναφερθήκαμε ήδη, καθώς αποτελεί τη δεύτερη κατά σειρά ανάγκη του ανθρώπου σύμφωνα με την πυραμίδα αναγκών του Maslow [2]. Η ανασφάλεια έχει χαρακτηριστικό αρνητικό αντίκτυπο στον άνθρωπο και επηρεάζει δραματικά την καθημερινότητά του. Εμφατικό παράδειγμα της αναφερόμενης παραδοχής αποτελεί το διάγραμμα που παρουσιάζεται στην Εικόνα 13, όπου η ρηγματώδης κάμψη του δείκτη ανθρώπινης ανάπτυξης είναι το αποτέλεσμα των συνεπειών της ανασφάλειας που δημιούργησε η πανδημία της Covid-19. Ταυτόχρονα, η πανδημία πυροδότησε τη μεγαλύτερη παγκόσμια οικονομική κρίση σε περισσότερο από έναν αιώνα, καθώς η οικονομική δραστηριότητα συρρικνώθηκε το 2020 στο 90% των χωρών παγκοσμίως και η παγκόσμια φτώχεια αυξήθηκε για πρώτη φορά μέσα σε μία γενιά [35].

Ενδεικτικό της διαμορφωθείσας κατάστασης είναι ότι οι άνθρωποι που επωφελούνται από καλού επιπέδου υπηρεσίες υγείας, είναι εύποροι και το μορφωτικό τους επίπεδο είναι υψηλότερο, εμφανίζουν μεγαλύτερα επίπεδα άγχους και ανασφάλειας συγκριτικά με τα αντίστοιχα της προηγούμενης δεκαετίας [36].



Εικόνα 13. Παγκόσμιος δείκτης ανθρώπινης ανάπτυξης [36]

2.5 Απαιτήσεις στις επικοινωνίες δημόσιας ασφάλειας

Η ανάλυση των καταστάσεων που μπορούν να θίξουν τη δημόσια ασφάλεια, οι οποίες δύναται ν' απαντηθούν στην καθημερινότητα του ανθρώπου, δημιούργησε το ανάγλυφο του πλαισίου των πραγματικών συνθηκών που καλούνται να αντιμετωπίσουν οι άνθρωποι που εκ της φύσης των καθηκόντων τους κατά βάση, ή ενδεχομένως στο πλαίσιο του εθελοντισμού, έχουν ορισθεί - διατεθεί προς τούτο. Από το ανάγλυφο αυτό πηγάζουν συγκεκριμένες απαιτήσεις - ανάγκες για τους ανθρώπους της δημόσιας ασφάλειας. Το εύρος των απαιτήσεων είναι μεγάλο, αλλά και πολυσχιδές. Το ενδιαφέρον μας, στο πλαίσιο της παρούσας εργασίας στρέφεται καθαρά στα θέματα της επικοινωνίας. Ακόμη και εκεί, θα θεωρήσουμε δύο πλήρως διακριτά επίπεδα απαιτήσεων. Αυτό των γενικότερων απαιτήσεων επικοινωνίας, που θα θέσει τις βάσεις για να εξειδικευτούν στη συνέχεια οι λειτουργικές και τεχνολογικές απαιτήσεις και προκλήσεις. Κάθε μία από αυτές πηγάζει από τη θεμελιώδη ανάγκη να ανταποκριθούμε στις καταστάσεις, έτσι όπως διαμορφώνονται και αναλύθηκαν ήδη.

2.5.1 Γενικές - λειτουργικές απαιτήσεις

Ως συνέχεια των όσων αναφέρθηκαν ήδη, πέντε είναι οι βασικοί πυλώνες απαιτήσεων και συγκεκριμένα [37]:

α)Στιβαρότητα και αξιοπιστία. Η ανάγκη για απρόσκοπτη επικοινωνία με το σημείο, ή τα σημεία που έλαβε χώρα ή εξελίσσεται το περιστατικό δημόσιας ασφάλειας, ή διαδραματίζεται το επιχειρησιακό σκέλος αυτού, κρίνεται μείζονος σημασίας, καθώς συναρτάται άμεσα με την επιτυχία ή αποτυχία της αποστολής. Οι άνθρωποι της δημόσιας ασφάλειας ενεργούν στο πεδίο με βάση συγκεκριμένο σχέδιο και πλάνο και τελούν σε διαρκή επικοινωνία με το επιχειρησιακό κέντρο. Μια σχέση αμφίδρομη, που περιλαμβάνει ανατροφοδότηση / ανταλλαγή κρίσιμων πληροφοριών ώστε αφενός να διαμορφωθεί η ασφαλής και με πλήρη σαφήνεια εικόνα του περιστατικού και διαλευκανθούν όλες οι πτυχές και παράμετροι που το περιγράφουν, σε όλο το γεωγραφικό του εύρος, και αφετέρου να μεταφερθούν οι κρίσιμες εντολές για τον χειρισμό του, στο πλαίσιο της λήψης αποφάσεων. Όπως είναι λογικό, οποιαδήποτε διακοπή στη συγκεκριμένη επικοινωνία, ή έστω τυχόν προβλήματα θα μπορούσαν να αποβούν επιζήμια και να κοστίσουν ανθρώπινες ζωές. Αξίζει στο σκέλος αυτό να γίνει ξεχωριστή μνεία στην ιδιαίτερη πρόκληση που η απρόσκοπτη επικοινωνία πρέπει να επιτευχθεί και να διατηρηθεί όταν η τεχνολογική υποδομή της έχει τεθεί εκτός λειτουργίας, λόγω φθοράς ή πλήρους καταστροφής. Ο καλύτερος τρόπος να οραματιστεί οποιοσδήποτε τη σημαντικότητα της στιβαρότητας και αξιοπιστίας του δικτύου επικοινωνίας δημόσιας ασφάλειας είναι να μπει στη θέση του αστυνομικού που ενεργεί

επιχειρησιακά στο πλαίσιο μιας ομηρίας και έχει λάβει την εντολή για επέμβαση, σε σχέση με την επικοινωνία του με τα υπόλοιπα μέλη της ομάδας και τον επικεφαλής.

β)Απόλυτη ασφάλεια. Η έννοια της δημόσιας ασφάλειας σε όλες τις θεματικές της, δεν θα μπορούσε να αφήνει περιθώρια ή να κάνει εκπτώσεις στο θέμα της ασφάλειας των επικοινωνιών. Μολυσματικό – κακόβουλο λογισμικό, επιθέσεις ενδιάμεσου, επιθέσεις άρνησης παροχής υπηρεσιών, επιθέσεις ransomware και κάθε άλλου είδους επιθέσεις θα μπορούσαν να δημιουργήσουν ολέθρια προβλήματα στις κρίσιμες επικοινωνίες, καθώς πλέον από τις προφανείς καταστάσεις που οποιαδήποτε τέτοια δόλια παρέμβαση θα καθιστούσε προβληματική την ανταπόκριση των ανθρώπων της δημόσιας ασφάλειας, κρίσιμης σημασίας πληροφορίες ή πρόσβαση θα αποκτούσαν δυνητικά άνθρωποι που δεν σχετίζονται με τη δημόσια ασφάλεια και έχουν εγκληματικούς σκοπούς. Γίνεται ξεκάθαρο, εάν θεωρήσουμε το παράδειγμα κατά το οποίο όταν σε μια οργανωμένη επιχείρηση για σύλληψη εμπόρων ναρκωτικών στο πλαίσιο μιας διασυνοριακής επιχείρησης, ή αντίστοιχα σε μια οργανωμένη επιχείρηση για σύλληψη τρομοκρατών, στις επικοινωνίες μεταξύ των ανθρώπων της δημόσιας ασφάλειας παρεμβάλλουν τρίτοι, που σχετίζονται μάλιστα με την διωχθείσα εγκληματική δραστηριότητα.

γ)Διαλειτουργικότητα. Βρίσκεται στο κύτταρο των κρίσιμων επικοινωνιών, καθώς αποτελεί έναν από τους κύριους σκοπούς δημιουργίας ενός δικτύου επικοινωνίας δημόσιας ασφάλειας. Η συγκεκριμένη παραδοχή εξηγείται με σαφήνεια αφού ο κίνδυνος, η απειλή και η αναγκαιότητα που έχει να αντιμετωπίσει κάθε ένας εκ των ανθρώπων της δημόσιας ασφάλειας που ενεργεί στο πεδίο, δεν «ενδιαφέρεται» για το χρώμα της στολής που έχει απέναντί του, ούτε για το είδος του αντικειμένου για το οποίο είναι υπεύθυνος. Ταυτόχρονα, η διαλειτουργικότητα εξυπηρετεί με τον καλύτερο δυνατό τρόπο τη συνεργασία, που καθίσταται απαραίτητη, ειδικότερα σε μεγάλης κλίμακας επιχειρήσεις ή δράσεις. Αξίζει βέβαια να σημειωθεί ότι η περισσότερο εμφατική της μορφής βρίσκει έρεισμα στις διακρατικές συνεργασίες, όπου οι άνθρωποι της δημόσιας ασφάλειας που δρουν στο πεδίο και επικοινωνούν μεταξύ τους προέρχονται τόσο από διαφορετικές υπηρεσίες, όσο και από διαφορετικές χώρες. Ο όρος διαλειτουργικότητας έχει ευρύ φάσμα που εκτείνεται και καλύπτει από τη δυνατότητα να επικοινωνεί επιτυχημένα και αποδοτικά η νέας προμήθειας συσκευή που κατέχει ο πρώτος ανταποκριτής με την παλαιότερή του, μέχρι να επικοινωνεί ο ίδιος, το ίδιο αποδοτικά με τον πρώτο ανταποκριτή που βρίσκεται στο πεδίο, προέρχεται από διαφορετική υπηρεσία, επικοινωνεί με διαφορετικό κέντρο επιχειρήσεων και μιλά άλλη γλώσσα. Γίνεται ξεκάθαρα, εάν για παράδειγμα μπούμε στη θέση του Ρουμάνου πυροσβέστη που ήρθε να συνδράμει τις προσπάθειες των Ελλήνων και βρέθηκε μαζί τους στη μάχη με τις φωτιές της Εύβοιας.

δ)Απαιτήσεις υλικού. Όπως είδαμε διεξοδικά στο πρώτο σκέλος αυτού του κεφαλαίου, ο κίνδυνος και οι απειλές διαρκώς αυξάνουν και οι απαιτήσεις στη διαχείρισή τους συνεχώς μεγαλώνουν, ποιοτικά και ποσοτικά. Τούτο συναρτά αυξημένα επίπεδα ανταπόκρισης σε επιχειρησιακό σκέλος. Σ` αυτό βέβαια εντάσσεται ως αναπόσπαστο κομμάτι και η επικοινωνία. Από την αναγκαιότητα της απρόσκοπτης φωνητικής επικοινωνίας του πρόσφατου παρελθόντος, έχουμε πλέον να διαχειριστούμε τον ιδιαίτερο πλουραλισμό διαφορετικών απαιτήσεων του σήμερα. Εντελώς ενδεικτικά απαριθμούμε:

- ανταλλαγή δεδομένων,
- λήψη εικόνας σε πραγματικό χρόνο και με μεγάλη ευκρίνεια,
- ακριβής προσδιορισμός της θέσης κάθε πρώτου ανταποκριτή,
- την εκπομπή και μεταφορά των βιομετρικών ή βιολογικών στοιχείων ενός τραυματία στο ιατρικό κέντρο σε πραγματικό χρόνο,
- την επαρκή κάλυψη επικοινωνίας των ανθρώπων της δημόσιας ασφάλειας σε όλο το εύρος του χώρου επιχειρήσεων, ακόμη και εάν αυτό εκτείνεται σε χιλιόμετρα, ή εάν μεταβάλλεται δυναμικά (κινητικότητα) και δυνατότητα άμεσης αυτό-οργάνωσης του δικτύου
- ευελιξία φάσματος και παροχή συγκεκριμένου επιπέδου ποιότητας διαθέσιμων υπηρεσιών

ε)Οικονομικές πτυχές. Θα ήταν κενό γράμμα να αναφερόμαστε σε σχέδια και έργα που δεν είναι υλοποιήσιμα λόγω αυξημένου κόστους προμήθειας, εγκατάστασης αλλά και συντήρησης. Η αποδοτικότητα λοιπόν ενός δικτύου επικοινωνίας δημόσιας ασφάλειας είναι άμεσα συνυφασμένη με το κόστος και την υλοποιησιμότητά του, ήτοι με καθαρά ρεαλιστικούς δείκτες, καθώς ακόμη και εάν για δεδομένη χρονική διάρκεια απαιτηθεί μια λύση υψηλού κόστους (επί παραδείγματι η υποστήριξη με δορυφορική επικοινωνία), η κύρια λύση θα πρέπει να είναι λιγότερο δαπανηρή, ώστε να καθίσταται εφικτή και βιώσιμη. Σε κάθε περίπτωση, θα πρέπει να λάβουμε υπόψη μας ότι τα συγκεκριμένα κόστη βαρύνουν συνήθως τους κρατικούς προϋπολογισμούς και εξ ορισμού ο οικονομικός παράγοντας είναι ένας από τους βασικότερους για να κριθεί και να επιλεγεί ένα έργο.

2.5.2 Τεχνολογικές απαιτήσεις

Επί των γενικών – λειτουργικών απαιτήσεων εξειδικεύονται οι ειδικότερες τεχνολογικές που συγκεκριμενοποιούν τις απαιτήσεις λειτουργίας των δικτύων δημόσιας ασφάλειας και των κρίσιμων επικοινωνιών και ταυτόχρονα γεννούν τις προκλήσεις υλοποίησης αυτών. Μάλιστα, αξίζει να σημειωθεί ότι στο πλαίσιο του έργου Broadway [38], για το οποίο θα γίνει εκτενής αναφορά στη συνέχεια, έγινε μια σημαντικότατη δουλειά στην καταγραφή των απαιτήσεων δημόσιας ασφάλειας, τόσο λειτουργικών όσο και τεχνολογικών. Μάλιστα, αποτέλεσε το

πρώτο και καθοριστικό βήμα στην υλοποίηση του συγκεκριμένου έργου, καθώς ήταν από την αρχή ξεκάθαρο ότι οι απαιτήσεις έχουν διαφοροποιηθεί σημαντικά προϊόντος του χρόνου και ότι είναι μια διαδικασία που χρήζει επικαιροποίησης ανά τακτά χρονικά διαστήματα. Από την ολοκλήρωση αυτού του πρώτου υποέργου προέκυψε η λεγόμενη βάση γνώσης, με συγκεκριμένες και σαφείς προτεραιότητες. Το πλέον σημαντικό βέβαια στην όλη διαδικασία είναι ότι τα συμπεράσματα ήταν αποτέλεσμα της αξιολόγησης πολλών και διαφορετικών παραγόντων και παραμέτρων. Μελετήθηκε διεξοδικά η υπάρχουσα βιβλιογραφία, η καταγεγραμμένη έως το σημείο της έρευνας (2017) εμπειρία και ερευνητική δραστηριότητα, αλλά και τα συμπεράσματα του εργαστηρίου που υλοποιήθηκε στο πλαίσιο του έργου, το οποίο έλαβε υπόψη του τα αποτελέσματα ερωτηματολογίου που διαμοιράστηκε στο σύνολο των ανταποκριτών των υπηρεσιών που εμπλέκονται στη δημόσια ασφάλεια, όλων των Χωρών μελών που συμμετείχαν, καθώς και την πληθώρα των σχετικών αναφορών. Η εξαγωγή συμπερασμάτων έγινε με πλουραλισμό κριτηρίων και διαφορετική κάθε φορά στόχευση, με βάση το αρχικό σχέδιο, ώστε να μειωθούν κατά το δυνατό τα περιθώρια εξαγωγής εσφαλμένων ή παραπλανητικών συμπερασμάτων.

Το συγκεκριμένο υποέργο (BroadMap, Πακέτο εργασίας 3 – WP3) [38], ως μέρος του Broadway, θεωρείται state-of-the-art του τρόπου λειτουργίας για όλες τις αντίστοιχες περιπτώσεις, καθώς στηρίχθηκε στις πέντε βασικές αρχές και συγκεκριμένα της ίσης μεταχείρισης, της διαφάνειας, της μη διάκρισης, της αμοιβαίας αναγνώρισης, της αναλογικότητας και στα αποτελέσματά του έχουν υπάρξει αναφορές έκτοτε, σε πλείστες περιπτώσεις. Βέβαια, η καταγραφή των απαιτήσεων είναι πρωταρχικό βήμα που επιχειρήθηκε από το σύνολο της επιστημονικής κοινότητας που ασχολήθηκε με τις επικοινωνίες δημόσιας ασφάλειας, τις κρίσιμες επικοινωνίες και τους πρώτους ανταποκριτές. Αξιοσημείωτα είναι τα συμπεράσματα που παρουσιάζονται σε σχετική έκθεση στο πλαίσιο του έργου SAFECOME[2], μέσα από το οποίο το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ (Department of Homeland Security - DHS), με αφορμή το τρομοκρατικό χτύπημα της 11ης Σεπτεμβρίου 2001 στη Νέα Υόρκη επιχείρησε να επικοινωνήσει σε ένα ευρύ κοινό τη σημασία της διαλειτουργικότητας μεταξύ των πρώτων ανταποκριτών σε όλη τη χώρα και να εξηγήσει γιατί απλά δεν αρκεί να δαπανώνται χρήματα μόνο για το πρόβλημα, χωρίς προγραμματισμό και σχέδιο [39]. Επίσης, αξίζει να σημειωθεί ότι πολλοί επιχείρησαν διαφορετικών ειδών κατηγοριοποιήσεις των απαιτήσεων. Η κατηγοριοποίηση που ενδεχομένως παρουσιάζει ιδιαιτερότητα είναι αυτή που καταγράφηκε από τους [40] στη σχετική τους εργασία, όπου οι απαιτήσεις κατατάχθηκαν ανάλογα με την τεχνολογία που εξυπηρετούν. Έτσι, αναφέρθηκε

[2] https://www.cisa.gov/safecom

ότι υπάρχει ένα ολοκληρωμένο σύνολο διαθέσιμων μελετών απαιτήσεων για PSN παλαιού τύπου.

Μέσα από τη συνδυαστική μελέτη όλων αυτών καταλήξαμε σε ένα βασικό σύνολο προδιαγραφών για την εκπλήρωση των απαιτήσεων, οι οποίες ανά θεματική είναι οι ακόλουθες [41], [42], [43]

2.5.2.1 Στιβαρότητα, αξιοπιστία και βασικές προδιαγραφές

2.5.2.1.1 Προδιαγραφές

- Κλήσεις μεταξύ δύο οντοτήτων που ανταλλάσουν δεδομένα φωνής και στις δύο κατευθύνσεις ταυτόχρονα (full duplex), ή σε μία κατεύθυνση κάθε φορά (half duplex PTT) - Push to Talk (PTT) επικοινωνίες
- Κλήσεις πλήρους ή μισής διπλής όψης που περιλαμβάνουν περισσότερες από δύο οντότητες (ομαδικές κλήσεις)
- Κλήσεις έκτακτης ανάγκης που απαιτούν υψηλή αξιοπιστία και προτεραιότητα
- Ακρόαση περιβάλλοντος, ήτοι εκπομπών φωνητικών καναλιών κοντινών οντοτήτων
- Ανταλλαγή φωνητικών μηνυμάτων και ειδοποιήσεων
- Αναγνώριση μελών που συμμετέχουν στις κλήσεις (αναγνωριστικό καλούντος), τόσο σε έναν προς έναν κλήσεις, όσο και σε ομαδικές
- Προσδιορισμός της θέσης των επαγγελματιών PS σε περιοχές που έλαβε χώρα η καταστροφή ή το γεγονός
- Δυνατότητα πρόσβασης σε βάσης δεδομένων PS από το πεδίο (π.χ. αρχιτεκτονικά σχέδια κτηρίων, βάθος ποταμών, κ.λπ.)
- Ανταλλαγή πληροφοριών θέσης και γεω-εντοπισμός
- Προσδιορισμός ατόμων με βάση τα βιομετρικά τους στοιχεία μέσα από διαδραστική επικοινωνία με τους επαγγελματίες του PS
- Αποστολή και λήψη μηνυμάτων κειμένου μεταξύ δύο οντοτήτων, αλλά και μεταξύ ομάδων
- Συλλογή πληροφοριών από ασύρματα δίκτυα αισθητήρων (WSN) που έχουν αναπτυχθεί ή είναι εγκατεστημένα στις περιοχές του πεδίου (καταστροφής, γεγονότος, κ.λπ.)
- Παρακολούθηση των επαγγελματιών του PS μέσω αισθητήρων που φέρουν, κατά το χρόνο που δρουν στο πεδίο
- Αναγνώριση προσώπων με βάση την εικόνα που δέχεται το κέντρο ελέγχου και συντονισμού
- Βιντεοκλήσεις ένας προς έναν ή ομαδικές
- Εγγραφή, πρόσβαση σε πραγματικό χρόνο ή μετάδοση βίντεο
- Κοινή χρήση, ή διαμοιρασμός εικόνων με άλλους επαγγελματίες του PS

2.5.2.1.2 Στιβαρότητα – αξιοπιστία

- Στιβαρότητα στην κατασκευή, στα δομικά στοιχεία του δικτύου (σταθμοί βάσης, backhaul, core, κ.λπ.) και λειτουργικότητα του δικτύου
- Ρητή ειδοποίηση χρηστών για την υποβαθμισμένη λειτουργία της εφαρμογής

- Εγκατεστημένες κάμερες σε οχήματα ή UAVs με δυνατότητα άμεσης μετάδοσης της εικόνας στο κέντρο ελέγχου
- Ύπαρξη στατικών καμερών σε συγκεκριμένους χώρους που ενδείκνυται, συνήθως αφορά στο εσωτερικό κτηρίων
- Εγκατεστημένος φορητός υπολογιστής με μεγάλη οθόνη και πληκτρολόγιο σε όχημα που επιχειρεί στο πεδίο
- Αξιοποίηση του συνόλου των εφαρμογών που παρέχουν στον χρήστη επίγνωση της κατάστασης
- Αξιοποίηση του συνόλου των συσκευών στο πεδίο (smartphone, pda, tablet, smartwatch, helmet, glasses, κ.λπ.), με οθόνες, ειδοποιήσεις ή ανάλυσης των δεδομένων σε επίπεδα, με ελάχιστη καταπόνηση της μπαταρίας
- Υψηλές ταχύτητες μετάδοσης δεδομένων
- D2D επικοινωνίες
- Ad hoc δίκτυα
- Διαθεσιμότητα καναλιού για να παραχωρηθεί για τις ανάγκες επικοινωνίας των επαγγελματιών του PS, όταν λαμβάνει χώρα περιστατικό, ώστε οι πρώτοι ανταποκριτές και οι ενεργούντες εντός της σκηνής του περιστατικού να χρησιμοποιήσουν αυτό χωρίς προβλήματα
- Το βασικό δίκτυο πυρήνα (Core Network) να βρίσκεται υπό κυβερνητικό έλεγχο και όχι από εταιρίες, ώστε να παρέχεται ένα σημαντικό επίπεδο ασφάλειας των τελικών χρηστών, αλλά επιπλέον και για ζητήματα εθνικής ασφάλειας.
- Δυνατότητα σχεδιασμού ομάδας συζητήσεων για να καλύψουν ανάγκες μεγάλων γεγονότων (πχ συγκεκριμένα κανάλια για χρήση κατά τη διάρκεια συγκεκριμένης επιχειρησιακής λειτουργίας)
- Μη επιτρεπτή αστοχία κατά τη διάρκεια κλιματικών γεγονότων, σεισμών, κραδασμών και συμβάντων μεγάλης έκτασης
- Ελάχιστος αριθμός σφαλμάτων δεδομένων στο πλαίσιο ευρυζωνικής επικοινωνίας
- Εξασφάλιση ενδοϋπηρεσιακής λειτουργικότητας και διυπηρεσιακής διαλειτουργικότητας των επικοινωνιών [39]
- Επαρκή χωρητικότητα ευρυζωνικού δικτύου με σχεδίαση για να καλύπτει φορτία αιχμής ώστε να εξυπηρετεί αυξημένο κυκλοφορικό φορτίο κατά τη διάρκεια μεγάλων και απαιτητικών επιχειρήσεων
- Διασφάλιση απρόσκοπτης λειτουργίας ευρυζωνικού δικτύου και μέγιστης απόδοσης αυτού. Λειτουργία ευρυζωνικού δικτύου 24/7, 365 ημέρες το χρόνο και ποσοστό αξιοπιστίας 99,98%
- Hotspot – WiFi για βελτιωμένη κάλυψη σε απομακρυσμένες περιοχές ή εντός κτηρίων
- Ευρυζωνικό δίκτυο που παρέχει δυνατότητα διαχείρισης συσκευών και εφαρμογών με διαφορετικές απαιτήσεις για QoS, όπου θα πραγματοποιείται δυναμική παραμετροποίηση
- Ιεράρχηση της κυκλοφορίας για την παροχή προτεραιότητας κλήσεων εντός του δικτύου
- Η αρχιτεκτονική ευρυζωνικού δικτύου να είναι στιβαρή, αξιόπιστη και να παρέχει «πλεόνασμα» σε όλα τα επιμέρους λειτουργικά στοιχεία δικτύου. Εφεδρικά τροφοδοτικά, εφεδρικό δίκτυο, κάρτες ραδιοφωνικών σταθμών βάσης, κ.λπ.
- Να είναι εφικτή η λειτουργία του ευρυζωνικού δικτύου σε συνθήκες απώλειας ισχύος, ή μη σταθερής τάσης ηλεκτρικού ρεύματος
- Πλατφόρμες λογισμικού και υλικού που παρέχουν ανοχή σε σφάλματα

- Να υποστηρίζεται τεχνική μείωσης ρυθμού εύρους ζώνης δικτύου που χρησιμοποιείται σε συνθήκες αυξημένης κίνησης ή συμφόρησης
- Το ευρυζωνικό δίκτυο θα πρέπει να μπορεί να είναι λειτουργικό σε σκληρά περιβάλλοντα (φυσικές καταστροφές), αλλά και σε περιπτώσεις που έχουμε διακοπή ηλεκτροδότησης, ή απώλεια κρίσιμων εξαρτημάτων (π.χ. ρελέ, πύργοι, κυψέλες, εξοπλισμός δρομολόγησης ή μεταγωγής πακέτων κ.λπ.)
- Να υφίσταται σχεδιασμός υψηλής διαθεσιμότητας, ποικιλομορφία και πλεονασμός, ώστε να αποφύγουμε περιπτώσεις απώλειας διαθεσιμότητας υπηρεσιών λόγω αστοχίας ενός τμήματος της υποδομής, έχοντας παράλληλα πρόβλεψη για λειτουργικές διαδικασίες δημιουργίας αντιγράφων ασφαλείας
- Ύπαρξη κρυφής μνήμης όπου θα αποθηκεύονται δεδομένα που σε συγκεκριμένη χρονική στιγμή δεν δύναται να μεταδοθούν λόγω προβλήματος, ώστε να μεταδοθούν με την αποκατάσταση.
- Λειτουργική όραση, μέσω ενός οικοσυστήματος προγραμματιστικών εφαρμογών που θα αξιοποιήσει τη δημιουργική ικανότητα του πεδίου και θα εντάξει στις προταθείσες λύσεις την καινοτομία, παρέχοντας ταυτόχρονα χρηστή διακυβέρνηση και επαρκή πιστοποίηση, ώστε να μην διακυβεύονται οι απαιτήσεις ασφάλειας και αποστολής [42].

2.5.2.2 Απόλυτη ασφάλεια

- Ενεργοποίηση συσκευής με προσωπικό αριθμό αναγνώρισης (PIN), φωνητικό έλεγχο ταυτότητας, σάρωση ίριδας ματιού ή δακτυλικά αποτυπώματα
- Οι συσκευές να εμφανίζουν ώρα, ημερομηνία και τοποθεσία
- Εμφάνιση τοποθεσίας και συντεταγμένων σε χάρτη
- Οι χρήστες να λαμβάνουν ρητή ειδοποίηση για την υποβαθμισμένη λειτουργία της εφαρμογής
- Οι εξουσιοδοτημένοι συντηρητές να μπορούν να ενεργούν χωρίς να προκύπτει υποβάθμιση των παρεχόμενων υπηρεσιών
- Καταγραφή χρόνου που λαμβάνουν χώρα οι αστοχίες ή ζημιές και η αποκατάσταση αυτών
- Οι εξουσιοδοτημένοι διαχειριστές θα πρέπει να είναι σε θέση να εκτελούν όλες τις διαχειριστικές λειτουργίες από οποιοδήποτε σημείο του δικτύου.
- Όλοι οι χρήστες του συστήματος θα έχουν ξεχωριστό μοναδικό αναγνωριστικό, αμετάβλητο και ανεξάρτητο από τη συσκευή που χρησιμοποιούν
- Όλες οι συσκευές θα φέρουν αμετάβλητο μοναδικό αναγνωριστικό και θα υφίσταται η δυνατότητα ο διαχειριστής του συστήματος να εκχωρήσει επιπλέον αναγνωριστικό
- Το σύστημα θα πρέπει να παρέχει μεθόδους διόρθωσης σφαλμάτων
- Ιδιωτική κλήση
- Δυνατότητα απομακρυσμένης απενεργοποίησης
- Άρνηση παροχής υπηρεσιών – υποκλοπή
- Πιστοποίηση χρηστών και ειδικές εξουσιοδοτήσεις κλιμακωτής πρόσβασης
- Ανάλυση επισκεψιμότητας και παρατήρηση της συμπεριφοράς των χρηστών
- Εμπλοκή και κλοπή συσκευών τελικού χρήστη
- Μέθοδοι ενθυλάκωσης και κρυπτογράφησης, επαναφοράς κλειδιών, χωρίς να διακόπτεται η υπηρεσία (διαθεσιμότητα και ακεραιότητα)

- Μόνο εξουσιοδοτημένοι χρήστες να έχουν τη δυνατότητα να δημιουργούν ομάδες χρηστών
- Μέτρα ελέγχου για μη εξουσιοδοτημένους χρήστες που επιχειρούν μη εξουσιοδοτημένη πρόσβαση
- Αμοιβαίος έλεγχος ταυτότητας στο σύνολο των συσκευών, υποστήριξη κρυπτογράφησης διεπαφών και μετάδοσης δεδομένων και φωνής
- Χρήση τυποποιημένων, πιστοποιημένων και δοκιμασμένων αλγορίθμων κρυπτογράφησης για τα δεδομένα που διακινούνται
- Αυτοέλεγχος εφαρμογών για αλλοιώσεις ή παρεμβάσεις από μη εξουσιοδοτημένους χρήστες
- Ασφάλεια δεδομένων και διασφάλιση πληροφοριών που διακινούνται μέσω των εφαρμογών, τήρηση πρωτοκόλλων ασφαλείας σε επίπεδο εφαρμογής, διασύνδεση με πρωτόκολλα ασφαλείας που βασίζονται στο δίκτυο και διασφάλιση μεταδόσεων δεδομένων με επαλήθευση

2.5.2.3 Διαλειτουργικότητα

- Ροή δεδομένων και βίντεο σε πραγματικό χρόνο για παροχή βοήθειας και απομακρυσμένης ιατρικής υποστήριξης (π.χ. απομακρυσμένη διάγνωση ασθενών, συμβουλή από ιατρό ή νοσοκομείο), μετάδοση βιομετρικών στοιχείων (σφυγμός, ρυθμός αναπνοής, θερμοκρασία σώματος, εξωτερική θερμοκρασία, κ.λπ.)
- Πρόσβαση σε βάσεις όπως εντοπισμού οχημάτων, γεωγραφικών πληροφοριών, βάσης δεδομένων του οργανισμού
- Σύνδεση με το διαδίκτυο (internet) η σε δίκτυο intranet, περιήγηση σε τηλεφωνικό κατάλογο, πρόσβαση σε ηλεκτρονική αλληλογραφία, βάσεις δεδομένων του οργανισμού, μέσα κοινωνικής δικτύωσης
- Πλήρης λειτουργικότητα ευρυζωνικού δικτύου τόσο σε σταθερούς χρήστες (0 km/h έως πεζοπορία), όσο και σε κινητούς που αγγίζουν ταχύτητες της τάξης των 200km/h.
- Κάλυψη εντός κτηρίων
- Εναλλακτική λειτουργία υποδομής, ταχεία ανάπτυξη κινητών κέντρων (οχήματα/UAV, satellites) σε περιπτώσεις καταστροφής των σταθερών υποδομών
- Υποστήριξη πρόσβασης σε ευρυζωνικό δίκτυο από χρήστες, ανεξαρτήτως της εταιρίας ή του φορέα που ανήκουν
- Κοινή χρήση φωνής και δεδομένων ανεξαρτήτως υπηρεσίας ή φορέα
- Το ευρυζωνικό δίκτυο θα πρέπει να είναι επεκτάσιμο και διαλειτουργικό, ώστε να υποστηρίζει επιτυχώς επικοινωνίες τόσο σε εθνικό επίπεδο, όσο και σε τοπικό (συγκεκριμένες τοποθεσίες)
- Διαλειτουργικότητα με δορυφορικά συστήματα
- Τα δίκτυα θα πρέπει να παρέχουν απρόσκοπτη λειτουργία υπηρεσιών και εφαρμογών κατά τη μεταφορά και μετάβαση από κόμβο σε κόμβο, εντός του ίδιου δικτύου, ή μεταξύ διαφορετικών δικτύων
- Το ευρυζωνικό δίκτυο να υποστηρίζει συνεχώς τις κρίσιμες λειτουργίες δικτύου, ανεξαρτήτως από την ύπαρξη σύνδεσης backhaul.
- Οι σταθμοί βάσης του ευρυζωνικού δικτύου να παρέχουν τη δυνατότητα εναλλακτικής λειτουργίας ώστε να παρέχουν μια ελάχιστη υπηρεσία, όταν έχει καταστραφεί η υποδομή και μέχρι την πλήρη υποστήριξή τους. Οι ελάχιστες απαιτήσεις αφορούν σε ομαδική και μεμονωμένη κλήση.

- Διαθεσιμότητα αποκλειστικού φάσματος συχνοτήτων για ευρυζωνικό δίκτυο, κατάλληλη απόσταση καναλιών μεταξύ τους και βασική συχνότητα εκπομπής και λήψης
- Μηχανισμούς για την ελαχιστοποίηση επίδρασης παρεμβολών από γειτονικά συστήματα ή κανάλια ώστε οι λειτουργίες των υπηρεσιών του συστήματος να είναι αδιάκοπες.

2.5.2.4 Απαιτήσεις υλικού και λογισμικού

- Διάρκεια ζωής της μπαταρίας, η οποία θα πρέπει να ξεπερνά τις 16 ώρες και να υπάρχει ανθεκτικότητα στη βροχή για το σύνολο των συσκευών που χρησιμοποιούνται στο πεδίο
- Εργονομικός σχεδιασμός και φιλικός προς τον χρήστη
- Χειριστήρια που δεν απαιτούν οπτική επαφή
- Έλεγχος έντασης ήχου και λειτουργία δόνησης
- Κουμπί κλήσης έκτακτης ανάγκης
- Η συσκευή να δέχεται ακουστικά και να υπάρχει η δυνατότητα ακουστικών hands free
- Η ενεργοποίηση της συσκευής να γίνεται με προσωπικό αριθμό αναγνώρισης (PIN), φωνητικό έλεγχο ταυτότητας, σάρωση ίριδας ματιού ή δακτυλικά αποτυπώματα
- Οι συσκευές να εμφανίζουν ώρα, ημερομηνία και τοποθεσία
- Να παρέχεται βάση στήριξης στον ώμο και στη ζώνη
- Εντοπισμός στο σκοτάδι με θετική οπτική ανάδραση
- Οθόνη ευανάγνωστη ακόμη και στο σκοτάδι
- Η συσκευή να διαθέτει κάμερα και να έχει δυνατότητα αποστολής και λήψης φωτογραφίας, βίντεο σε λειτουργία χαμηλής ή υψηλής ανάλυσης κατ' επιλογή
- Επαρκής εσωτερική μνήμη συσκευής για αποθήκευση δεδομένων και να παρέχεται εύκολη και γρήγορη διαγραφή των αποθηκευμένων δεδομένων
- Αποστολή και λήψη μηνυμάτων κατάστασης μεταξύ χρηστών
- Επιλογή κλήσης μιας προκαθορισμένης ομάδας με απλό τρόπο (όχι περισσότερα από τρία πλήκτρα)
- Σύντομοι κωδικοί κλήσης και πλήκτρα ενός αγγίγματος
- Αλφαριθμητικό πληκτρολόγιο για ρύθμιση της συσκευής
- Αναγνώριση κλήσης, εμφάνιση καλούντος, δυνατότητα αναμονής κλήσης και να παρέχεται ηχητική ή φωτεινή ένδειξη αναμονής κλήσης στον χρήστη
- Να είναι εφικτό να χειρίζεται ο χρήστης τη συσκευή με γάντια
- Ποιότητα ήχου που να είναι ευκρινής και σε δύσκολα – θορυβώδη περιβάλλοντα, κατανόηση του καλούντος χωρίς να προκύπτει αναγκαιότητα επανάληψης του ομιλητή και χωρίς να δημιουργούνται προβλήματα κατανόησης της φωνής, να είναι εφικτό να ανιχνεύεται το άγχος στη φωνή του χρήστη
- Οι εφαρμογές να παρέχουν τη δυνατότητα μετάφρασης
- Αρχείο επαφών
- Εύκολη εγκατάσταση, εκκίνηση και χρήση εφαρμογών, χωρίς να απαιτείται εκτενής εκπαίδευση των χρηστών για τη χρήση τους. Λειτουργικότητα της εφαρμογής να είναι συνεπής και διαισθητική
- Οι εφαρμογές και οι υπηρεσίες να μπορούν να διευκολύνουν τη διαφήμιση της παρουσίας, τη διαθεσιμότητα και την εν γένει κατάσταση ενός χρήστη

- Ομαδική κλήση (φωνή, βίντεο, εικόνα, δεδομένα)
- Δυνατότητα επικοινωνίας χωρίς χρήση δικτύου (direct mode call)
- Φωνητική κλήση έκτακτης ανάγκης
- Οι χρήστες να λαμβάνουν ρητή ειδοποίηση για την υποβαθμισμένη λειτουργία της εφαρμογής
- Η συσκευή να υποστηρίζει εμφάνιση τυπικών εγγράφων (pdf, word, excel, power point, κ.λπ.)
- Δυνατότητα απομακρυσμένης απενεργοποίησης
- Οι συσκευές να διατηρούν και εμφανίζουν λίστα με τις δέκα τελευταίες κλήσεις

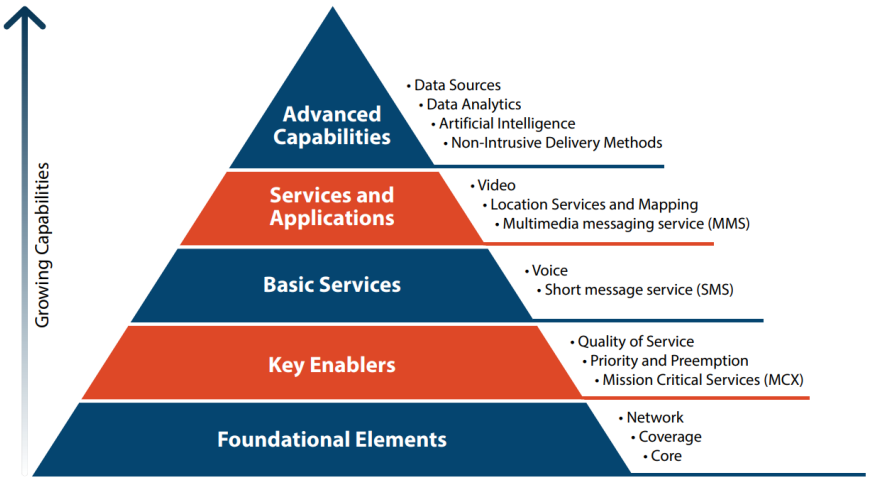
2.5.2.5 Οικονομικές πτυχές

- Διαλειτουργικότητα προμηθευτών για τις συσκευές, οι οποίες θα πρέπει να είναι δεκτικές νέων τεχνολογιών, να παρέχουν δυνατότητα ενσωμάτωσης νέων συστημάτων και υποδομή με επαρκείς διεπαφές
- Οι εφαρμογές να ελέγχονται για πιστοποίηση συμμόρφωσης με τις κατάλληλες πολιτικές συμπεριφοράς και απόδοσης δικτύου
- Ανθεκτικότητα σε σφάλματα και δυνατότητα να διορθώνει τις βλάβες του συστήματος και να επιτρέπει την απομακρυσμένη διάγνωση και διόρθωση σφαλμάτων ή βλαβών
- Να παρέχεται η δυνατότητα στους πρώτους ανταποκριτές να έχουν πρόσβαση στα διαθέσιμα εμπορικά δίκτυα στην περιοχή που επιχειρούν

Φυσικά η κατηγοριοποίηση δεν έχει στεγανά, ούτε και αφορά σε λίστα αποκλειστικών προδιαγραφών και απαιτήσεων, αλλά σε μια κατάσταση με τις βασικότερες εξ αυτών, που αποτελούν τον οδικό χάρτη για έρευνα και τυποποίηση στο πλαίσιο των μελλοντικών εξελίξεων στο πεδίο. Κάθε μία από τις καταγεγραμμένες παρατηρήσεις θα πρέπει να ιδωθεί υπό το πρίσμα ότι τα άτομα που ανταποκρίνονται πρώτοι χρειάζονται απλές, εύχρηστες συσκευές και εφαρμογές με δυνατότητα επικοινωνίας, συνεργασίας και πρόσβασης σε πληροφορίες κατά τη διάρκεια καθημερινών λειτουργιών ρουτίνας και περιστατικών απόκρισης έκτακτης ανάγκης. Μάλιστα, λόγω της κρίσιμης φύσης των επικοινωνιών με τη δημόσια ασφάλεια, πρέπει να ληφθούν υπόψη όλοι οι τρόποι με τους οποίους οι ανταποκριτές μπορούν και θα έχουν διασύνδεση ή εμπειρία με το δίκτυο. Οι τεχνολογίες συσκευών και εφαρμογών που χρησιμοποιούνται πρέπει να είναι αποτελεσματικές, αξιόπιστες και ανθεκτικές και πρέπει να βελτιώνουν αντί να εμποδίζουν τις λειτουργίες δημόσιας ασφάλειας [10].

Βέβαια, θα ήταν λάθος να ισχυρισθούμε ότι όλες οι ανάγκες, οι απαιτήσεις και προδιαγραφές έχουν την ίδια βαρύτητα και αξία. Είναι βέβαιο ότι υπάρχει ιεραρχία των αναγκών, καθώς από το σύνολο των στοιχείων που καταγράφηκαν κάποια έχουν αυξημένη προτεραιότητα έναντι των υπολοίπων. Χαρακτηριστικό παράδειγμα προς απόδειξη αυτού αποτελεί η

«Ιεραρχία των αναγκών» που προέκυψε από ερωτήματα στους πρώτους ανταποκριτές στο πλαίσιο της ανατροφοδότησης που επιχειρείται στο έργο FirstNet των Η.Π.Α. (Εικόνα 14).



Εικόνα 14. Ιεραρχία των αναγκών των πρώτων ανταποκριτών [10]

Είναι εμφανές ότι οι πρώτοι ανταποκριτές δίνουν προτεραιότητα στα θεμελιώδη στοιχεία (δηλαδή, δίκτυο, πυρήνας, κάλυψη), τα οποία θέλουν να λειτουργούν με υψηλή αξιοπιστία, καθώς χωρίς αυτά τίποτε δεν μπορεί να είναι λειτουργικό. Ακολούθως, οι βασικοί ενεργοποιητές υποστηρίζουν βασικές υπηρεσίες φωνής, οι οποίες συνεχίζουν να αποτελούν την εφαρμογή υψηλότερης προτεραιότητας και η εφαρμογή με τον υψηλότερο δείκτη χρήσης. Οι υπηρεσίες τοποθεσίας και χαρτογράφησης αξιολογούνται ως σημαντικές και γενικά διαθέσιμες, αλλά χρειάζονται βελτίωση. Τέλος, οι πιο υποσχόμενες μελλοντικές τεχνολογίες, που ονομάζονται στην ιεραρχία «προηγμένες δυνατότητες» αποτελούν επί του παρόντος χαμηλή προτεραιότητα για την κοινότητα της δημόσιας ασφάλειας, αλλά θα προσφέρουν μεγάλα οφέλη στο μέλλον [10].

2.6 Η ιδιαίτερη κατηγορία των πρώτων ανταποκριτών

Γιατί όμως ρωτάμε τους πρώτους ανταποκριτές; Είναι αυτοί μόνο που γνωρίζουν καλά τα ζητήματα δημόσιας ασφάλειας ή είναι άλλοι οι λόγοι που τους καθιστά ιδιαιτέρως σημαντικούς;

Την απάντηση τη δίνει ο Jason Porter, Senior Vice President, FirstNet Program στην AT&T των Η.Π.Α., αναφέροντας: «*Οι πρώτοι ανταποκριτές είναι η καρδιά της FirstNet και είναι η συμβολή τους που διαμορφώνει τα νέα εργαλεία και τεχνολογίες στο δίκτυό τους, σήμερα και για τις επόμενες δεκαετίες. Αυτές οι καινοτόμες λύσεις (σ.σ. αναφέρεται στο FirstNet) εξοπλίζουν τους πρώτους ανταποκριτές με καλύτερη επίγνωση της κατάστασης -είτε διεξάγουν μια αποστολή έρευνας και διάσωσης σε απομακρυσμένη περιοχή, είτε στους επάνω ορόφους*

ενός φλεγόμενου κτηρίου- συμβάλλοντας στη διασφάλιση μιας απρόσκοπτης, διαλειτουργικής σύνδεσης».

Οι πρώτοι ανταποκριτές που ενεργούν στο πεδίο παρέχουν ανεκτίμητες πληροφορίες για την απόδοση του υφιστάμενου δικτύου, για την καλύτερη διάγνωση ζητημάτων που αφορούν καίρια προβλήματα, όπως σημεία με προβληματική ή καθόλου λήψη και παρεμβολές, ή χρηστικότητα εξοπλισμού και διαθέσιμων μέσων, καθώς και περαιτέρω ανάγκες που δημιουργούνται από τις καταστάσεις που καλούνται να αντιμετωπίσουν. Κάθε σοβαρή προσπάθεια στην υλοποίηση έργων στα δίκτυα δημόσιας ασφάλειας ή τις κρίσιμες επικοινωνίες κατέγραψε τις απόψεις, γνώμες και οπτική των πρώτων ανταποκριτών. Οι εφαρμογές δημόσιας ασφάλειας ποικίλουν, όπως χαρακτηριστικά φαίνεται στην Εικόνα 15, πλην όμως σε κάθε μία απ‘ αυτές, οι ιδιαιτερότητες που καλούνται ν‘ αντιμετωπίσουν οι επαγγελματίες που φτάνουν πρώτοι στο σημείο είναι παρεμφερείς, εάν όχι ίδιες.

Εικόνα 15. Εφαρμογές δημόσιας ασφάλειας [44]

Σε αυτές τις συνθήκες καθίσταται αναγκαίο να διασφαλίζεται η αξιόπιστη επικοινωνία, η επίγνωση της κατάστασης από απομακρυσμένες τοποθεσίες και ο συντονισμός της ομάδας. Οι αποτυχίες πληρώνονται σε ανθρώπινες ζωές ακόμη και μεταξύ των πρώτων ανταποκριτών. Ο καθένας, ακόμη και μη σχετικός με τα καθήκοντα των υπηρεσιών και φορέων, θα μπορούσε να φανταστεί έναν μεγάλο αριθμό εφαρμογών και υποστηρικτικών λειτουργιών των πρώτων ανταποκριτών από ένα δίκτυο επικοινωνίας που θα ήταν σε θέση να παρέχει επίγνωση της κατάστασης πριν ή κατά τη διάρκεια προσέγγισης στο σημείο. Προφανώς, υποστήριξη με τέτοιες εφαρμογές θα ήταν ιδιαιτέρως χρήσιμο να είναι εφικτές ακόμη και σε περιοχές χωρίς υποδομή επικοινωνίας, ή σε περιπτώσεις καταστροφής της υφιστάμενης επικοινωνιακής υποδομής και άμεσης θεραπείας με εναλλακτικές μεθόδους (Οχήματα, Μη επανδρωμένα αεροσκάφη, Δορυφόροι, κ.λπ.) [45].

Ποιοι είναι οι επαγγελματίες που ενεργούν ως πρώτοι ανταποκριτές; Είναι οι άνθρωποι που στελεχώνουν οργανισμούς, φορείς και υπηρεσίες που υποστηρίζουν τη δημόσια ασφάλεια.

Είναι οι άνθρωποι που έχουν υποστεί την εκπαίδευση και έχουν αποκτήσει κουλτούρα συνεργασίας και ομαδικής δουλείας. Πιο συγκεκριμένα είναι τα στελέχη που ανήκουν [41]:

- Αστυνομία
- Πυροσβεστική
- Φύλαξη συνόρων
- Λιμενικό / Ακτοφυλακή
- Φύλαξη δασών
- Επαγγελματίες υγείας (Νοσοκομεία, ΕΚΑΒ, ασθενοφόρα, κ.λπ.)
- Στρατό
- Επαγγελματίες αστυνόμευσης κρίσιμων υποδομών (οδικό δίκτυο, σιδηρόδρομοι, αεροδρόμια, κ.λπ.)

Η κυβερνητική λειτουργία κάθε χώρας μπορεί να διαφέρει σημαντικά. Στη χώρα μας, τα ως άνω αναφερόμενα καθήκοντα έχουν ανατεθεί ως ακολούθως:

- Στην Ελληνική Αστυνομία (ΕΛ.ΑΣ.), τα καθήκοντα της Αστυνομίας, της φύλαξης των συνόρων ως προς το διασυνοριακό έγκλημα και τη λαθρομετανάστευση και της αστυνόμευσης κρίσιμων υποδομών και εν μέρη της φύλαξης των δασών. Έχει σήμερα περίπου 55.000 στελέχη.
- Στο Πυροσβεστικό Σώμα (Π.Σ), τα καθήκοντα της Πυροσβεστικής και εν μέρη της φύλαξης των δασών. Έχει σήμερα περίπου 18.200 (9.800 μόνιμοι και λοιποί εθελοντές, εποχικοί κ.λπ.) στελέχη.
- Στο Λιμενικό Σώμα (ΛΣ) Ελλάδος τα καθήκοντα του Λιμενικού και της Ακτοφυλακής. Έχει σήμερα περίπου 7.400 στελέχη.
- Στο Εθνικό Κέντρο Άμεσης Βοήθειας (ΕΚΑΒ) του Ελληνικού Συστήματος Υγείας (ΕΣΥ) τα καθήκοντα των επαγγελματιών υγείας που σχετίζονται με τη δημόσια ασφάλεια.
- Στον Ελληνικό Στρατό (ΕΣ), τα καθήκοντα της αποστολής του. Έχει σήμερα περίπου 12.000 μόνιμα στελέχη, ενώ στους στρατευθέντες φτάνει στις 98.000.

Πέραν των δημόσιων αυτών οργανισμών όμως υπάρχουν και εθελοντικές ομάδες, ή μη κυβερνητικές οργανώσεις, τα μέλη των οποίων προστρέχουν σε περιπτώσεις κρίσιμων περιστατικών ή μεγάλων καταστροφών. Εξ αυτών αξίζει ν` αναφερθούμε στις ακόλουθες περιπτώσεις:

- Ελληνική Ομάδα Διάσωσης (ΕΟΔ)[3], είναι μη κυβερνητική οργάνωση έρευνας και διάσωσης, που ιδρύθηκε το 1978. Διαθέτει περισσότερους από 3.000 εθελοντές σε όλη την Ελλάδα, συμμετέχει σε επιχειρήσεις Έρευνας και Διάσωσης σε περιπτώσεις

[3] https://www.helping.gr/2F08DE41.el.aspx

έκτακτης ανάγκης και μαζικών καταστροφών, οπουδήποτε λαμβάνουν χώρα στην Ελλάδα και στο εξωτερικό. Στελεχώνεται από επαγγελματίες και ερασιτέχνες διασώστες με άριστη επιστημονική και τεχνική κατάρτιση που ενεργούν με εθελοντική συνείδηση.

- Ελληνικός Ερυθρός Σταυρός[4], που ανάμεσα στα άλλα διαθέτει τομέα Εθελοντών Σαμαρειτών, Διασωστών και Ναυαγοσωστών.
- Ελληνικό Ινστιτούτο Διαχείρισης Κρίσεων και Καταστροφών[5] είναι ένας ιδιωτικός οργανισμός που ιδρύθηκε το 2018 και αποτελεί μια πρωτοβουλία μιας ομάδας επαγγελματιών εμπειρογνωμόνων και επιστημόνων υγείας, πολιτικής προστασίας, άμυνας και ασφάλειας, εκπαίδευσης και εθελοντισμού, απ' όλη την Ελλάδα, με αντικείμενο δραστηριότητας τα πεδία της προνοσοκομειακής φροντίδας υγείας, της διαχείρισης κρίσεων, της πολιτικής προστασίας και της αντιμετώπισης καταστροφών, μέσα από προγράμματα σπουδών, συνέργειες, δράσεων και επιχειρήσεων πεδίου, εθνικής και διεθνούς εμβέλειας.

Γιατί όμως δεν στηριζόμαστε στα εμπορικά δίκτυα επικοινωνιών, τα οποία λειτουργούν ήδη πολλά χρόνια και ως εκ τούτου είναι πλήρως δοκιμασμένα, συνεχώς εξελίσσονται και παρέχουν μια βεβαιότητα συνέχεια και ικανοποιητικής λειτουργίας; Μα επειδή τα εμπορικά δίκτυα είναι προσανατολισμένα να καλύπτουν τις ανάγκες των χρηστών «πελατών» τους και δεν μπορούν να καλύψουν βασικές ανάγκες των πρώτων ανταποκριτών. Ειδικότερα, τα εμπορικά δίκτυα [46]:

- Έχουν ως βασικό κριτήριο στην παρεχόμενη κάλυψη την πληθυσμιακή συγκέντρωση των «πελατών» τους. Συνεπώς, τίθενται σε προτεραιότητα οι μεγάλες πόλεις που συγκεντρώνεται το μεγαλύτερο ποσοστό των συνδρομητών, ενώ αποτελεί δευτερευούσης σημασίας ζήτημα η κάλυψη απομακρυσμένων περιοχών.
- Δεν παρέχουν υπηρεσίες ιεράρχησης των κλήσεων σύμφωνα με τις ανάγκες
- Δεν προσφέρουν τις αναγκαίες για τη δημόσια ασφάλεια φωνητικές υπηρεσίες (ομαδικές κλήσεις, επείγουσες κλήσεις, Direct Mode Operation - DMO) μεταξύ δύο τερματικών χρηστών, χωρίς την παρεμβολή της υποδομής επικοινωνίας.
- Υποπίπτουν σε καταστάσεις συμφόρησης κατά τη διάρκεια εξαιρετικών συνθηκών (πολυπληθείς εκδηλώσεις και γεγονότα) και δεν μπορούν να εγγυηθούν την απαιτούμενη διαθεσιμότητα, στοιχείο μη διαπραγματεύσιμο στις κρίσιμες επικοινωνίες.
- Δεν παρέχουν τα επιθυμητά επίπεδα ασφάλειας

[4] http://www.redcross.gr/default.asp?pid=1&la=1

[5] https://www.hellenicinstitute.gr

2.7 Πρώτοι ανταποκριτές στην Ελλάδα – Διεξαγωγή έρευνας

Αντιλαμβανόμενοι την αξία της εμπειρίας των πρώτων ανταποκριτών, σχεδιάστηκε να υλοποιηθεί έρευνα με σαφή σκοπό να διερευνηθούν οι αντιλήψεις αυτών αναφορικά με τη χρήση τηλεπικοινωνιακού εξοπλισμού στο πεδίο, οι εκτιμήσεις τους για το υφιστάμενο τηλεπικοινωνιακό δίκτυο και να καταγραφούν οι ανάγκες τους για καινοτόμες λύσεις εξοπλισμού, με απώτερο στόχο την συγκριτική αποτύπωση των στοιχείων και την ανάδειξη των απαιτήσεων τους, αλλά και των προκλήσεων που καλούνται να αντιμετωπίσουν.

Για τη διεξαγωγή της έρευνας επιλέχθηκε η κατάρτιση ερωτηματολογίου με το εργαλείο Google Forms ώστε αφενός να δοθεί η δυνατότητα οι συμμετέχοντες να αποτυπώσουν ελεύθερα και με ασφάλεια την άποψή τους, αφετέρου τούτο να διαμοιραστεί σε όσο το δυνατό μεγαλύτερο αριθμό επαγγελματιών της δημόσιας ασφάλειας. Ομάδα στόχος αποτέλεσε το σύνολο του προσωπικού των Υπηρεσιών που εμπλέκονται στη δημόσια ασφάλεια στη χώρα μας και συγκεκριμένα της Αστυνομίας, της Πυροσβεστικής, του Λιμενικού και του ΕΚΑΒ. Υπήρχε η πρόθεση και σκέψη, μετά την εξασφάλιση σχετικής έγκρισης, το ερωτηματολόγιο να διαμοιραστεί σε πολίτες που εθελοντικά συμμετέχουν σε δράσεις δημόσιας ασφάλεια, όπως Ομάδες Διασωστών, Ερυθρός Σταυρός, Μ.Κ.Ο. που παρέχουν εθελοντικό έργο συμπληρωματικά και υποστηρικτικά των αναφερόμενων υπηρεσιών. Επιπλέον, η ομάδα στόχος ήταν το σύνολο του προσωπικού των Υπηρεσιών που προαναφέρθηκαν, καθώς με δεδομένο το καθεστώς εκτέλεσης υπηρεσίας, η πλειοψηφία εξ αυτών ασκούν γενικά καθήκοντα, που συνεπάγεται ότι εναλλάσσονται σε θέσης πρώτου ανταποκριτή, στελέχωσης κέντρων ελέγχου και λήψης αποφάσεων, ή διοικητικής λειτουργίας, το οποίο παρέχει μια επιπλέον αξία στην έρευνα.

Το ερωτηματολόγιο υποβλήθηκε στην αρμόδια Επιτροπή Ηθικής και Δεοντολογίας της Έρευνας του Διεθνούς Ελληνικού Πανεπιστημίου, από όπου έλαβε σχετική έγκριση (Συνεδριάση υπ` αρίθμ: 18/22-12-2022). Ακολούθως, υποβλήθηκε με πλήρη φάκελο δικαιολογητικών στα Αρχηγεία της Ελληνικής Αστυνομίας, Πυροσβεστικού Σώματος, Λιμενικού Σώματος και ΕΚΑΒ, με αίτημα να λάβει έγκριση και να διαμοιραστεί στα στελέχη τους. Παρά το γεγονός ότι η υποβολή του αναφερόμενου αιτήματος έγινε την 1-1-2023, ελήφθη θετική απάντηση από το Πυροσβεστικό Σώμα την 15-2-2023, αρνητική απάντηση από την Ελληνική Αστυνομία την 17-2-2023 και μέχρι τη στιγμή ολοκλήρωσης της συγγραφής καμία απάντηση από τους λοιπούς αποδέκτες.

2.7.1 Ερωτηματολόγιο

Παρά το γεγονός ότι δεν υπάρχουν δεδομένα, καθώς αφενός δεν υπήρξε χρόνος να συγκετρωθεί ικανοποιητικός αριθμός απαντήσεων που θα μπορούσε να δώσει ένα

αξιοποιήσιμο αποτέλεσμα, αφετέρου με δεδομένη την αρνητική απάντηση από την Ελληνική Αστυνομία, τα στοιχεία δεν θ` αποτύπωναν όλο το εύρος της ομάδας στόχου, παρουσιάζεται συνοπτικά η μέθοδος κατάρτισης του ερωτηματολογίου και οι σκοποί της έρευνας.

Το ερωτηματολόγιο χωρίστηκε περιλαμβάνει τέσσερις (4) ενότητες:

- Πρώτη Ενότητα. Περιλαμβάνει εννιά (9) συνολικά ερωτήσεις για δημογραφικά στοιχεία που βοηθούν στην ομαδοποίηση των αποτελεσμάτων της έρευνας, ώστε να εξαχθούν εύστοχα και χρήσιμα συμπεράσματα.
- Δεύτερη Ενότητα. Περιλαμβάνει οκτώ (8) ερωτήσεις για στοιχεία που αφορούν στην έρευνα και σχετίζονται με τη συνήθη, καθημερινή εκτέλεση υπηρεσίας. Εξειδικεύεται σε:
  - Α. Επίπεδο χρήσης της τεχνολογίας. Τεχνολογικό υλικό που είναι διαθέσιμο και χρησιμοποιείται στην υπηρεσιακή καθημερινότητα
  - Β. Προβλήματα κατά τη χρήση της τεχνολογίας. Προβλήματα στη χρήση της τεχνολογίας και των συσκευών επικοινωνίας στην υπηρεσιακή καθημερινότητα
- Τρίτη ενότητα. Περιλαμβάνει συνολικά έξι (6) ερωτήσεις που αφορούν σε μεγάλες καταστροφές και σε μεγάλα προγραμματισμένα γεγονότα αναφορικά με τη χρήση της τεχνολογίας για τη διαχείριση αυτών.
- Τέταρτη ενότητα. Περιλαμβάνει εννιά (9) συνολικά ερωτήσεις που αφορούν και σκιαγραφούν το επίπεδο γνώσης και αντίληψης εξειδικευμένων τεχνολογικών ζητημάτων επικοινωνίας, αλλά και έργων που βρίσκονται σε ερευνητικό στάδιο, ή υλοποιούνται ήδη σε παγκόσμιο επίπεδο.

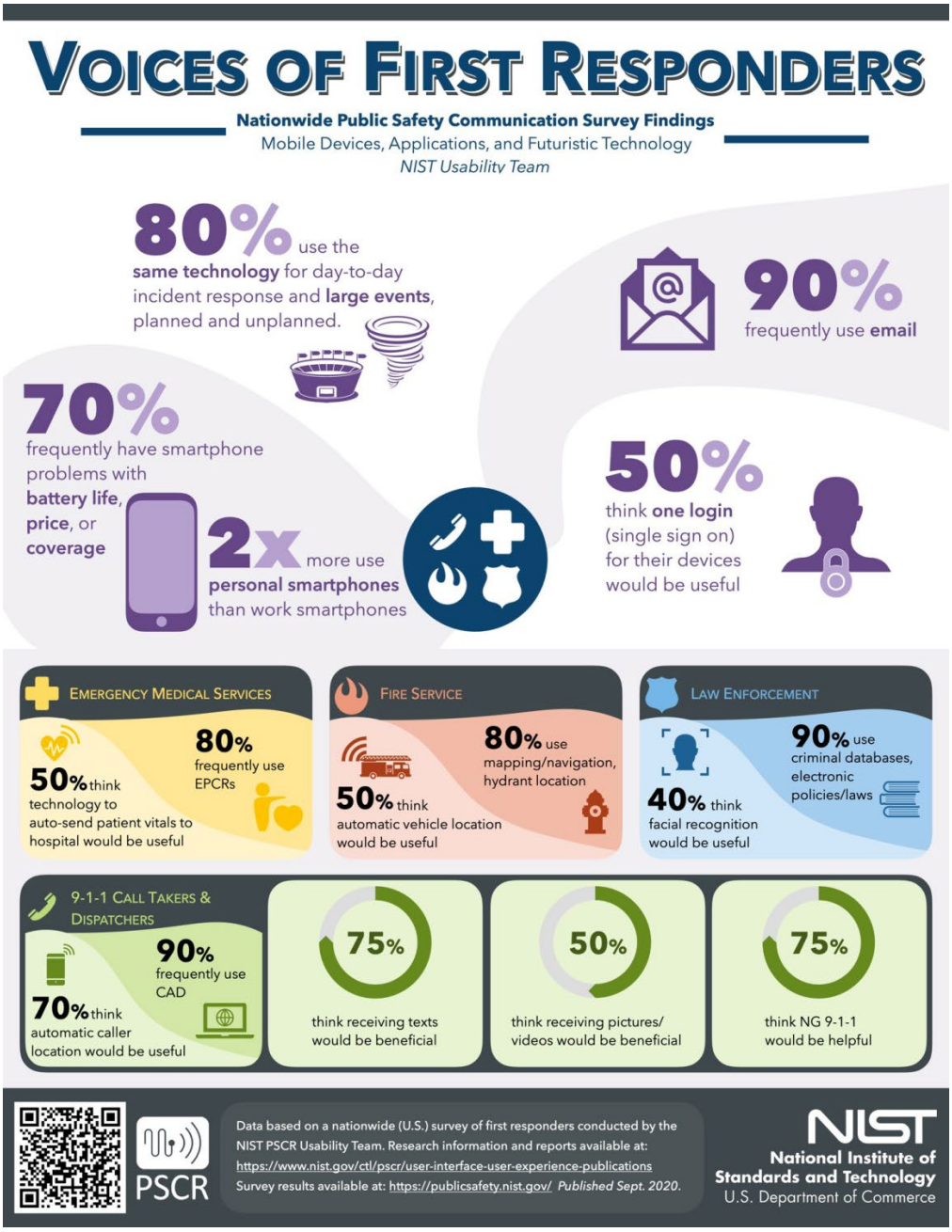
Οι ερωτήσεις και ο τρόπος συλλογής των απαντήσεων προκύπτει αναλυτικά από το ερωτηματολόγιο, μια πλήρη ανάπτυξη του οποίου έχει αποτυπωθεί στο Παράρτημα.

2.7.2 Παρόμοιες έρευνες

Παρόμοιες έρευνες σε Ευρωπαϊκό επίπεδο έχουν πραγματοποιηθεί στο πλαίσιο υλοποίησης έργων. Χαρακτηριστικά παραδείγματα που αναλύσαμε ήδη στο πλαίσιο της ανάλυσης των απαιτήσεων αποτελούν τα έργα BroadWay και Respond-A.

Πέρα από τα ευρωπαϊκά σύνορα, οι Η.Π.Α. έχουν αναθέσει την αντίστοιχη έρευνα στο Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST). Συγκεκριμένα, η Ομάδα Ευχρηστίας για την Έρευνα Επικοινωνιών Δημόσιας Ασφάλειας (Public Safety Communications Research - PSCR) του NIST διεξήγαγε ένα ερευνητικό έργο μεικτών μεθόδων πολλαπλών φάσεων, προκειμένου να παρέχει καλύτερη κατανόηση των χρηστών δημόσιας ασφάλειας, τις εμπειρίες τους και τις

τεχνολογικές τους ανάγκες και προβλήματα [47]. Η έρευνα, τα αποτελέσματα της οποίας παρουσιάζονται στην αναφερόμενη έκθεση, περιλαμβάνει ερωτηματολόγιο που συμπλήρωσαν 7.182 πρώτοι ανταποκριτές, καθώς επίσης και στοχευμένες συνεντεύξεις 193 πρώτων ανταποκριτών. Κάποια από τα πιο σημαντικά αποτελέσματα αυτής φαίνονται συνοπτικά στην Εικόνα 16. Αξιοσημείωτο είναι ότι από τις απαντήσεις που συλλέχθηκαν το 21,78% ανήκει στους υπηρετούντες σε κέντρα «911», το 12,56% σε μονάδες άμεσης υγειονομικής επέμβασης (ΕΚΑΒ), το 34,44% σε Πυροσβέστες και το 29,23% σε Αρχές επιβολής του νόμου (Αστυνομία).



Εικόνα 16. Αποτελέσματα έρευνας που διεξήχθη το 2020 στους πρώτους ανταποκριτές των Η.Π.Α. από το NIST [47]

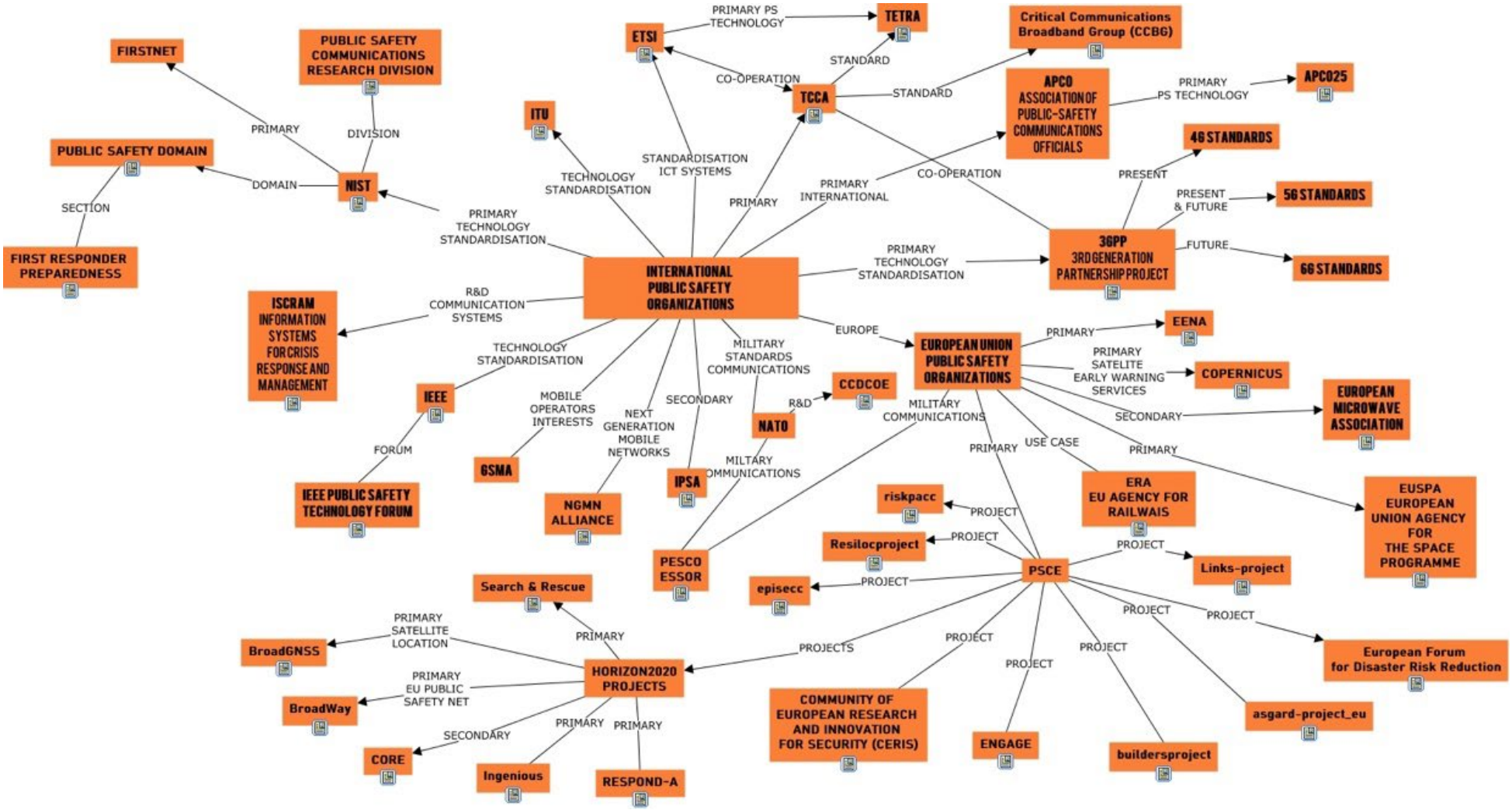
3 *Οργανισμοί και Ενώσεις*

Έχουμε ήδη αναφερθεί στις υπηρεσίες και οργανισμούς που σε κάθε χώρα έχουν επωμιστεί θεσμικά τα καθήκοντα της δημόσιας ασφάλειας και την ανακούφιση από καταστροφές. Λόγω της διαφορετικής δομής, λειτουργίας και διοικητικού μοντέλου, υπάρχουν διαφορές και στην οργάνωση των υπηρεσιών αυτών. Ωστόσο, στο σύνολό τους καλύπτουν το ουσιαστικό αντικείμενο της δημόσιας ασφάλειας σε επιχειρησιακό επίπεδο και είναι αυτοί στους οποίους βασίζονται οι πολίτες να προστρέξουν όποτε απαιτηθεί.

Στον τομέα των κρίσιμων επικοινωνιών που αφορούν στα δίκτυα δημόσιας ασφάλειας και υποστηρίζουν τους οργανισμούς αυτούς έχουν αναπτυχθεί, ανά τον κόσμο, εκατοντάδες οργανισμοί, υπηρεσίες, φορείς, ενώσεις και έχει αναληφθεί κάθε είδους πρωτοβουλία για να υποστηρίξει και βελτιώσει τεχνολογικά την προσπάθεια αυτή. Θα ήταν άτοπο και αχρείαστο να επιχειρηθεί η εξαντλητική παράθεση όλων αυτών. Από την άλλη, κρίνεται επιβεβλημένη η αναφορά στους κύριους διεθνείς οργανισμούς και ενώσεις που είτε άμεσα, είτε έμμεσα διαδραματίζουν πρωταγωνιστικό ρόλο στο χώρο των επικοινωνιών δημόσιας ασφάλειας και σε κάποιες περιπτώσεις καθορίζουν τις εξελίξεις. Οι οργανισμοί αυτοί δεν έχουν στεγανά λειτουργικότητας, αλλά συνεργάζονται στενά μεταξύ τους, με τους οργανισμούς του πεδίου (Αστυνομία, Πυροσβεστική, Λιμενικό, ΕΚΑΒ, Στρατό, κ.λπ.), με εταιρίες, αλλά και με την επιστημονική κοινότητα (Πανεπιστήμια, Ιδρύματα, κ.λπ.). Ο στόχος είναι κοινός και θα επιτευχθεί γρηγορότερα και καλύτερα μέσα από συνεργασίες.

Επειδή ο καλύτερος τρόπος αντίληψης των οντοτήτων και των αλληλεξαρτήσεών τους είναι ο εποπτικός, δημιουργήσαμε έναν εννοιολογικό χάρτη των οργανισμών και φορέων στους οποίους θα αναφερθούμε στη συνέχεια. Ο χάρτης (Εικόνα 17) δημιουργήθηκε με το σχεδιαστικό εργαλείο CmapTools[6] και εδώ θα βρείτε την ενεργή έκδοσή του.

[6] https://cmap.ihmc.us



Εικόνα 17. Συνοπτικός διαδραστικός χάρτης των οργανισμών που απασχολούνται με τη δημόσια ασφάλεια

3.1 Διεθνείς Οργανισμοί

3.1.1 Διεθνής Ένωση Δημόσιας Ασφάλειας

Η Διεθνής Ένωση Δημόσιας Ασφάλειας (International Public Safety Assosiation - IPSA) ιδρύθηκε τον Ιούλιο του 2014 ως μη κερδοσκοπικός οργανισμός. Το όραμά της είναι η ισχυρότερη, πλήρης κοινότητα δημόσιας ασφάλειας, ικανή να ανταποκρίνεται αποτελεσματικά σε όλα τα περιστατικά. Εκπροσωπεί όλους τους κλάδους δημόσιας ασφάλειας και διαχείριση έκτακτης ανάγκης. Με μήνυμα κινητοποίησης το «*Μαζί είμαστε δυνατότεροι*» φιλοδοξεί να δραστηριοποιήσει τους οργανσιμούς, υπηρεσίες, φορείς και πολίτες να εμπλακούν και να γίνουν μέλη. Διεξάγει διεθνή συνέδρια και θεματικά διαδικτυακά σεμινάρια (webinars) ιδιαίτερης αξίας και σπουδαιότητας για τον κλάδο και τα στελέχη της συμμετέχουν σε αντίστοιχες εκδηλώσεις. Η επόμενη προγραμματισμένη τέτοια εκδήλωση είναι το διεθνές συνέδριο την 1/2 Μαίου 2023 στη Μέσα της Αριζόνας (ΗΠΑ). Ο διαδικτυακός της τόπος είναι προσβάσιμος από το σύνδεσμο International Public Safety Association - Home (joinipsa.org).

3.1.2 Ένωση Υπαλλήλων Επικοινωνιών Δημόσιας Ασφάλειας

Η Ένωση Υπαλλήλων Επικοινωνιών Δημόσιας Ασφάλειας (Association of Public-Safety Communications Officials – APCO) ιδρύθηκε το 1935 και είναι οργανισμός επαγγελματιών επικοινωνίας δημόσιας ασφάλειας. Εξυπηρετεί τις ανάγκες των επικοινωνιών δημόσιας ασφάλειας σε όλο τον κόσμο και την ευημερία του ευρύτερου κοινού στο σύνολό του, παρέχοντας τεχνογνωσία, επαγγελματική ανάπτυξη, τεχνική βοήθεια, υπεράσπιση και προβολή. Αριθμεί πλέον των 35.000 μελών, στα οποία εντάσσονται όσοι διαχειρίζονται, χειρίζονται, κατασκευάζουν και υποστηρίζουν συστήματα επικοινωνίας για υπηρεσίες δημόσιας ασφάλειας. Διεξάγει διεθνή συνέδρια και θεματικά διαδικτυακά σεμινάρια (webinars) και τα στελέχη της συμμετέχουν σε αντίστοιχες εκδηλώσεις. Ο διαδικτυακός της τόπος είναι προσβάσιμος από το σύνδεσμο APCO International - Leaders in Public Safety Communications (apcointl.org).

3.1.3 Πρωτοβουλία του Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών

Το Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers – IEEE) είναι ένας επαγγελματικός οργανισμός που ιδρύθηκε το 1963 και αποτελεί το μεγαλύτερο οργανισμό επαγγελματιών τεχνολογίας με περισσότερα απο 400.000 μέλη σε διάφορα τμήματα ανά τον κόσμο. Βασικοί σκοποί του Ινστιτούτου αποτελούν η εκπαιδευτική προώθηση και η τεχνική εξέλιξη της ηλεκτρονικής και

ηλεκτρολογικής μηχανικής, των τηλεπικοινωνιών, της επιστήμης των υπολογιστών και των ενοποιημένων προτύπων. Στο πλαίσιο του IEEE λειτουργούν διάφορες πρωτοβουλίες, ομάδες και επιτροπές. Η αντίστοιχη που έχει αναλάβει την ανάδειξη μελλοντικών κατευθύνσεων, η IEEE Future Directions, η οποία το 2020 δημιούργησε μια ομάδα εργασίας για να μελετήσει και να εντοπίσει τα κενά και τις ευκαιρίες της τεχνολογίας δημόσιας ασφάλειας. Αυτή η πρωτοβουλία ονομάστηκε IEEE Public Safety Technology Initiative (PSTI) και είναι αφιερωμένη στο να γίνει το παγκόσμιο κέντρο αριστείας για φορείς δημόσιας ασφάλειας, προμηθευτές, επαγγελματίες, ερευνητές και όλους τους συμμετέχοντες στον κλάδο ώστε να πραγματοποιηθεί ανταλλαγή ιδεών για το πώς οι αναδυόμενες τεχνολογίες μπορούν να βοηθήσουν το προσωπικό δημόσιας ασφάλειας να είναι πιο αποτελεσματικό στην εργασία του. Η πρωτοβουλία προσδιορίζει τις υπάρχουσες τεχνολογίες του χώρου, ερευνά νέες ευκαιρίες, εγκαινιάζει νέες δραστηριότητες και συνεργάζεται με φορείς δημόσιας ασφάλειας για τη βελτίωση όλων των ενδιαφερομένων του κλάδου. Στο πλαίσιο αυτής της εργασίας παρακολουθήσαμε δια ζώσης τις εργασίες του Συνεδρίου Προτύπων για Επικοινωνίες και Δικτύωση (IEEE Conference on Standards for Communications and Networking – CSCN) που διεξήχθη το Νοέμβριο στη Θεσσαλονίκη. Ο διαδικτυακός του τόπος είναι προσβάσιμος από το σύνδεσμο Home - IEEE Public Safety Technology Initiative.

3.1.4 Έργο Συνεργασίας Τρίτης Γενιάς

Το Έργο Συνεργασίας Τρίτης Γενιάς (3rd Generation Partnership Project - 3GPP) ενώνει επτά οργανισμούς ανάπτυξης τηλεπικοινωνιακών προτύπων και συγκεκριμένα:

1. Ιαπωνική Ένωση Ραδιοβιομηχανιών και Επιχειρήσεων (Association of Radio Industries and Businesses - ARIB),
2. Συμμαχία Λύσεων για τον Κλάδο των Τηλεπικοινωνιών (Alliance for Telecommunications Industry Solutions - ATIS,
3. Ένωση Προτύπων Επικοινωνιών της Κίνας (China Communications Standards Association - CCSA,
4. Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (European Telecommunications Standards Institute – ETSI)
5. Ένωση Τηλεπικοινωνιών Βιομηχανίας Η.Π.Α. (Telecommunications Industry Association - TIA),
6. Ένωση Τεχνολογίας Τηλεπικοινωνιών Ν. Κορέας (Telecommunications Technology Association - TTA) και
7. Επιτροπή Τεχνολογίας Τηλεπικοινωνιών της Ιαπωνίας (Telecommunication Technology Committee - TTC),

γνωστούς ως «Οργανωτικούς Συνεργάτες» και παρέχει στα μέλη του ένα σταθερό περιβάλλον για την παραγωγή των αναφορών και των προδιαγραφών. Το 3GPP ιδρύθηκε επίσημα το 1998 με αρχικό στόχο την ανάπτυξη προδιαγραφών παγκόσμιας εφαρμογής για κινητά συστήματα τρίτης γενιάς (3G). Το έργο βασίστηκε αρχικά στις προδιαγραφές του Παγκόσμιου Συστήματος Κινητών Επικοινωνιών (GSM) και στην προσπάθεια της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU). Το 3GPP εκτός από την ανάπτυξη του προτύπου 3G, έχει αναπτύξει τα παγκόσμια πρότυπα τέταρτης γενιάς (4G) και πέμπτης γενιάς (5G). Ο διαδικτυακός του τόπος είναι προσβάσιμος από το σύνδεσμο 3GPP – The Mobile Broadband Standard Partnership Project.

3.1.5 Αμερικανικό Εθνικό Ινστιτούτο Προτύπων

Το Αμερικανικό Εθνικό Ινστιτούτο Προτύπων (American National Standards Institute – ANSI) είναι ένας ιδιωτικός, μη κερδοσκοπικός οργανισμός που διαχειρίζεται και συντονίζει τα εθελοντικά πρότυπα και το σύστημα αξιολόγησης της συμμόρφωσης των Η.Π.Α., χωρίς ωστόσο να αποτελεί οργανισμό ανάπτυξης προτύπων. Ιδρύθηκε το 1918 και βρίσκεται σε στενή συνεργασία με ενδιαφερόμενα μέρη από τη βιομηχανία και την κυβέρνηση για τον εντοπισμό και την ανάπτυξη λύσεων που βασίζονται σε πρότυπα και συμμόρφωση σε εθνικές και παγκόσμιες προτεραιότητες. Συγκεντρώνει εμπειρογνώμονες και ενδιαφερόμενους του ιδιωτικού και του δημόσιου τομέα με στόχο συνεργατικές δραστηριότητες τυποποίησης που ανταποκρίνονται στις εθνικές προτεραιότητες. Ταυτόχρονα λειτουργεί ως εθελοντική κοινότητα προτύπων των ΗΠΑ. Εκπροσωπεί τα συμφέροντα περισσότερων από 270.000 εταιρειών και οργανισμών και 30 εκατομμυρίων επαγγελματιών παγκοσμίως. Ο διαδικτυακός του τόπος είναι προσβάσιμος από το σύνδεσμο https://www.ansi.org/.

3.1.6 Διεθνής Ένωση Τηλεπικοινωνιών

Η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union – ITU) είναι η εξειδικευμένη υπηρεσία των Ηνωμένων Εθνών για τις τεχνολογίες πληροφοριών και επικοινωνιών ΤΠΕ. Ιδρύθηκε το 1865 και εργάζεται για τη διευκόλυνση της διεθνούς συνδεσιμότητας σε δίκτυα επικοινωνιών, εκχωρεί παγκόσμιο ραδιοφάσμα και δορυφορικές τροχιές, αναπτύσσει τα τεχνικά πρότυπα που διασφαλίζουν την απρόσκοπτη διασύνδεση δικτύων και τεχνολογιών και βελτιώνει την πρόσβαση σε ΤΠΕ των υποεξυπηρετούμενων κοινοτήτων σε όλο τον κόσμο. Στις δεσμεύσεις της εντάσσεται η παγκόσμια συνδεσιμότητα, ανεξάρτητα από τις δυνατότητες των χωρών, προστατεύοντας έτσι το βασικό δικαίωμα του ανθρώπου για επικοινωνία. Στο πλαίσιο αυτής της εργασίας παρακολουθήσαμε απομακρυσμένα πολλά από τα webinars που διοργάνωσε ο ITU. Ο διαδικτυακός της τόπος είναι προσβάσιμος από το σύνδεσμο ITU: Committed to connecting the world.

3.1.7 Η Ένωση Κρίσιμων Επικοινωνιών

Η Ένωση Κρίσιμων Επικοινωνιών (The Critical Communication Association – TCCA) αποτελεί ένα φόρουμ για τις κυβερνήσεις, τις ρυθμιστικές αρχές, τους κατασκευαστές, τους φορείς εκμετάλλευσης, τους τελικούς χρήστες, κάθε ενδιαφερόμενο στον τομέα των κρίσιμων επικοινωνιών. Συνεργάζεται και αλληλεπιδρά με άλλες ενώσεις, φορείς και υπηρεσίες για την αποτελεσματική λειτουργία των κρίσιμων επικοινωνιών. Τα μέλη της TCCA σχεδιάζουν, υλοποιούν, χρησιμοποιούν, αναλύουν, προωθούν και αναπτύσσουν κρίσιμες επικοινωνίες σε όλο τον κόσμο. Διεξάγει διεθνή συνέδρια και webinars ιδιαίτερης αξίας και σπουδαιότητας για τον κλάδο και τα στελέχη της συμμετέχουν σε αντίστοιχες εκδηλώσεις. Στο πλαίσιο αυτής της εργασίας παρακολουθήσαμε απομακρυσμένα τις εργασίες του συνεδρίου Critical Communication World 2022 (ο σύνδεσμος πρόσβασης είναι: On-Demand Sessions (swapcard.com)) που έλαβε χώρα στη Βιέννη τον Μάιο του 2022. Ο διαδικτυακός της τόπος είναι προσβάσιμος από το σύνδεσμο The Critical Communications Association - TCCA.

3.1.8 Πληροφοριακά Συστήματα Αντιμετώπισης και Διαχείρισης Κρίσεων

Η κύρια αποστολή της Ένωσης των Πληροφοριακών Συστημάτων Αντιμετώπισης και Διαχείρισης Κρίσεων (Information Systems for Crisis Response and Management – ISCRAM) είναι να ενθαρρύνει την προώθηση της έρευνας, της ανταλλαγής γνώσεων και της ανάπτυξης συστημάτων πληροφοριών για τη διαχείριση κρίσεων, συμπεριλαμβανομένων των κοινωνικών, τεχνικών και πρακτικών πτυχών όλων των συστημάτων πληροφοριών και επικοινωνιών που χρησιμοποιούνται σε όλες τις φάσεις διαχείρισης καταστάσεων έκτακτης ανάγκης, καταστροφές και κρίσεις. Το ISCRAM χρησιμοποιήθηκε για πρώτη φορά στο πρώτο διεθνές εργαστήριο στις Βρυξέλλες το 2004. Διαθέτει μια πολύ καλή ηλεκτρονική βιβλιοθήκη άρθρων που σχετίζονατι με τα ζητήματα επικοινωνίας στη διαχείριση καταστάσεων έκτακτης ανάγκης. Ο διαδικτυακός της τόπος είναι προσβάσιμος από το σύνδεσμο ISCRAM Digital Library -- Home.

3.1.9 Ένωση Κινητών Δικτύων Επικοινωνίας Επόμενης Γενιάς

Η Ένωση Κινητών Δικτύων Επικοινωνίας Επόμενης Γενιάς (Next Generation Mobile Network Alliance – NGMN) είναι ένα ανοιχτό φόρουμ που ιδρύθηκε από παρόχους δικτύων κινητής τηλεφωνίας παγκοσμίως. Στόχος του είναι να διασφαλίσει ότι οι υποδομές δικτύου επόμενης γενιάς, οι πλατφόρμες υπηρεσιών και οι συσκευές θα ανταποκρίνονται στις απαιτήσεις των παρόχων και θα ικανοποιούν τη ζήτηση και τις προσδοκίες του τελικού χρήστη. Οι συμμετέχοντες είναι:

1. Φορείς εκμετάλλευσης δικτύων κινητής τηλεφωνίας (Μέλη),

2. Προμηθευτές, εταιρείες λογισμικού και άλλοι παράγοντες του κλάδου (Συντελεστές) και
3. Ινστιτούτα έρευνας που συμβάλλουν ουσιαστικά στη μεσοπρόθεσμη έως μακροπρόθεσμη καινοτομία (Σύμβουλοι)

Το όραμα της NGMN Alliance είναι να παρέχει αποτελεσματική καθοδήγηση για την επίτευξη καινοτόμων και οικονομικά προσιτών υπηρεσιών κινητής τηλεφωνίας για τον τελικό χρήστη, με ιδιαίτερη έμφαση στην υποστήριξη της πλήρους εφαρμογής του 5G. Οι πρωτοβουλίες στο πλαίσιο του οράματός της συνεισφέρουν σημαντικά στη δημόσια ασφάλεια, της οποίας οι σχέσεις με την κινητή τηλεφωνία αναλύονται διεξοδικά στην παρούσα εργασία. Μάλιστα, στο πλαίσιο της μελέτης της βιβλιογραφίας για τα δίκτυα δημόσιας ασφάλειας και τις τεχνολογίες που υλοποιούν αυτά αξιοποιήθηκαν πολλές δημοσιεύεις και ερευνητικές προσπάθειες που φιλοξενούνται στον διαδικτυακό της τόπο, ο οποίος είναι προσβάσιμος από το σύνδεσμο NGMN – We make better connections.

3.2 Ευρωπαϊκοί Οργανισμοί

3.2.1 Επικοινωνίες για τη Δημόσια Ασφάλεια στην Ευρώπη

Οι Επικοινωνίες για τη Δημόσια Ασφάλεια στην Ευρώπη (Public Safety Communication Europe – PSCE) είναι ένας μόνιμος αυτόνομος οργανισμός, που εργάζεται για την προώθηση της αριστείας στην ανάπτυξη και χρήση συστημάτων επικοινωνίας και διαχείρισης πληροφοριών δημόσιας ασφάλειας μέσω της οικοδόμησης συναίνεσης. Το PSCE ιδρύθηκε ως αποτέλεσμα ενός έργου που χρηματοδοτήθηκε από την Ευρωπαϊκή Επιτροπή το 2008. Έκτοτε, έχει εξελιχθεί σε ένα ανεξάρτητο φόρουμ, όπου εκπρόσωποι οργανώσεων χρηστών δημόσιας ασφάλειας, βιομηχανίας και ερευνητικών ινστιτούτων μπορούν να συναντηθούν για να συζητήσουν και ανταλλάσσουν ιδέες και βέλτιστες πρακτικές, αναπτύσσουν οδικούς χάρτες και βελτιώνουν το μέλλον των επικοινωνιών για τη δημόσια ασφάλεια. Συμμετέχει σε πολλά ερευνητικά έργα στο πεδίο, τα οποία εντάχθηκαν επί το πλείστον στο πρόγραμμα Horizon 2020, σε κάποια από τα οποία αναφερόμαστε εκτενώς στην παρούσα εργασία. Χαρακτηριστικότερα εξ αυτών είναι το BroadWay, BroadGNSS, RESPOND-A, Search and Rescue, Core, Copernicus. Διεξάγει διεθνή συνέδρια και webinars ιδιαίτερης αξίας και σπουδαιότητας για τον κλάδο και τα στελέχη της συμμετέχουν σε αντίστοιχες εκδηλώσεις. Η αμέσως προηγούμενη εκδήλωση ήταν η ετήσια διάσκεψη που πραγματοποιήθηκε την 5/6 Δεκεμβρίου 2022 στις Βρυξέλλες, με αξιοσημείωτα αποτελέσματα για τις επικοινωνίες των πρώτων ανταποκριτών και πολλές από τις προσεγγίσεις που επιχειρήθηκαν στο πλαίσιο της διάσκεψης αποτέλεσαν αντικείμενο μελέτης. Ο διαδικτυακός της τόπος είναι προσβάσιμος από το σύνδεσμο Homepage - PSCE (psc-europe.eu).

3.2.2 Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων

Το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (European Telecommunications Standards Institute – ETSI) είναι ένα περιβάλλον που υποστηρίζει την έγκαιρη ανάπτυξη, επικύρωση και δοκιμή παγκόσμιων προτύπων για συστήματα, εφαρμογές και υπηρεσίες με δυνατότητα ΤΠΕ. Αριθμεί ως μέλη πλέον των ενιακοσίων (900) οργανισμών που προέρχονται από περισσότερες από 60 χώρες και πέντε ηπείρους. Το ETSI παρέχει συνεργατικές πλατφόρμες για την ανάπτυξη και την προώθηση των προτύπων για συστήματα και υπηρεσίες ΤΠΕ, που χρησιμοποιούνται παγκοσμίως προς όφελος όλων. Επιπλέον, παρέχει στα μέλη ένα ανοιχτό και χωρίς αποκλεισμούς περιβάλλον για την υποστήριξη της έγκαιρης ανάπτυξης, επικύρωση και δοκιμή παγκόσμιων προτύπων για συστήματα με δυνατότητα ΤΠΕ, εφαρμογές και υπηρεσίες σε όλους τους τομείς της βιομηχανίας και της κοινωνίας και οδηγεί στην ανάπτυξη προτύπων που επιτρέπουν μια βιώσιμη και ασφαλώς συνδεδεμένη κοινωνία. Αναγνωρίζεται επίσημα από την Ευρωπαϊκή Ένωση ως Ευρωπαϊκός Οργανισμός Τυποποίησης (ESO). Ο διαδικτυακός του τόπος είναι προσβάσιμος από το σύνδεσμο ETSI - Welcome to the World of Standards!.

3.2.3 Ευρωπαϊκή Ένωση Αριθμών Έκτακτης Ανάγκης

Η Ευρωπαϊκή Ένωση Αριθμών Έκτακτης Ανάγκης (European Emergency Number Association – EENA) είναι μη κυβερνητική οργάνωση με αποστολή να συμβάλει στη βελτίωση της ασφάλειας και της ασφάλειας των ανθρώπων. Περιλαμβάνει πάνω από 1500 εκπροσώπους υπηρεσιών έκτακτης ανάγκης από περισσότερες από 80 χώρες παγκοσμίως (παρόχους, ερευνητές, μέλη του Ευρωπαϊκού Κοινοβουλίου κ.λπ.) και λειτουργεί ως πλατφόρμα για όσους ασχολούνται με τη δημόσια ασφάλεια. Η συμβολή του στη δημόσια ασφάλεια αναλύεται διεξοδικά στο κεφάλαιο 5.1.2.2.1. Ο διαδικτυακός της τόπος είναι προσβάσιμος από το σύνδεσμο EENA - The European Emergency Number Association.

3.2.4 EURESCOM

Η Eurescom είναι κορυφαίος ευρωπαϊκός πάροχος υπηρεσιών διαχείρισης και υποστήριξης στον τομέα της υψηλής τεχνολογίας, με έμφαση στις ΤΠΕ. Η αποστολή της είναι να επιτρέψει την καινοτομία μέσω της συνεργασίας. Η εταιρεία έχει περισσότερες από δύο δεκαετίες εμπειρίας στη διαχείριση πολυεθνικών συνεργατικών έργων, προγραμμάτων και πρωτοβουλιών στον τομέα των ΤΠΕ. Οι υπηρεσίες της περιλαμβάνουν την έναρξη, τη διαχείριση και την υποστήριξη διεθνών προγραμμάτων και έργων έρευνας και ανάπτυξης καθώς και την παροχή της διοικητικής υποδομής για τεχνολογικές πρωτοβουλίες. Οι πελάτες της Eurescom περιλαμβάνουν μεγάλους ευρωπαϊκούς φορείς εκμετάλλευσης τηλεπικοινωνιακών δικτύων και παρόχους υπηρεσιών, παγκόσμιους κατασκευαστές ΤΠΕ,

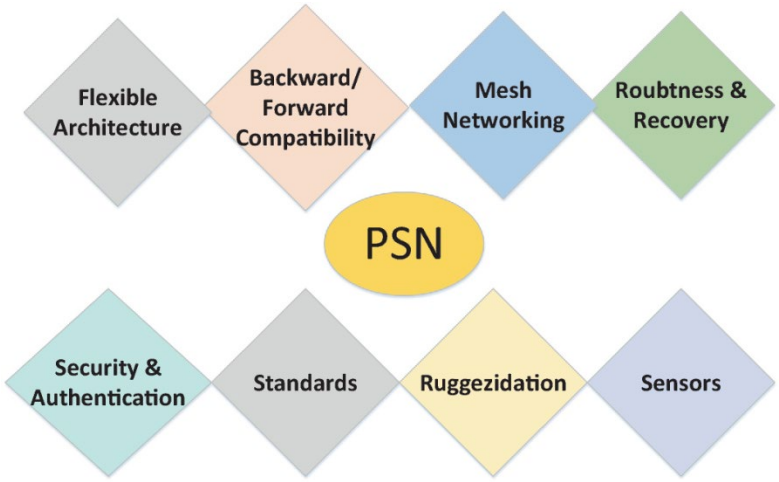
πολυεθνικές πρωτοβουλίες τεχνολογίας και την Ευρωπαϊκή Ένωση. Την παρούσα χρονική στιγμή είναι ανοιχτά έντεκα (11) ερευνητικά προγράμματα που στοχεύουν στη διερεύνηση υλοποίησης συνδεσιμότητας με την εμπλοκή της τεχνητής νοημοσύνης, καθώς επίσης έξυπνα δίκτυα και υπηρεσίες επόμενης γενιάς (6G), τα οποία δυνητικά και ως μελλοντικές προεκτάσεις μπορούν να εμπλακούν στην υλοποίηση των PSNs. Ο διαδικτυακός της τόπος είναι προσβάσιμος από το σύνδεσμο Eurescom GmbH – Innovation through collaboration.

4 *Τεχνολογίες στις κρίσιμες επικοινωνίες*

Πρωτεύοντα ρόλο στην υλοποίηση του εγχειρήματος βελτίωσης των παρεχόμενων τεχνολογικών λύσεων στους πρώτους ανταποκριτές και τους επαγγελματίες της δημόσιας ασφάλειας, όπως είναι αναμενόμενο, διαδραματίζουν οι διαθέσιμες τεχνολογίες. Ποιες τεχνολογίες είναι εφικτό να εμπλέκονται στη δημιουργία δικτύων δημόσιας ασφάλειας, την κατασκευή συσκευών και υλοποίηση εφαρμογών από τις εταιρίες του χώρου; Είναι δόκιμη προσέγγιση να θεωρούμε κάθε τεχνολογία, δοκιμασμένη ή μη, ικανή να υποστηρίζει μια τέτοια «λύση»;

Όπως έχει κατ` επανάληψη αποτυπωθεί στη σχετική βιβλιογραφία, η δημόσια ασφάλεια δεν μπορεί να κάνει οποιαδήποτε έκπτωση στη διαθεσιμότητα, πολύ απλά επειδή οι συνέπειες όποιας ενδεχόμενης αστοχίας στο πεδίο συνεπάγεται αυτόματα την απώλεια ανθρώπινης ζωής. Επομένως, οι επιλογές θα πρέπει να είναι ιδιαιτέρως προσεκτικές και να «ντύνουν» τις στολές των επαγγελματιών, μόνον εφόσον υπάρχει η διαβεβαίωση ότι θα λειτουργήσουν στο πεδίο. Δεν αποκλείουμε τις τεχνολογίες που είναι σε εξέλιξη, ή που δεν μπορούν να μας δώσουν εγγυημένα αποτελέσματα, αλλά τις προσαρτούμε προσεκτικά, με μικρά και σταθερά βήματα, τέτοια που η όποια αστοχία δεν θα χαρακτηρίζεται μοιραία.

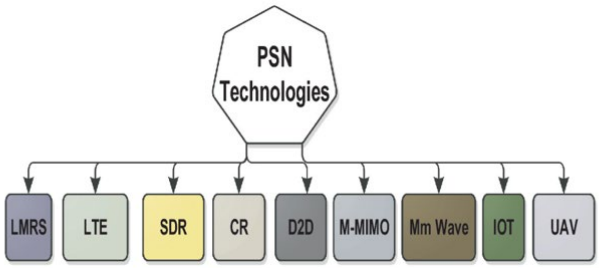
Ας δούμε όμως αναλυτικά με ποιον τρόπο αυτό το μίγμα δοκιμασμένων τεχνολογικών απαντήσεων, φιλόδοξων λύσεων του σήμερα, αλλά και του τεχνολογικού αύριο μπορούν να συνθέσουν το καλύτερο δυνατό αποτέλεσμα. Ο λόγος για τις τεχνολογίες που εμπλέκονται στη δημιουργία δικτύων δημόσιας ασφάλειας και κρίσιμων επικοινωνιών (Critical Communications Networks - CCN), που περιλαμβάνουν ένα ασύρματο δίκτυο που αναπτύσσεται για να καλύψει τις ανάγκες υπηρεσιών όπως η αστυνομία, η πυροσβεστική, το λιμενικό, ή το ΕΚΑΒ που προστρέχουν να επιληφθούν επιχειρησιακά [48]. Αυτονόητο είναι ότι ένα τέτοιο δίκτυο μπορεί να καταλαμβάνει από μια περιοχή ενός δήμου, έως την γεωγραφική έκταση μιας η περισσοτέρων χωρών, ανάλογα το περιστατικό.



Εικόνα 18. Επιθυμητά χαρακτηριστικά των δικτύων δημόσιας ασφάλειας [49], [50]

Οι ανάγκες για επικοινωνία και αποστολή δεδομένων ποικίλλει κατά περίπτωση, καθώς αυτές μπορεί να περιοριστούν μέσα στο δίκτυο, ή το δίκτυο αυτό να συνδεθεί με άλλα δίκτυα, ή βάσεις δεδομένων, ή ακόμη και με το διαδίκτυο ώστε να αυξηθεί η αποτελεσματικότητα των πρώτων ανταποκριτών [51]. Στο δεύτερο κεφάλαιο του βιβλίου [49] ορίζεται ότι τα δίκτυα δημόσιας ασφάλειας είναι ειδικά σχεδιασμένα ασύρματα δίκτυα που χρησιμοποιούνται από τους πρώτους ανταποκριτές και τις υπηρεσίες έκτακτης ανάγκης σε περίπτωση οποιασδήποτε καταστροφής. Η ίδια προσέγγιση αναφέρεται σε έναν αριθμό απαιτητών χαρακτηριστικών των PSN, τα οποία προκύπτουν σχηματικά από την Εικόνα 18 [50].

Οκτώ διαφορετικά στοιχεία – πυλώνες συνθέτουν τα επιθυμητά χαρακτηριστικά των δικτύων δημόσιας ασφάλειας. Η *ευέλικτη αρχιτεκτονική (Flexible Architecture)*, που ερμηνεύεται αφενός με την αποδοτική συνεργασία διαφορετικών τύπων συσκευών και την ανταλλαγή διαφορετικών μορφών δεδομένων (φωνή, κείμενο, εικόνα) και αφετέρου με τη δημιουργία προοπτικής για ένταξη νέων τεχνολογιών στις υφιστάμενες δομές. Αυτό συνεπάγεται τη δεύτερη καίρια απαίτηση, που ορίζεται ως *συμβατότητα* (*Backward/Forward Compatibility*) τόσο προς τα πίσω, ήτοι με τις παλαιότερες τεχνολογικές γενικές, όσο και προς τα εμπρός, στο οποίο ήδη αναφερθήκαμε. Μια άλλη απαίτηση είναι η *δικτύωση πλέγματος (Mesh Networking)*, ικανή να παρέχει στο δίκτυο χρήση υψηλών συχνοτήτων και μεγάλου εύρους φασματική ζώνη. Σημαντικά στοιχεία του δικτύου, όπως ήδη έχουμε αναφέρει και σε επίπεδο απαιτήσεων, είναι η *ανθεκτικότητα (Robustness)*, καθώς σε πλείστες περιπτώσεις καλείται ν' ανταποκριθεί ακόμη και με κατεστραμμένα κύρια τμήματα της υποδομής του, όσο και η γρήγορη *ανάκαμψη (Recovery)* από τέτοιες κατατάσσεις. Στην ίδια λογική και ταυτόσημα με τις απαιτήσεις, η *ασφάλεια* (*Security*) και ο *έλεγχος ταυτότητας (Authentication)* των χρηστών συνιστούν ξεχωριστούς πυλώνες απαιτητών χαρακτηριστικών, ενώ η συμβατότητα και η ευελιξία της αρχιτεκτονικής αλληλεξαρτώνται από το βαθμό που η αρχιτεκτονική των δικτύων δημόσιας ασφάλειας στηρίζεται σε *τεχνολογικά πρότυπα (Standards)*.



Εικόνα 19. Τεχνολογίες ενεργοποίησης των δικτύων δημόσιας ασφάλειας: (a)Land Mobile Radio System, (b)Long Term Evolution, (c)Software Defined Radio, (d)Cognitive Radio, (e)Device-to-Device, (f) Multiple Input Multiple Output, (g)Millimeter Wave, (i)Internet of Things, (j)Unmanned Air Vehicle [49]

Τα δύο τελευταία βασικά χαρακτηριστικά είναι αφιερωμένα στο υλικό, τα «μάτια και τ` αυτιά» των δικτύων που είναι οι *αισθητήρες (Sensors)* και οι συσκευές χρήστη, θα πρέπει να χαρακτηρίζονται από *ανθεκτικότητα (Ruggedization)*, αξιοπιστία και αποτελεσματικότητα. Στις εμπλεκόμενες τεχνολογίες, όπως προκύπτει στην Εικόνα 19, περιλαμβάνεται το σύνολο της τεχνολογικής παλέτας που εκτείνεται από τα αναλογικά συστήματα επικοινωνίας έως την αντικατάσταση αυτών από ασύρματα ψηφιακά [44].

Σαφέστατα, η παλέτα αυτή μπορεί να εμπλουτιστεί περαιτέρω από ένα σύνολο αξιόλογων και σημαντικών τεχνολογιών. Ήδη στην προσέγγιση που επιχειρούν οι [52] έχουν προστεθεί οι οπτικές ασύρματες επικοινωνίες, αλλά και οι δορυφορικές όμοιες, τις οποίες θα αναλύσουμε διεξοδικά σε ξεχωριστό κεφάλαιο στη συνέχεια. Επιπρόσθετα, θα ήταν άστοχο να μην ενταχθούν στις τεχνολογίες που θα μας απασχολήσουν, οι όποιες εξελίξεις έχουν επιτευχθεί σε κάθε ξεχωριστό πεδίο. Χαρακτηριστικό είναι λοιπόν ότι η τεχνολογική εξέλιξη που έφερε το LTE, οδήγησε στην αντίστοιχη του LTE-Advanced και αντίστοιχα στο 5G, που είναι ο σημερινός σταρ του πεδίου. Επιπλέον, στη λογική της δυνατότητας πλήρους πλουραλιστικής προσέγγισης του θέματος των εμπλεκόμενων τεχνολογιών, η οπτική των [53] προκύπτει σχηματικά στην Εικόνα 20, όπου οι τεχνολογίες συσχετίζονται με τους χρήστες δημόσιας ασφάλειας, με σύνθημα: «*για ν' αποκτήσετε / παρέχετε τις σωστές πληροφορίες, τη σωστή στιγμή, στο σωστό μέρος, στο σωστό άτομο... για τη σωστή απόφαση*».

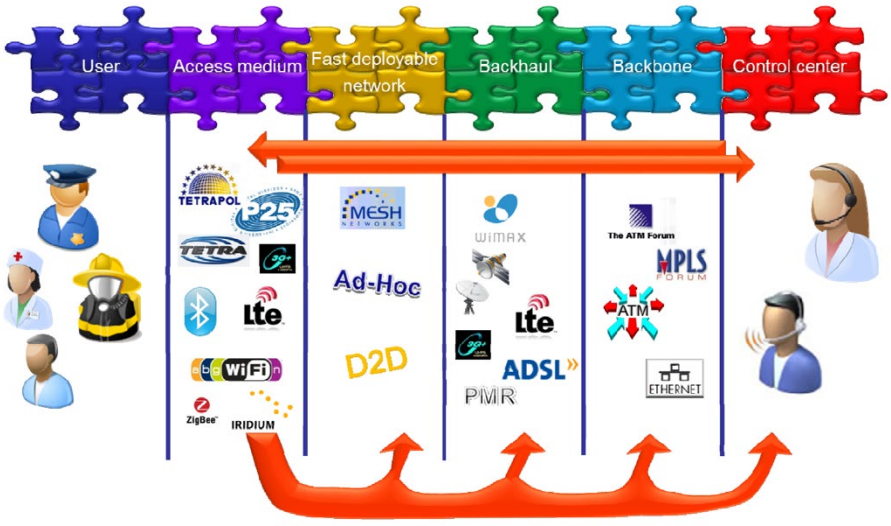
Τέλος, σύμφωνα με την πρώτη έκδοση White Paper της IEEE Future Directions Committee [54], οι τεχνολογίες που χρησιμοποιούνται σήμερα στη δημόσια ασφάλεια, αλλά και αυτές που εκτιμάται ότι θα χρησιμοποιηθούν στην τεχνολογική εξέλιξη του πεδίου, κατηγοριοποιήθηκαν ως ακολούθως:

1. *Τεχνολογίες επικοινωνίας στενής ζώνης* (LMR, P25, TETRA, DMR, TETRAPOL), που επιτυγχάνουν κυρίως κάλυψη μεγάλων περιοχών, αποδοτική χρησιμοποίηση φάσματος και καλές φωνητικές επικοινωνίες.
2. *Ευρυζωνικές τεχνολογίες επικοινωνίας* (LTE, 5G, FirstNet, Wi-Fi), που επιτυγχάνουν γρήγορη πρόσβαση στο διαδίκτυο, μετάδοση δεδομένων, γεωεντοπισμό και υποστηρίζουν πολλές και απαιτητικές από άποψη πόρων εφαρμογές δεδομένων

3. Εξειδικευμένα δίκτυα και επικοινωνίες, όπως *Ad Hoc, Mesh, Tactical, Ham Radio*, που επιτυγχάνουν επέκταση κάλυψης, επιτρέπουν τις συσκευές να επικοινωνούν μεταξύ τους όταν η υποδομή έχει προβλήματα και μπορεί να παρέχει σύνδεση σε ετερογενή δίκτυα.
4. *Δορυφορικές επικοινωνίες, επικοινωνίες αέρα και οχημάτων* (Δορυφόροι, UAVs, αεροσκάφη, ηλεκτρικά οχήματα, συσκευές επικοινωνίας, προσαρτημένες συσκευές, αισθητήρες, υπολογιστές εγκατεστημένοι σε οχήματα, κ.λπ.), που επιτυγχάνουν επιχειρησιακή υποστήριξη όταν η κύρια σταθερή επικοινωνιακή υποδομή έχει καταστραφεί ή δεν επαρκεί να καλύψει τις ανάγκες σε κρίσιμες καταστάσεις και συμβάντα (επιχειρήσεις διάσωσης, καταστροφικές πυρκαγιές, κ.λπ.)
5. Δικτύωση στα άκρα ή στο σύννεφο (*Cloud/Fog/Edge Computing and Networking*) που παρέχει γρήγορη επεξεργασία, αποδοτικότερη διαχείριση πόρων και πρόσβαση σε βάσεις δεδομένων από παντού
6. *Σύστημα γεωγραφικού εντοπισμού* και *συστήματα προσδιορισμού θέσεως*, που μπορεί να λειτουργήσει υποστηρικτικά σε πλείστες περιπτώσεις καταστροφών και διαχείρισης κρίσεων (προσδιορισμός θέσης πρώτων ανταποκριτών και θυμάτων)
7. Σύστημα αναγνώρισης προσώπων, που μπορεί να παρέχει ουσιαστική συνδρομή σε περιπτώσεις επιβολής του νόμου (γρήγορη ταυτοποίηση αναζητούμενων ατόμων), αλλά και να υποστηρίξει σε επίπεδο ασφάλειας τα συστήματα και τις εφαρμογές δημόσιας ασφάλειας, παρέχοντας τη δυνατότητα διασφάλισης της πρόσβασης
8. Τεχνολογίες επιτήρησης, οι οποίες μπορούν να χρησιμοποιηθούν σε ευρύ φάσμα περιπτώσεων δημόσιας ασφάλειας (επιτήρηση κρίσιμων υποδομών, παρακολούθηση χώρων, κ.λπ.)
9. Έξυπνοι αισθητήρες και συστήματα (Έξυπνο σύστημα ηλεκτροφωτισμού, Smart Streets Lighting systems, Κάμερες σώματος, Βιομετρικοί αισθητήρες σώματος, Biometric monitoring systems, Συστήματα αντιμετώπισης καταστάσεων έκτακτης ανάγκης και ακραίων καιρικών συνθηκών, Αισθητήρες, IoT συσκευές), που χρησιμοποιούνται στην λήψη κρίσιμων μετρικών από το περιβάλλον που λαμβάνουν χώρα τα γεγονότα, και βιομετρικών στοιχείων των πρώτων ανταποκριτών ή των θυμάτων.
10. Τεχνητή νοημοσύνη (Αναλυτική δεδομένων, Τεχνητή Νοημοσύνη, Μηχανική Μάθηση, Ρομποτική, Προβλεπτική αστυνόμευση). Η άκρως αναπτυσσόμενη πτυχή της τεχνολογικής εξέλιξης που ακούει στο όνομα τεχνητή νοημοσύνη, αλλά και όλα τα παρακλάδια αυτής, όπως η μηχανική μάθηση, φιλοδοξούν να υποστηρίξουν ουσιαστικά και τον τομέα της δημόσιας ασφάλειας. Μεγάλο εύρος εφαρμογών μπορούν να «στηριχθούν» πλέον στον τομέα της τεχνητής νοημοσύνης με αναμενόμενα οφέλη σε χαρακτηριστικούς τομείς όπως για παράδειγμα την

εγκληματικότητα, την αντιμετώπιση εκτάκτων αναγκών (μοντέλα πρόβλεψης), την αποτελεσματικότητα στο πεδίο (καταπολέμηση του εγκλήματος, πυρκαγιών, διαχείριση κρίσεων, υποστήριξη ανακρίσεων, κ.λπ.). Στον τομέα αυτό έχουν σημαντική απήχηση και τα μέσα κοινωνικής δικτύωσης.

11. Ψηφιακός κόσμος (Ψηφιακή Πραγματικότητα, Επαυξημένη πραγματικότητα, Εικονική Πραγματικότητα, Ψηφιακά Δίδυμα). Η εικονική πραγματικότητα, η επαυξημένη πραγματικότητα και τα ψηφιακά αντίγραφα μπορούν να συνεισφέρουν τα μέγιστα στη βελτίωση της επίγνωσης της κατάστασης, της λήψης αποφάσεων, τη μείωση του κόστους, τη βελτίωση των συνθηκών εκπαίδευσης του προσωπικού και την ασφαλή προσομοίωση των συνθηκών μιας κρίσιμης κατάστασης προς την κατεύθυνση καλύτερης αντιμετώπισης αυτής.
12. Blockchain, το οποίο έχει κατ` εξοχήν εφαρμογή στα δίκτυα, καθώς βρίσκει εφαρμογή η κυρίαρχη φιλοσοφία που το διακατέχει και αφορά στα δίκτυα ομότιμων κόμβων.
13. Ζητήματα ενεργειακής διαχείρισης για την αποδοτική ενεργειακή υποστήριξη των υποδομών και συσκευών



Εικόνα 20. Τεχνολογίες και συσχετίσεις χρηστών δημόσιας ασφάλειας [53]

4.1 Land Mobile Radio System

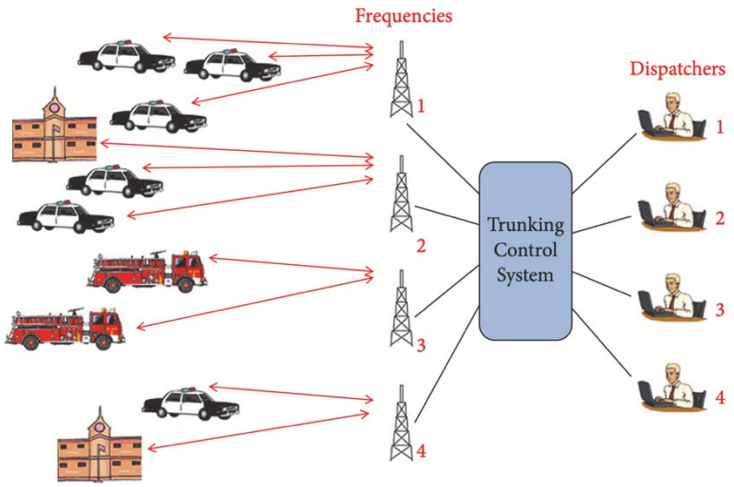
Οι τεχνολογίες Επίγειου Κινητού Ραδιοσυστήματος (Land Mobile Radio – LMR) έχουν χρησιμοποιηθεί εκτενώς στην ανάπτυξη των PSNs μέχρι σήμερα. Τα δίκτυα LMR υποστηρίζουν εξελιγμένες εφαρμογές φωνής που μπορούν, ως ένα βαθμό, να αντιμετωπίσουν την κρισιμότητα της φύσης των υπηρεσιών της δημόσιας ασφάλειας. Ωστόσο, τα δίκτυα LMR δεν διαθέτουν τις απαιτούμενες τεχνολογικές εξελίξεις για την υποστήριξη ευρυζωνικών εφαρμογών [43]. Τα πιο γνωστά παραδείγματα δικτύων LMR για PSN αποτελούν το TETRA, το DMR και το P25, τα οποία μαζί με άλλους εκπροσώπους του

πεδίου θα αναλυθούν εκτενώς στο επόμενο κεφάλαιο. Στην παραδοσιακή εκδοχή ενός δικτύου LMR, οι πρώτοι ανταποκριτές συνδέονται με τις υπηρεσίες αποστολής και μεταξύ τους μέσω σημείων πρόσβασης ραδιοφώνου ή επαναλήπτες [55] (Εικόνα 21).

Το Επίγειο Κινητό Ραδιοσύστημα (Land Mobile Radio System – LMRS) εξασφαλίζει αμφίδρομες φωνητικές επικοινωνίες. Υπάρχουν *Δημόσια* LMRSs, τα οποία προορίζονται να καλύψουν τις ανάγκες της δημόσιας ασφάλειας και *Ιδιωτικά* LMRSs, που προορίζονται για εμπορική χρήση (π.χ. βιομηχανία, δίκτυα ραδιοταξί, εταιρίες παροχής υπηρεσιών ασφάλειας, κ.λπ.). Τα LMRSs χρησιμοποιούν κανάλια στις ζώνες VHF ή UHF, καθώς οι κεραίες σε αυτά τα μικρά μήκη κύματος είναι αρκετά μικρές για να τοποθετηθούν τόσο σε οχήματα, όσο και σε πομποδέκτες χειρός. Η ισχύς του πομπού περιορίζεται συνήθως σε λίγα Watt και παρέχει αξιόπιστη εμβέλεια εργασίας της τάξης των 4,8 έως 32 km, ανάλογα με το έδαφος. Για την αύξηση της περιοχής κάλυψης χρησιμοποιούνται επαναλήπτες, που τοποθετούνται σε «ορατά» σημεία (π.χ. συνήθως πολύ ψηλά κτίρια, λόφους ή βουνοκορφές). Τα παλαιότερα συστήματα χρησιμοποιούν διαμόρφωση AM, ή FM, ενώ ορισμένα πρόσφατα συστήματα χρησιμοποιούν ψηφιακή διαμόρφωση (FDMA, TDMA) που τους επιτρέπει να μεταδίδουν δεδομένα καθώς και ήχο [56].

Το LMR έχει χρησιμοποιηθεί παγκοσμίως και έχει αποδειχθεί ως ένα από τα πιο αξιόπιστα εργαλεία φωνητικής επικοινωνίας για κρίσιμους χρήστες σε πολύ σκληρά περιβάλλοντα και τις πιο ακραίες συνθήκες. Συνεργάζεται στενά με εφαρμογές συστήματος, αποστολής και λογισμικού και γίνεται διαλειτουργικό μέσω της ενσωμάτωσης με άλλα συστήματα (π.χ. PSTN, η τηλεδιάσκεψη, κ.λπ.), επεκτείνοντας περαιτέρω την ικανότητά του να ενδυναμώνει κρίσιμους χρήστες επικοινωνίας.

Η αρχιτεκτονική, τα τεχνικά χαρακτηριστικά, οι εφαρμογές και οι περιπτώσεις χρήσης των βασικών προτύπων παρουσιάζονται αναλυτικά στη συνέχεια, για κάθε μία περίπτωση ξεχωριστά.



Εικόνα 21. Τυπική αρχιτεκτονική διάταξη δικτύου LMR για PSN [55]

4.2 Long Term Evolution

4.2.1 Ιστορικό

Το Long Term Evolution (LTE) είναι μια εξέλιξη των τεχνολογιών δεύτερης γενιάς και συγκεκριμένα του Παγκόσμιου Συστήματος Κινητών Επικοινωνιών (Global System for Mobile Communications - GSM) και τρίτης γενιάς και συγκεκριμένα της Πολλαπλής Πρόσβασης Διαίρεσης Κώδικα Ευρυζωνικής (Wideband Code Division Multiple Access – WCDMA) [57]. Αναπτύχθηκε από το 3GPP ως κινητή ευρυζωνική τεχνολογία τέταρτης γενιάς (4G), με κυρίαρχο σκοπό ν‘ αυξήσει τη χωρητικότητα και την ταχύτητα μετάδοσης δεδομένων στα ασύρματα δίκτυα επικοινωνίας [48]. Βασικός στόχος της εργασίας που ξεκίνησε το 2004, στο πλαίσιο της όγδοης έκδοσης του προτύπου (3GPP Release 8) ήταν να επιτευχθούν υψηλότεροι ρυθμοί δεδομένων (πάνω από 100 Mbps downlink, πάνω από 50 Mbps uplink) και χαμηλότερη καθυστέρηση, καθώς και ένας αριθμός άλλων βελτιώσεων [58].

Η «γέννηση» του LTE στηρίχθηκε στα καίρια τεχνολογικά επιτεύγματα των προγενέστερων εκδόσεων του 3GPP. Στον Πίνακας 1 προκύπτει μια συνολική αποτύπωση των οροσήμων αυτών, εκ των οποίων αξίζει να σταθούμε σε τρείς τεχνολογικές καινοτομίες:

- Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών (Universal Mobile Telecommunications System - UMTS) (Release 99/4),
- Πρόσβαση Πακέτων Υψηλής Ταχύτητας (High Speed Packet Access - HSPA) (Release 5,6,7) και
- HSPA+ (Release 7, 8, 9, 10).

Από την αναλογική τεχνολογία κινητής τηλεφωνίας της πρώτης γενιάς και το πρότυπο Προηγμένο Σύστημα Κινητής Τηλεφωνίας (Advanced Mobile Phone System - AMPS), του φασματικού εύρους συχνοτήτων 800-900MHz (τεχνική διαμόρφωσης σήματος FDMA) που έδινε χαμηλής ποιότητας φωνητικές υπηρεσίες και ογκώδεις τερματικές συσκευές σε ρυθμούς που άγγιζαν τα 1,9 Kbps, μεταβήκαμε στα δίκτυα δεύτερης γενιάς (2G, 2.5G, 2.75G), τη μετεξέλιξη από αναλογικά σε ψηφιακά δίκτυα και το πρότυπο General Packet Radio Service (GPRS), που βασίστηκε στην κυψελοειδή τεχνολογία και το πρότυπο GSM που λειτουργούσε στην μπάντα συχνοτήτων 890-915 MHz (uplink) / 935-960 MHz (downlink), ή σε αντίστοιχου εύρους ζώνες των 1800,1900 MHz (τεχνικές διαμόρφωσης σήματος TDMA/CDMA) με νέες υπηρεσίες όπως δυνατότητα ανταλλαγής μηνυμάτων (SMS/MMS) και ρυθμούς μετάδοσης από 9,6Kbps έως 384 Kbps [58].

Ο βασικός στόχος της ανάπτυξης των κινητών δικτύων τρίτης γενιάς ήταν η παροχή των κινητών υπηρεσιών «οπουδήποτε» και «οποτεδήποτε», αλλά και η δυνατότητα παροχής υπηρεσιών διαδικτύου και πολυμέσων (ήχος, εικόνα, κείμενο) [59]. Για να επιτευχθεί ο στόχος, στα δίκτυα τρίτης γενιάς το φάσμα συχνοτήτων που αξιοποιείται κυμαίνεται από 1,8 έως 2,4GHz και χρησιμοποιείται πλέον η τεχνολογία WCDMA που είναι η πιο γνωστή παραλλαγή του UMTS [60]. Λόγω της αρχιτεκτονικής του δικτύου UMTS επιτυγχάνονται ρυθμοί μετάδοσης από 384 Kbps (αυξημένη κινητικότητα) έως 2Mbps (ακίνητοι χρήστες). Περαιτέρω αύξηση του ρυθμού μετάδοσης επιτεύχθηκε με τα τεχνολογικά πρότυπα του 3GPP που εισήγαγαν τήν Πρόσβαση Πακέτων Υψηλής Ταχύτητας Καθόδου (High Speed Downlink Packet Access – HSDPA) (Release 5) και την Πρόσβαση Πακέτων Υψηλής Ταχύτητας Ανόδου (High Speed Uplink Packet Access – HSUPA) (Release 6), αντίστοιχα. Οι συγκεκριμένες τεχνολογίες ουσιαστικά αποτελούν εξέλιξη του UMTS, αφού κατάφεραν ρυθμούς μετάδοσης των δεδομένων έως και 14,4 Mbps (downlink) και 5.76 Mbps (uplink) [61]. Η αρχιτεκτονική του UMTS αναλύεται διεξοδικά στο [60] και βασίζεται σε δύο βασικές οντότητες: το δίκτυο κορμού (Core Network - CN) και το Δίκτυο Επίγειας Ασύρματης Πρόσβασης (UMTS Terrestrial Radio Access Network - UTRAN). Το δίκτυο κορμού είναι υπεύθυνο για την δρομολόγηση των τηλεφωνημάτων καθώς και για τις συνδέσεις για μεταφορά δεδομένων με εξωτερικά δίκτυα. Αντίθετα, το UTRAN είναι υπεύθυνο για οτιδήποτε σχετίζεται με το ασύρματο μέρος του δικτύου.

Release	Date	Main content
Phases 1 and 2	1992 and 1995	Basic GSM functions
Release 96, 97, 98, 99	1996, 1997, 1998, 1999	GPRS, HSCSD, EDGE, UMTS
Release 4	2001	MSC server split architecture
Release 5	2002	HSDPA, IMS
Release 6	2004	HSUPA, MBMS, Push to Talk over Cellular (PoC)
Release 7	2007	HSPA, EDGE evolution
Release 8	2008	LTE/SAE
Release 9	2009	LTE/SAE enhancements, Public Warning System (PWS), IMS emergency sessions over LTE/HSPA
Release 10	2011	LTE Advanced Local IP Access (LIPA) Selective IP Traffic Offload (SIPTO)
Release 11	2012	Heterogeneous Network (HetNet) Support Coordinated Multipoint Operation (CoMP)
Release 12	2014	Public Safety Machine type communication HSPA/LTE carrier aggregation

Πίνακας 1. Τεχνολογικά ορόσημα των εκδόσεων του 3GPP έως την 12η έκδοση

	WCDMA (UMTS)	HSPA HSDPA/HSUPA	HSPA+	LTE	LTE ADVANCED (IMT ADVANCED)
Max downlink speed (bps)	384K	14M	28M	100M	1G
Max uplink speed (bps)	128K	5,7M	11M	50M	500M
Latency Round Trip Time (RTT)	150ms	100ms	50ms (max)	~10ms	Less than 5ms
3GPP Release	Rep99/4	Rel5/6	Rel7	Rel8/9	Rel10
Approx years of initial roll out	2003/4	2005/6HSDPA 2007/8 HSUPA	2008/9	2009/10	
Access methodology	CDMA	CDMA	CDMA	OFDMA/SC-FDMA	OFDMA/SC-FDMA

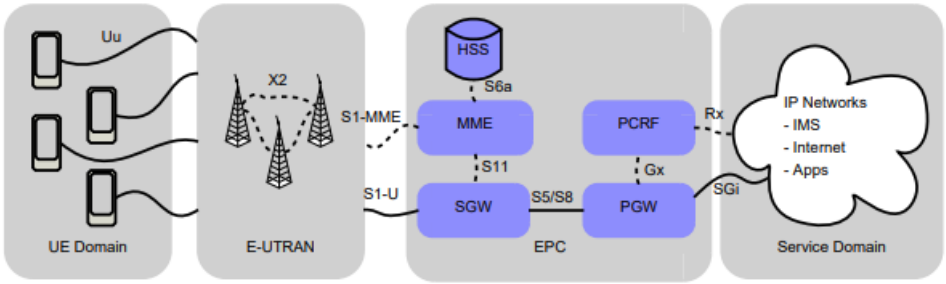
Πίνακας 2. Συγκριτικά στοιχεία τεχνολογικών εξελίξεων έως το LTE-A

Τα δίκτυα UMTS που βασίζονται σε WCDMA παρέχουν μια σαφή εξελικτική διαδρομή για πρόσβαση HSPA. Το HSPA εκτός από τους αυξημένους ρυθμούς μετάδοσης δεδομένων, ενισχύει τη χωρητικότητα και παρέχει σημαντικές μειώσεις καθυστέρησης. Αντίστοιχα, το HSPA+ καθορίζεται στην 7η έκδοση του 3GPP (Release 7) και περιλαμβάνει λειτουργία Πολλαπλής Εισόδου Πολλαπλής Εξόδου (Multiple Input, Multiple Output - MIMO κατερχόμενης ζεύξης, διαμόρφωση υψηλότερης τάξης (downlink 64QAM, uplink 16QAM) και βελτιώσεις πρωτοκόλλου που επιτρέπουν την υποστήριξη μεγάλου αριθμού χρηστών «always on» στο δίκτυο. Οι μέγιστοι ρυθμοί δεδομένων φτάνουν τα 28 Mbps (downlink) και τα 11,5 Mbps (uplink) με χρόνους μετ` επιστροφή, κάτω των 50 ms [61].

Το HSPA+ εμφανίσθηκε και στην 8η και στην 9η έκδοση του 3GPP (Release 8,9), όπου καθορίστηκαν περαιτέρω βελτιώσεις, όπως η λειτουργία διπλού φορέα κατερχόμενης ζεύξης και ο συνδυασμός διαμόρφωσης MIMO και 64QAM. Και οι δύο λειτουργίες επιτρέπουν μέγιστο ρυθμό μετάδοσης δεδομένων 42,2 Mbps (downlink) και 23 Mbps (uplink). Τέλος, στη 10η έκδοση του 3GPP (Release 10) περιλαμβάνονται βελτιώσεις σε σχέση με την αξιοποίηση του φάσματος. Με βάση όσα αναφέρθηκαν ήδη, αλλά και τις σημειώσεις των [59] και [62] συνοψίζουμε τις «επιδόσεις» των τεχνολογιών στις οποίες έγινε αναφορά και θεωρούνται η τεχνολογική βάση του LTE, στον Πίνακας 2.

4.2.2 Βασικά στοιχεία αρχιτεκτονικής του LTE

Τα βασικά στοιχεία της αρχιτεκτονικής του δικτύου LTE φαίνονται στην Εικόνα 22. Ξεχωρίζουν τέσσερα κύρια μέρη (α) Τομέας Εξοπλισμού Χρήστη (User Equipment Domain), (β)Εξελιγμένη Παγκόσμια Υπηρεσία Κινητών Επικοινωνιών (Evolved UMTS), τα οποία αποτελούν Επίγειο Δίκτυο Ραδιοπρόσβασης (Terrestrial Radio Access Network) και συγκεκριμένα E-UTRAN, (γ)Εξελιγμένος Πυρήνας Πακέτου (Evolved Packet Core – EPC) και (δ)Τομέας Υπηρεσιών (Service Domain) [43]. Αντίστοιχα, η αρχιτεκτονική του προτύπου LTE περιγράφεται στην Εικόνα 23 και διεξοδικά στα [57] και [58]. Από τα κύρια χαρακτηριστικά της, γίνονται κατανοητοί οι λόγοι της υπεροχής του LTE έναντι των τότε διαθέσιμων προτύπων και αποσαφηνίζονται τα στοιχεία που το καθιστούν λύση για τη δημιουργία αξιόπιστων, στιβαρών και αποδοτικών PSNs [63].



Εικόνα 22. LTE Network Architecture [43]

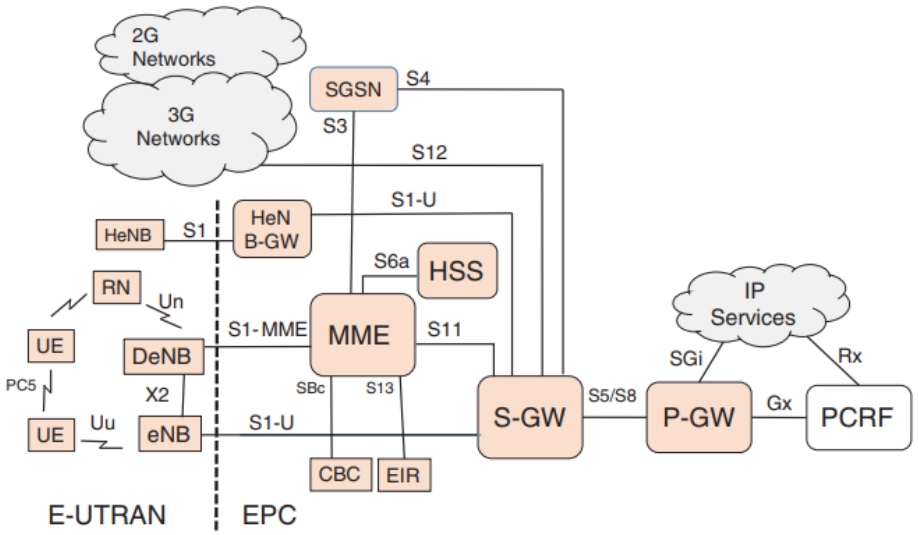
Το E-UTRAN είναι η διεπαφή αέρα μεταξύ του Εξοπλισμού Χρήστη (User Equipment - UE) και των Ενισχυμένων Κόμβων (enhanced Node B - eNB). Με τον όρο UE χαρακτηρίζουμε κάθε συσκευή που επιτρέπει στον τελικό χρήστη να επικοινωνεί μέσω των δικτύων LTE. Οι συνηθέστερες τέτοιες συσκευές είναι ένα έξυπνο τηλέφωνο, ένα tablet, ή ένας φορητός υπολογιστής, ενώ μέσω των συσκευών αυτών γίνεται η έναρξη ή ο τερματισμός των κλήσεων και παρέχονται βασικές υπηρεσίες, όπως η κινητικότητα εντός της κάλυψης του δικτύου και η ενδεχόμενη συνεργασία με άλλα δίκτυα. Στο E-UTRAN, δεν υπάρχει κεντρικός και ξεχωριστός ελεγκτής ραδιοφωνικού δικτύου. Αυτή η λειτουργία είναι ενσωματωμένη στο eNB. Αυτό απλοποιεί την αρχιτεκτονική, καθιστά το δίκτυο πιο αξιόπιστο και επιτρέπει ταχύτερους χρόνους απόκρισης [57]. Όπως φαίνεται από το σχήμα της Εικόνα 23, ένας UE μπορεί να συνδεθεί στο δίκτυο LTE μέσω ενός eNB, ενός Κόμβου Αναμετάδοσης (Relay Node – RN), ενός Δότη eNB (Donor eNB - DeNB), ή ενός Οικίου eNB (Home eNB – HeNB). Τα RN χρησιμοποιούνται για ν` αυξήσουν την απόδοση στα άκρα των κυψελών, την πυκνότητα του δικτύου και την επέκταση κάλυψης. Το DeNB είναι ένα βελτιωμένο eNB που μπορεί να λειτουργήσει ως Φορέας Διαχείρισης Κινητικότητας (Mobility Management Entity - MME, eNB και Πύλη Υπηρεσίας (Service Gateway - S-GW). Το HeNB είναι ένα βελτιστοποιημένο eNB για χρήση σε μικρότερες κυψέλες. Συνολικά, υπάρχουν δώδεκα διαφορετικά ήδη UE.

Το EPC είναι υπεύθυνο για τον συνολικό έλεγχο του δικτύου και των στοιχείων του, για τη διευκόλυνση των υπηρεσιών δεδομένων και φωνής στους χρήστες του. Αποτελείται από τις ακόλουθες λειτουργικές οντότητες:

- S-GW, η οποία χρησιμοποιείται για τη διαχείριση της κινητικότητας των χρηστών και τη διατήρηση των διαδρομών δεδομένων μεταξύ των eNB και της Πύλης Δικτύου Πακέτων Δεδομένων (Packet Data Network Gateway - P-GW), ενώ παράλληλα παρέχει διευκολύνσεις στη διασύνδεση με δίκτυα 2G και 3G.
- MME, που είναι οντότητα υπεύθυνη για τις λειτουργίες διαχείριση σύνδεσης και αυτές που σχετίζονται με τη διαχείριση του φορέα και ως εκ τούτου καθίσταται κρίσιμο δομικό στοιχείο ελέγχου στο LTE. Ελέγχει τη διαδικασία σηματοδότησης, διατήρησης καταστάσεων λειτουργίας και χρόνων αυτών, διαχείρισης ελέγχου ταυτότητας και κινητικότητας με το σύνολο των κόμβων. Αναλαμβάνει να παρακολουθεί τα UE σε κατάσταση αδράνειας, τις διαδικασίες σελιδοποίησης, την ενεργοποίηση και απενεργοποίηση του φορέα, αλλά και άλλες διαδικασίες που σχετίζονται με την πιστοποίηση ταυτότητας του χρήστη. Ένας MME μπορεί να συνδεθεί με ένα Κέντρο Εκπομπής Κυψέλης (Cell Broadcast Center- CBC), που χρησιμοποιείται για τη μετάδοση μηνυμάτων σε όλους τους χρήστες που είναι συνδεδεμένοι στο eNB, που με τη σειρά του είναι συνδεδεμένα σ‘ αυτό. Αυτό είναι

ένα βασικό χαρακτηριστικό που αναμένεται να χρησιμοποιηθεί σε μεγάλο βαθμό σε κρίσιμες εφαρμογές επικοινωνιών. Ο MME μπορεί επίσης να συνδεθεί με το Μητρώο Ταυτότητας Εξοπλισμού (Equipment Identity Register - EIR), μια βάση δεδομένων που περιέχει την κατάσταση των κινητών συσκευών που είναι καταχωρημένες στο δίκτυο και χρησιμοποιείται για τον έλεγχο ταυτότητας των UE.

- Πύλη δικτύου πακέτων δεδομένων (Packet Data Network Gateway - P-GW), λειτουργεί ως διεπαφή μεταξύ του δικτύου LTE και άλλων Πακέτων Δεδομένων Δικτύου (Packet Data Networks - PDNs) αποτελώντας το σημείο εισόδου και εξόδου για την κυκλοφορία των UE. Επιπλέον, εκτελεί υποστηρικτικές λειτουργίες που αφορούν στη φόρτιση των συσκευών και τη διασφάλιση της παροχής του προβλεπόμενου επιπέδου QoS, ενώ διασφαλίζει τη διαλειτουργικότητα μεταξύ τεχνολογιών που λειτουργούν με πρότυπα 3GPP και αυτών που δεν λειτουργούν μ' αυτά (π.χ. WiMAX και CDMA)
- Διακομιστής Συνδρομητών Οικίας (Home Subscriber Server - HSS) είναι μια κεντρική βάση που περιέχει δεδομένα συνδρομής χρηστών και περιλαμβάνει λειτουργίες που σχετίζονται με τη διαχείριση κινητικότητας, τον έλεγχο ταυτότητας του χρήστη, την πρόσβαση, τις εξουσιοδοτήσεις χρηστών και την ασφάλεια αυτών. Επίσης, διατηρεί δεδομένα σχετικά με τα PDNs στα οποία μπορεί να είναι εγγεγραμμένα τα UE.



CBC	Cell Broadcast Center
eNB	Enhanced Node B
DeNB	Donor eNB
EIR	Equipment Identity Register
EPC	Evolved Packet Core
E-UTRAN	Evolved UTRAN
GPRS	General Packet Radio Service
GSM	Global System Mobile
GW	Gateway
HeNB	Home eNB
HeNB-GW	Home eNB GW
HSS	Home Subscriber Server
MME	Mobility Management Entity
PCRF	Policy and Charging Rules Function
P-GW	Packet Data Network GW
RN	Relay Node
S-GW	Serving GW
SGSN	Serving GPRS Support Node
UMTS	Universal Mobile Telecomm. System
UTRAN	UMTS Terrestrial Radio Access Network

Εικόνα 23. LTE functional architecture [57]

- Λειτουργία Πολιτικής και Κανόνων Χρέωσης (Policy and Charging Rules Function - PCRF) περιλαμβάνει πληροφορίες που σχετίζονται με την πολιτική χρέωσης και την παροχή QoS στο P-GW, ενώ διαχειρίζεται τις συνεδρίες δεδομένων με βάση τα προφίλ των συνδρομητών.
- Πύλη HeNB (HeNB-GW) χρησιμοποιείται για τη συγκέντρωση και διαχείριση της κίνησης μιας μεγάλης ομάδα μικρών κυψελών (HeNBs) σε S-GW και για την απρόσκοπτη επικοινωνία για χρήστες καθώς μετακινούνται μέσα και έξω μεταξύ των κυψελών HeNB και eNB. Ζήτημα βέβαια στις περιπτώσεις αυτές αποτελεί το θέμα της ασφάλειας, καθώς ορισμένα από αυτά τα κελιά ενδέχεται να μην αποτελούν μέρος ενός αξιόπιστου δικτύου.
- Προσφορά υποστηρικτικών κόμβων GPRS (Serving GPRS support node - SGSN), καταχρηστικά απεικονίζεται στο EPS, καθώς δεν αποτελεί μέρος αυτού, αλλά διαχειρίζεται τη διασύνδεση του δικτύου LTE με το δίκτυο GPRS, μέσω του οποίου ανταλλάσσονται πακέτα σε δίκτυα 2G και 3G που βασίζονται σε πρότυπο GSM.

Άλλο βασικό συστατικό στην αρχιτεκτονική του δικτύου LTE, αποτελούν οι διεπαφές. Υπάρχουν, όπως αναφέρθηκε αρχικά και προκύπτει από την Εικόνα 22 και την Εικόνα 23, τέσσερεις βασικές κατηγορίες διεπαφών:

i. Διεπαφή αέρα (Air Interface). Η διεπαφή μεταξύ του UE και του eNB ονομάζεται επίσημα LTE Uu. Τα bits σ` αυτήν την ασύρματη διεπαφή μεταδίδονται μέσω κωδικοποιημένου, διαμορφωμένου, κρυπτογραφημένου ηλεκτρομαγνητικού σήματος στο φυσικό στρώμα. Τη διεκπεραίωση αυτής της μετάδοσης αναλαμβάνουν μια σειρά πρωτοκόλλων γνωστά ως πρωτόκολλα AS. Επίσης, υπάρχουν οι διεπαφές Un, μεταξύ RN και του DeNB του, ως παραλλαγή του Uu και η διεπαφή PC5 μεταξύ δύο UE. Η διεπαφή PC5 εισήχθη στην Release 12 και εμπλέκεται στην παρχοή υπηρεσιών εγγύτητα (Proximity-based Services, ProSe), μια ιδιαιτέρως σημαντική υπηρεσία του LTE, στην οποία θα αναφερθούμε ξεχωριστά, καθώς παρέχουν δυνατότητα απ‘ ευθείας επικοινωνίας μεταξύ των UE, άρα διασφαλίζει τη συνέχεια λειτουργίας σε περιπτώσεις καταστροφής της υποδομής.
ii. Διεπαφές E-UTRAN Network. Οι διεπαφές αυτές ορίζουν δύο μεγάλες κατηγορίες. Αυτές που χρησιμοποιούνται στη σύνδεση τελικών συσκευών και αυτές που χρησιμοποιούνται στη σύνδεση των eNB στα διακριτά στοιχεία του EPC. Βλέπουμε και στην Εικόνα 23 μια σειρά από διεπαφές και συγκεκριμένα:
    - X2, για τη σύνδεση των άκρων. Ομοιάζει με τη διεπαφή S-MME, με μόνη διαφορά να εντοπίζεται στο πρωτόκολλο του επιπέδου εφαρμογής.
    - S1, για τη σύνδεση των eNB σε διάφορα στοιχεία του δικτύου πυρήνα, με χρήση σχετικού αναγνωριστικού.

- S1-MME, για τη σύνδεση eNB και MME για τον έλεγχο και τη διαχείριση των επικοινωνιών.
- S1-U, για τη σύνδεση eNB και S-GW για τη διευκόλυνση των λειτουργιών επιπέδου χρήστη.

iii. Διεπαφή EPC. Είναι διεπαφές που χρησιμοποιούνται για την ανταλλαγή πληροφοριών χρήστη μεταξύ των στοιχείων του δικτύου κορμού (Core Network, CN) και περιλαμβάνουν:

- S5, για τη σύνδεση S-GW και P-GW (εντός του εσωτερικού του δικτύου LTE)
- S8, για τη σύνδεση επίσης μεταξύ S-GW και P-GW (για την περιαγωγή μεταξύ διαφορετικών δικτύων)
- S6a, για τη σύνδεση MME και HSS
- S9, μεταξύ του διαφορετικών ειδών PCRF
- S10, μεταξύ των MME
- S11, για τη σύνδεση του MME σε S-GW (ένα MME μπορεί να υποστηρίξει πολλά S-GWs)
- S13, συνδέει το MME για να ανταλλάξει πληροφορίες που χρησιμοποιούνται στο πλαίσιο του ελέγχου ταυτότητας των UE
- Gx, είναι η διεπαφή μεταξύ του P-GW και του PCRF
- SBc, η διεπαφή μεταξύ CBC και MME για την παράδοση προειδοποιητικών μηνυμάτων μετάδοσης και λειτουργίες ελέγχου

iv. Διεπαφές διασύνδεσης (Interworking Interfaces). Είναι διεπαφές που χρησιμοποιούνται για τη διευκόλυνση των επικοινωνιών μεταξύ των στοιχείων EPC και αυτών που ανήκουν σε εξωτερικά δίκτυα:

- S3, για διασυνεργασία με δίκτυα 2G και 3G GSM που βασίζονται σε GPRS (τυποποιημένα από 3GPP).
- S4, για διασυνεργασία μεταξύ ενός χρήστη LTE και ενός χρήστη που δεν είναι LTE
- SGi, για τη σύνδεση του P-GW σε ένα δίκτυο πακέτων δεδομένων, το οποίο θα μπορούσε να είναι εσωτερικού ή εξωτερικού χρήστη LTE.
- Rx, για τη σύνδεση του PCRF σε ένα δίκτυο πακέτων δεδομένων.
- S12, μεταξύ του P-GW και ενός δικτύου 3G

Το LTE αναπτύσσεται ευρέως ως παγκόσμιο πρότυπο ευρυζωνικής κινητής τηλεφωνίας. Η μεγάλης κλίμακας ανάπτυξή του δημιουργεί ένα τεχνολογικό οικοσύστημα που παρέχει στους χρήστες έναν λιγότερο ακριβό εξοπλισμό βασισμένο σε ενιαία πρότυπα, ικανά να υιοθετηθούν από το σύνολο των επαγγελματιών που εμπλέκονται με τη δημόσια ασφάλεια [64].

4.2.3 Βασικά τεχνικά χαρακτηριστικά του LTE

Τα κύρια τεχνικά χαρακτηριστικά της επίπεδης αρχιτεκτονικής, της χρήσης μεταγωγής πακέτων και του πρωτοκόλλου IP για την επικοινωνία του έδωσαν το προβάδισμα έναντι των υπολοίπων τεχνολογικών προτύπων, μέχρι τη δεδομένη στιγμή. Τα τεχνικά στοιχεία και επιδώσεις του προκύπτουν συγκεντρωτικά στον Πίνακας 3. Πλέον αυτού, θα επικεντρωθούμε σε δύο βασικές υπηρεσίες του LTE, τις Υπηρεσίες Εγγύτητας LTE (Proximity Services - ProSe) και Ομαδική Επικοινωνία μέσω LTE (Group Communication over LTE).

Οι ProSe επικοινωνίες οι οποίες είναι επίσης γνωστές ως υπηρεσίες επικοινωνίας συσκευή προς συσκευή (Device to Device - D2D), είναι ένας μηχανισμός με τον οποίο ένα UE ανακαλύπτει και επικοινωνεί με άλλα UE απ' ευθείας, δηλαδή χωρίς τη μεσολάβηση του δικτύου LTE. Η συγκεκριμένη επικοινωνία, για την οποία θα γίνει αναλυτική αναφορά στη συνέχεια, εξοικονομεί πόρους του δικτύου και καθιστά εφικτή την επικοινωνία, ακόμη και στις περιπτώσεις εκτός κάλυψης, ή όταν το δίκτυο έχει υποστεί ζημία και δεν είναι λειτουργικό [43].

Η Group Communication over LTE είναι μια υπηρεσία για την ταυτόχρονη χρήση διαφορετικών τύπων δεδομένων, μεταξύ πολλών χρηστών του συστήματος, δυνατότητα που καθίσταται μείζονος σημασίας για τις κρίσιμες επικοινωνίες και τα δίκτυα δημόσιας ασφάλειας [43]. Η υπηρεσία αυτή ανοίγει το δρόμο των πολύπλοκων και απαιτητικών εφαρμογών για τη δημόσια ασφάλεια στο δίκτυο LTE, όπως το Mission Critical Push-To-Talk (MCPTT) μέσω LTE. Η υπηρεσία αυτή στηρίζεται σε δύο βασικά στοιχεία της υποδομής του δικτύου:

- Στον ενεργοποιητή του συστήματος ομαδικής επικοινωνίας (Group Communication System Enabler - GCSE) που αναλαμβάνει την αποτελεσματική παράδοση φωνής, βίντεο ή δεδομένων μεταξύ μιας ομάδας των UE, καθώς και λειτουργίες διαχείρισης ομάδας, ήτοι επικοινωνιών παράλληλης σύνδεσης, μηχανισμούς προτεραιότητας και δημιουργία, αλλαγή ή διαγραφή ομάδας.
- Στη λειτουργία MCPTT, οι απαιτήσεις του οποίου ορίσθηκαν στην Release 13 [58].

4.2.4 Πλεονεκτήματα και μειονεκτήματα του LTE

Τα πλεονεκτήματα του LTE έχουν ήδη διαφανεί από τις τεχνολογικές του δυνατότητες, οι οποίες συνοψίζονται στ' ακόλουθα [43], [57], [58], [64], [65]:

- Υπηρεσίες (φωνή και δεδομένα) πολύ υψηλής χωρητικότητας
- Κινητή επικοινωνία με γρήγορη παράδοση μέσω του δικτύου
- Χαμηλή καθυστέρηση

- Εξαιρετική ανθεκτικότητα και ευελιξία (ομοιογενή και ετερογενή δίκτυα: macro, pico και femtocells)
- Ενσωματωμένη QoS
- Χαμηλή κατανάλωση ενέργειας
- Εξαιρετική απόδοση φάσματος (από 5 MHz έως 20 MHz)
- Ταχύτητα, που ξεπερνά το WiFi και είναι πολύ χαμηλότερη από το LMR.
- Επικοινωνίες μηχανή προς μηχανή σε πραγματικό χρόνο
- Υλοποίηση εφαρμογών με αισθητήρες και έξυπνους αυτοματισμούς
- Υπηρεσία μετάδοσης φωνής μέσω IP, υπηρεσίας Φωνής μέσω LTE (Voice over LTE - VoLTE) με εξαιρετικές δυνατότητες.

Αντίστοιχα, στα μειονεκτήματα θα μπορούσαμε, αντλώντας στοιχεία από τις ίδιες βιβλιογραφικές πηγές, να εντάξουμε:

- Για να επιτευχθεί η ίδια κάλυψη με το LMR απαιτούνται σημαντικά περισσότερες κεραίες, με ό,τι αυτό συνεπάγεται σε επίπεδο οικονομικού κόστους. Οπότε μπορεί να εκτιμηθεί ως εξαιρετικά ακριβό, συγκριτικά με το LMR , αλλά και το WiFi.
- Υφίστανται αντιληπτές διαφορές απόδοσης στο άκρο της κυψέλης, σε σχέση με την περιοχή δίπλα στην κεραία (πύργο), ενώ ταυτόχρονα, η κάλυψη είναι ιδιαιτέρως ευαίσθητη στο εύρος ζώνης και εξαρτάται από το πόσο φορτωμένο είναι το δίκτυο, κάθε στιγμή. Κάποιες δε από τις εφαρμογές δεν λειτουργούν σε οριακές συνθήκες και αυτό μπορεί να προκαλέσει σημαντικά προβλήματα λειτουργικότητας και ανταπόκρισης.
- Εντοπίζονται κάποια ζητήματα ασφάλειας, ειδικότερα σε επιθέσεις ενδιάμεσου (Man in the Middle).
- Δεν έχει δοκιμαστεί αρκετά και σε όλο το εύρος των εφαρμογών που παρέχει.

	LTE (Release 8)	LTE-A (Release 9 and Beyond)
Peak data rate—DL	• 300 Mbps (4 × 4 MIMO)	• 1 Gbps
Peak data rate—UL	• 75 Mbps (64 QAM)	• 500 Mbps in 15 bps/Hz
Peak spectral efficiency—DL	• 16.3 b/s/Hz (4 × 4 MIMO)	• 30 b/s/Hz (up to 8 × 8 MIMO)
Peak spectral efficiency—UL	• 4.32 b/s/Hz (64 QAM SISO)	• 15 b/s/Hz (up to 4 × 4 MIMO)
Cell range	• 5 km—optimal size • 30 km sizes with reasonable performance • Up to 100 km cell sizes supported with acceptable performance	
Cell capacity	• Up to 200 active users per cell (5 MHz) (i.e. 200 active data clients)	
Mobility	• Optimized for low mobility (0–15 km/h) but supports high speed	
Transmission bandwidth (MHz)	• ≤20	• ≤100
Radio access	• OFDMA for DL data transmission • SC-FDMA for UL transmission	• OFDMA for DL data transmission • SC-FDMA for UL transmission
Latency (delay)	• User plane <5 ms • Control plane <50 ms	• From idle to connected in less than 50 ms and then shorter than 5 ms one way for individual packet transmission
Channel bandwidth	• 1.4, 3, 5, 10, 15, 20	
Modulation types	• QPSK, 16 QAM, 64 QAM (UL and DL)	
Duplex schemes	• FDD and TDD	
Carrier aggregation	• No	• Yes (up to five of these "component carriers," each offering up to 20 MHz of bandwidth, can be combined, which creates a maximum aggregated data pipe up to 100 MHz)
MIMO	• Some (only for DL) four transmitters	• Yes (up to eight antenna pairs for the DL and up to four pairs for the UL)
Relay node	• Yes	• Yes—more advanced (first decode the transmissions and then forward only those destined for the mobile units that each relay is serving)
Coordinated multipoint	• Yes (ICIC)—optional	• Yes—eICIC
Device to device	• No	• Yes

Πίνακας 3. Κύρια τεχνολογικά χαρακτηριστικά του LTE

4.3 4G

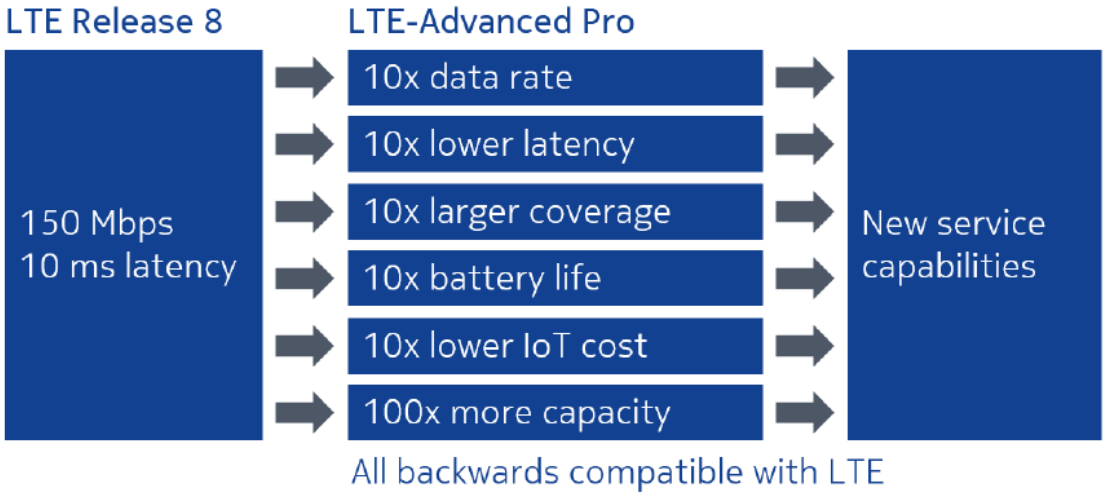
Η εξέλιξη του LTE φαίνεται μέσω των εκδόσεων που ακολούθησαν την πρώτη εμφάνισή του. Συγκεκριμένα, όπως προκύπτει από τον Πίνακας 4, από την έκδοση 8 και έπειτα καταγράφηκαν σημαντικές βελτιώσεις στο πρότυπο LTE [57].

Από την όγδοη έκδοση 8 (Release 8) έως την δέκατη τέταρτη (Release 14), οπότε και έχουμε το LTE Advanced Pro (LTE-A Pro), επιτεύχθηκαν σημαντικοί στόχοι, οι οποίοι συνοψίζονται εποπτικά στον Πίνακας 5 και αφορούν σε δεκαπλασιασμό του ρυθμού μετάδοσης δεδομένων, της καθυστέρησης διάδοσης, της περιοχής κάλυψης και της ενεργειακής απόδοσης. Παράλληλα υποδεκαπλασιάστηκε το κόστος της υποδομής και συσκευών και εκατονταπλασιάστηκε η χωρητικότητα.

Σύμφωνα με το [66] τρεις είναι οι βασικοί τομείς των PSNs επόμενης γενιάς: οι εφαρμογές, οι υποδομές και οι συσκευές. Στο πλαίσιο αυτό, αν οι επικοινωνίες στενής ζώνης δίνουν ένα σημαντικό εύρος εφαρμογών και υπηρεσιών, οι ευρυζωνικές επικοινωνίες μπορούν να οδηγήσουν τα πράγματα ακόμη πιο αποδοτικά και σε κάθε περίπτωση στο επιθυμητό και τεχνολογικά εφικτό σημείο.

Version	Released	Info
Release 8	March 2009	First LTE release
Release 9	March 2010	LTE Enhancements
Release 10	Sept. 2011	LTE Advanced
Release 11	March 2013	LTE-A Enhancements
Release 12	March 2015	LTE-A Enhancements
Release 13	March 2016	Critical communication+other enhancement
Release 14	June 2017	LTE-A Pro

Πίνακας 4. 3GPP Releases σχετικά με το LTE [57]



Πίνακας 5. Δυνατότητες LTE-Advanced [67]

Χαρακτηριστικά παραδείγματα αναφέρονται αναλυτικά στο [66] και συνοπτικά ως ακολούθως:

- Ένα ερώτημα βάσης δεδομένων περιέχει πλήθος πληροφοριών (μακροσκελή κείμενα, φωτογραφίες, βίντεο), αντί μιας μικρής παραγράφου και μεταδίδεται σε δευτερόλεπτα, αντί 3 έως 10 λεπτών.
- Οι αστυνομικοί έχουν πρόσβαση σε πληροφορίες (χάρτες, σχέδια κτηρίων, βίντεο, κ.λπ.) που είτε προσεγγίζοντας ένα περιστατικό, είτε διερευνώντας μια υπόθεση, κάνουν τη δουλειά τους πιο ασφαλή και αποδοτική.
- Σε πολύ λίγο και υπερπολύτιμο χρόνο η φωτογραφία ενός εξαφανισμένου παιδιού, ή ενός καταζητούμενου δράστη μπορεί να φτάσει σε τόσους πολλούς και από διαφορετικές υπηρεσίες αποδέκτες, που πολλαπλασιάζει τις πιθανότητες επιτυχούς ανεύρεσης ή σύλληψης, αντίστοιχα.
- Η πληροφορία ότι έλαβε χώρα ένα ατύχημα μπορεί να φτάσει ταχύτατα από κάμερες παρακολούθησης και έτσι να ενεργοποιηθεί ο μηχανισμός ανταπόκρισης των υπηρεσιών πολύ πιο γρήγορα και σαφέστατα με μεγαλύτερη ετοιμότητα ως προς τις συνθήκες που επίκειται να συναντήσει (π.χ. σε περίπτωση ατυχήματος με επικίνδυνα υλικά, σε περιπτώσεις που απαιτείται εκκένωση του χώρου κ.λπ.).
- Ομοίως, η ανταπόκριση του κρατικού μηχανισμού σε περιπτώσεις μεγάλων καταστροφών από φυσικά ή ανθρωπογενή αίτια, μπορεί να βοηθηθεί σημαντικά από δυναμικούς χάρτες, εφαρμογές καιρού ή ροής κυκλοφορίας.
- Οι παρεχόμενες υπηρεσίες δημόσιας ασφάλειας που σχετίζονται με την οδική ασφάλεια, την εγκληματικότητα, τη λιμενική και πυροσβεστική επιτήρηση θαλάσσιων και δασικών περιοχών αντίστοιχα, μπορούν να βοηθηθούν σημαντικότατα.
- Οι εργασίες σε κρίσιμες υποδομές μπορούν να γίνουν αποδοτικότερες, καθώς λιγότερο προσωπικό μπορεί ν` απασχοληθεί λιγότερες εργατοώρες και να φέρει τα ίδια ή και καλύτερα αποτελέσματα.

Σε κάθε περίπτωση, το 4G θεωρείται μια καλή βάση για να υποστηρίξει επικοινωνιακά εφαρμογές δημόσιας ασφάλειας, για όλους τους λόγους που διεξοδικά αναλύθηκαν ήδη, αλλά κυρίως για το γεγονός ότι ικανοποιεί αυστηρά τις απαιτήσεις QoS, ανθεκτικότητας και ασφάλειας των PSN. Παράλληλα, παρέχει τη δυνατότητα να ενοποιηθούν αποδοτικά τα παλαιότερης τεχνολογίας PSN (TETRA, P25, VHF, UHF), με την αρχιτεκτονική στην Εικόνα 24 [51].

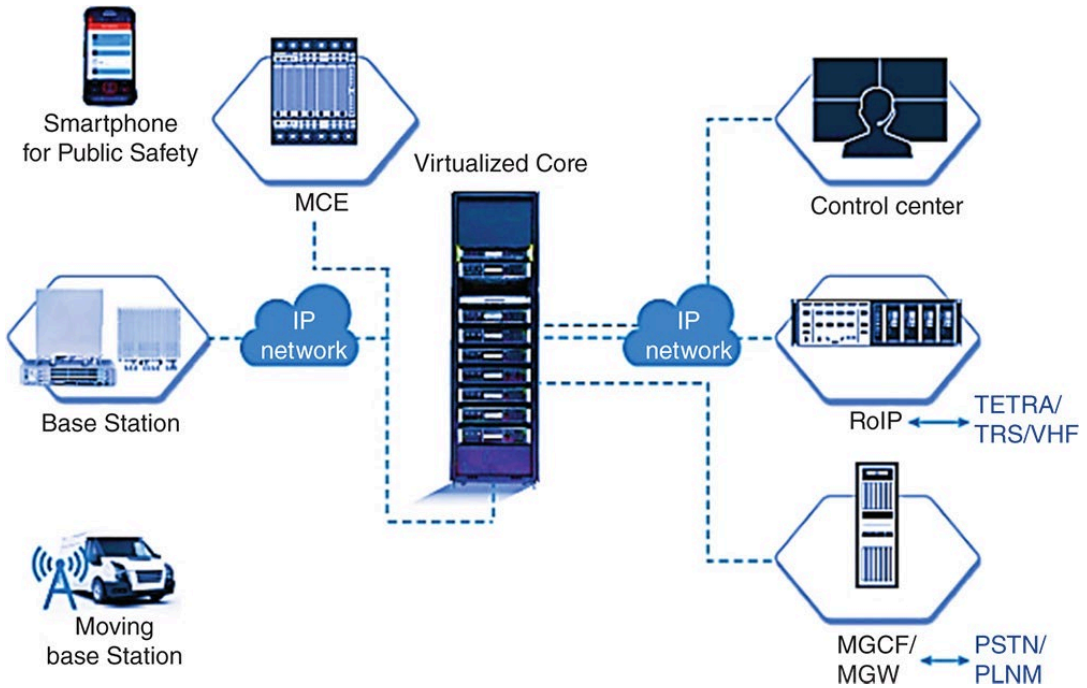
Τεχνολογικά το 4G οφείλει τις αυξημένες δυνατότητες λήψης και μετάδοσης έναντι του 3G, στην τεχνολογία MIMO και Πολυπλεξία Ορθογωνικής Διαίρεσης Συχνότητας (Orthogonal Frequency Division Multiplexing - OFDM). Τόσο το MIMO όσο και το OFDM επιτρέπουν

μεγαλύτερη χωρητικότητα και εύρος ζώνης, ενώ το OFDM παρέχει μεγαλύτερη ταχύτητα από τις κύριες τεχνολογίες που τροφοδοτούν το 3G, οι οποίες περιλαμβάνουν την τεχνολογία Πολλαπλή Πρόσβαση Διαίρεσης Χρόνου (Time Division Multiple Access - TDMA) και Πολλαπλή Πρόσβαση Διαίρεσης Κώδικα (Code Division Multiple Access - CDMA). Με το MIMO, το 4G μειώνει τη συμφόρηση δικτύου σε σύγκριση με το 3G, επειδή μπορούν να υποστηριχθούν περισσότεροι χρήστες [68]. Επιπλέον, το πρότυπο 4G βασίζεται αποκλειστικά σε IP (πρωτόκολλο Διαδικτύου) τόσο για τη μετάδοση φωνής, όσο και για τη μετάδοση δεδομένων. Η σαφής διαφορά με το 3G, είναι ότι αυτό χρησιμοποιεί IP μόνο για μετάδοση δεδομένων και επιτρέπει τη φωνή με δίκτυο μεταγωγής κυκλώματος.

Αναλυτικά στοιχεία απόδοσης, συγκριτικά με τις άλλες γενιές κινητής επικοινωνίας παρουσιάζονται στον Πίνακας 6.

Η εξέλιξη των δικτύων κινητής επικοινωνίας	**1G**	**2G**	**3G**	**4G**	**5G**
Δεκαετία εμφάνισης	1980	1990	2000	2010	2020
Ταχύτητα	2Kbps	384Kbps	56Mbps	1Gbps	10Gbps
Καθυστέρηση	-	629ms	212ms	60-98ms	<1ms

Πίνακας 6. Συγκριτικά στοιχεία των διαφορετικών γενιών δικτύων κινητής τηλεφωνίας [66]



Εικόνα 24. 4G LTE ενοποίηση διαφορετικών τεχνολογικών προτύπων σε PSN [51]

4.4 5G

Η «Πέμπτη γενιά» τηλεπικοινωνιακών συστημάτων, γνωστή ως «5G», βρίσκεται ήδη στην επόμενη της φάση, την «5G-Advanced» Έκδοση 18 (Release 18), προσθέτοντας συνεχώς νέες δυνατότητες και βελτιώνοντας τα χαρακτηριστικά της. Με την ενσωμάτωση των MCX χαρακτηριστικών της 17ης έκδοσης (Release 17) του 3GPP εξασφαλίστηκαν και όλες οι ζητούμενες προδιαγραφές των οργανισμών δημόσιας ασφάλειας. Άλλωστε το γεγονός πως οι ΗΠΑ με το FirstNet, η Φινλανδία με το Vivre 2.0 αλλά και το Ηνωμένο Βασίλειο με το Δίκτυο Υπηρεσιών Έκτακτης ανάγκης (Emergency Service Network - ESN) [69] έχουν ήδη ξεκινήσει τις διαδικασίες μετάβασης προς το 5G, οδηγούν ουσιαστικά τις εξελίξεις για τα επόμενης γενιάς ασύρματα δημόσια δίκτυα ασφαλείας. Μια συνολική εποπτική αποτύπωση των Χωρών που έχουν αναπτύξει, αναπτύσσουν ή επενδύουν σε δίκτυα πέμπτης γενιάς παρουσιάζεται στην Εικόνα 25.

Τα τελευταία χαρακτηριστικά της πέμπτης γενιάς που προτυποποιήθηκαν (Έκδοση 17), καλύπτουν όλες τις απαιτούμενες προδιαγραφές που ενδελεχώς παρουσιάσαμε στο δεύτερο κεφάλαιο με τίτλο: «Απαιτήσεις στις επικοινωνίες δημόσιας ασφάλειας». Συγκεκριμένα το σύστημα είναι πιο στιβαρό και αξιόπιστο, διαθέτει βελτιωμένη ασφάλεια, υψηλότερο ρυθμό μετάδοσης δεδομένων, χαμηλή καθυστέρηση και εξασφαλίζει τόσο την διαθεσιμότητα όσο και την διαλειτουργικότητα ανάμεσα στους πρώτους ανταποκριτές διαφορετικών οργανισμών και υπηρεσιών καθιστώντας το εξίσου αξιόπιστο με τα παλαιότερα δίκτυα στενής ζώνης όπως το TETRA.

Εικόνα 25. Χάρτης ανάπτυξης εμπορικών δικτύων 5G [70]

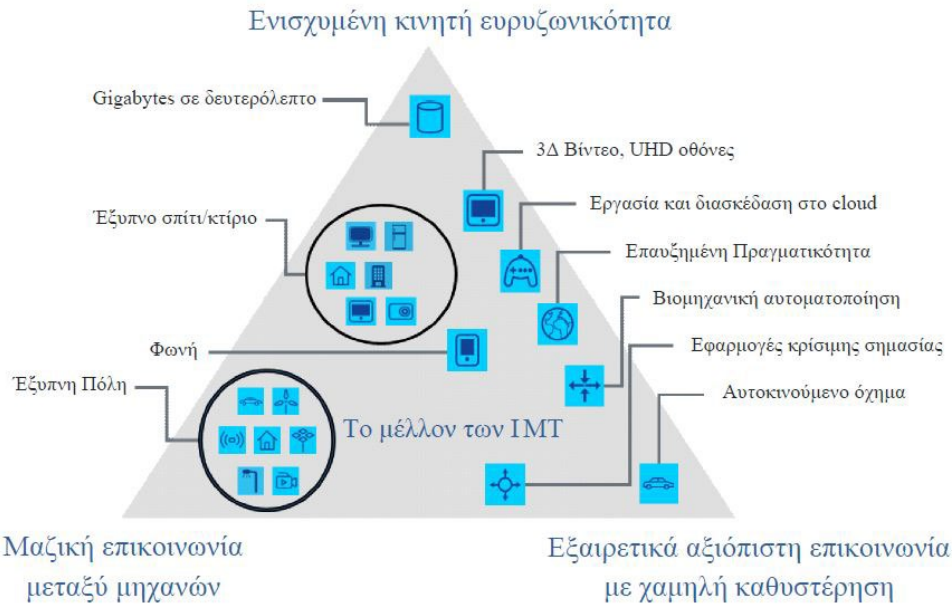
Παρακάτω θα εξηγήσουμε αναλυτικά τους λόγους για τους οποίους σήμερα οι πέμπτης γενιάς τεχνολογίες επικοινωνίας του 3GPP βρίσκονται στην πιο ώριμη φάση τους και αποτελούν το μέλλον στα επόμενης γενιάς δίκτυα δημόσιας ασφαλείας.

4.4.1 Κύρια χαρακτηριστικά του 5G

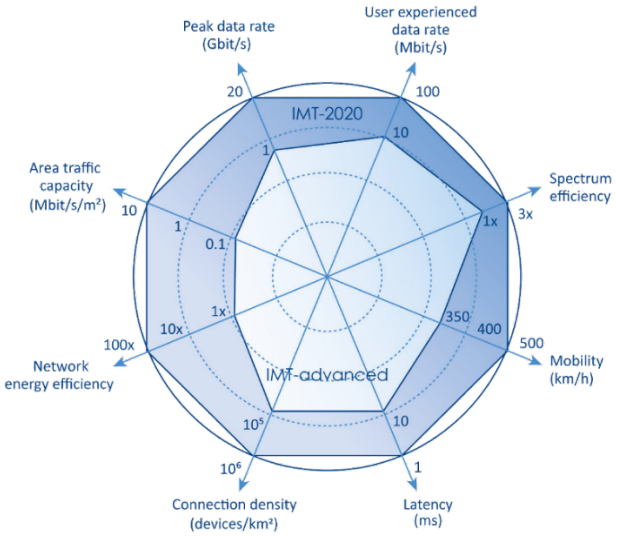
Τα κύρια χρακτηριστικά του 5G συνοψίζονται στις ακόλουθες κατηγορίες, οι οποίες ακολούθως αναλύονται διεξοδικά:

4.4.2 Ενισχυμένη Κινητή Ευρυζωνικότητα

Το 5G μπορεί να προσφέρει υψηλό εύρος ζώνης και ταχύτητες ικανές να υποστηρίξουν τόσο την αμφίδρομη μεταφορά βίντεο υψηλής ευκρίνειας όσο και μεγάλου όγκου δεδομένων. Η Ενισχυμένη Κινητή Ευρυζωνικότητα (Enhanced Mobile Broadband – eMBB) είναι θεμελιώδης για τη λειτουργία εφαρμογών όπως η Διευρυμένη Πραγματικότητα (Extended Reality – XR), που απαιτεί αμφίδρομη μεταφορά δεδομένων μεγάλου όγκου δημιουργώντας νέους τρόπους αλληλεπίδρασης μεταξύ των χρηστών. Η Όραση των υπολογιστών (Computer Vision - CV) και η μηχανική μάθηση (Machine Learning - ML) τεχνολογίες που συναντώνται σε πλήθος εφαρμογών στον τομέα της δημόσιας ασφάλειας και της προστασίας του πολίτη προϋποθέτουν την ύπαρξη της eMBB. Άλλωστε αυτές οι τεχνολογίες μαζί με το Απτικό Διαδίκτυο (Tactile Internet -TI) [71]) προσφέρουν σημαντικές λύσεις στη δημιουργία ρεαλιστικών εκπαιδευτικών σεναρίων στους οργανισμούς PS, μειώνοντας έτσι το κόστος εκπαίδευσης του προσωπικού αυξάνοντας παράλληλα τη συμμετοχή.



Εικόνα 26. Το όραμα του ITU για το 5G. ITU-R M.2083 [72]



Εικόνα 27. Προδιαγραφές της Διεθνούς Κινητής Τηλεπικοινωνίας (International Mobile Telecommunications IMT-2020) γνωστές και ως 5G [73]

Επίσης για πρώτη φορά παρέχεται η δυνατότητα υλοποίησης σεναρίων ανέφικτων να πραγματοποιηθούν σε φυσιολογικές συνθήκες όπως η εξομοίωση μεγάλων καταστροφών, σεισμοί – πλημμύρες κ.λπ..

4.4.2.1 Μαζικό Διαδίκτυο των Πραγμάτων (massive IoT - mIoT)

Το 5G μπορεί να παρέχει ταυτόχρονη συνδεσιμότητα σε έως ένα εκατομμύριο συνδέσεις ανά τετραγωνικό χιλιόμετρο. Αυτή η πυκνή συνδεσιμότητα είναι απαραίτητη για την αποτελεσματική λειτουργία προηγμένων εφαρμογών του IoT στη Βιομηχανία (Industrial Internet of Things -IIoT).Για παράδειγμα η συλλογή τεράστιων όγκων δεδομένων από εκτεταμένα δίκτυα αισθητήρων, που χρησιμοποιεί η τεχνητή νοημοσύνη σε έξυπνους σταθμούς ηλεκτροπαραγωγής αποσκοπώντας στη βελτίωση της αποδοτικότητας τους.

4.4.2.2 Υπηρεσίες Κρίσιμης Αποστολής (Mission Critical Services - MCS)

Για εφαρμογές κρίσιμης αποστολής, όπως αυτόνομα οχήματα ή απομακρυσμένες μονάδες εντατικής θεραπείας (ΜΕΘ), η αξιοπιστία και η ταχύτητα της σύνδεσης είναι ζωτικής σημασίας. Το 5G μπορεί να μεταφέρει μεγάλο όγκο δεδομένων με καθυστέρηση μικρότερη του 1ms, υποστηρίζοντας με ασφάλεια περιπτώσεις, στις οποίες ένα κλάσμα του δευτερολέπτου μπορεί να κάνει τη διαφορά μεταξύ ζωής και θανάτου.

4.4.2.3 Φάσμα και συχνότητες λειτουργίας του 5G

Ο σχεδιασμός ενός δικτύου με τα παραπάνω χαρακτηριστικά, ικανά να υποστηρίξει εφαρμογές υψηλών απαιτήσεων αποτελεί μια πολύπλοκη διαδικασία. Με δεδομένο πως για αντικειμενικούς λόγους δεν υφίσταται μια προσέγγιση ικανή να καλύψει όλες τις ανάγκες

όπως για παράδειγμα την μεταφορά πολύ μεγάλου όγκου δεδομένων, την κάλυψη μεγάλων αποστάσεων, ή τον συνδυασμό των παραπάνω, ως συνέπεια αυτού, οι ομάδες εργασίας του 3GPP οδηγήθηκαν στη επιλογή τριών ζωνών στο φάσμα συχνοτήτων για την επίτευξη των παραπάνω απαιτήσεων.

Οι συχνότητες λειτουργίας [74] του 5G ξεκινούν από την χαμηλή ζώνη κάτω του 2GHz και φτάνει έως τις εξαιρετικά υψηλές συχνότητες γνωστές ως «χιλιοστομετρικά κύματα» (mmWave). Η φασματική αυτή ευελιξία εξασφαλίζει τόσο τις μεταδόσεις σε μακρινές αποστάσεις με χρήση των χαμηλών συχνοτήτων όσο και τις μεταδόσεις μεγάλου όγκου δεδομένων με την χρήση των υψηλών συχνοτήτων. Συγκεκριμένα οι τρεις ζώνες συχνοτήτων των δικτύων 5G είναι:

α. Η υψηλή ζώνη (mmWave) παρέχει τις υψηλότερες συχνότητες του 5G και συγκεκριμένα από 24 GHz έως περίπου 100 GHz. Το 5G υψηλής ζώνης θεωρείται εκ φύσεως μικρής εμβέλειας, καθώς οι υψηλές συχνότητες είναι δύσκολο να διαδοθούν μέσα από εμπόδια. Επιπλέον, η κάλυψη στη χιλιοστομετρική ζώνη είναι περιορισμένη και απαιτεί περισσότερες κυψελοειδείς υποδομές.

β. Η μεσαία ζώνη λειτουργεί στην περιοχή 2-6 GHz και διαθέτει χωρητικότητα κατάλληλη για αστικές και προαστιακές περιοχές με ρυθμούς μετάδοσης της τάξης εκατοντάδων Mbps.

γ. Η χαμηλή ζώνη λειτουργεί κάτω από τα 2 GHz και παρέχει ευρεία κάλυψη. Άλλωστε τμήμα αυτής της ζώνης χρησιμοποιείται σήμερα από το 4G LTE. Κατά συνέπεια και οι επιδόσεις είναι αντίστοιχες.

4.4.2.4 Αρχιτεκτονική Δικτύου 5G

Η επικοινωνίες 5ης γενιάς σχεδιάστηκαν για να ενσωματώσουν ένα πλήθος εν μέρει αντιφατικών απαιτήσεων και προϋποθέσεων. Έτσι τεχνολογίες όπως η ιδεατοποίηση λειτουργιών δικτύου (Network Function Virtualization - NVF) και η καθορισμένη από λειτουργικό δικτύωση (Software-Defined Networking - SDN) αναπτύχθηκαν με στόχο να εξασφαλίσουν την απαιτούμενη ευελιξία των μελλοντικών δικτύων και κυρίως του δικτύου πυρήνα.

4.4.2.5 Ιδεατοποίηση Λειτουργίας Δικτύου (Network Function Virtualization - NVF)

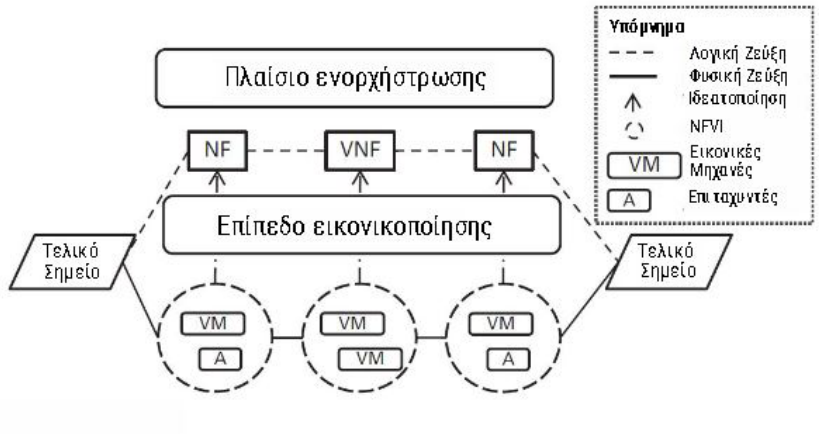
Η NVF χρησιμοποιεί διαδικασίες λογισμικού με τις οποίες αντικαθιστά υπηρεσίες που παρέχονται από υλισμικό του δικτύου.

- Ο έλεγχος αυτών των διαδικασιών πραγματοποιείται από έναν επόπτη (hypervisor), ένα πλαίσιο ενορχήστρωσης (Σχ. 3) που ελέγχεται μέσω λογισμικού το οποίο καθορίζει και την δικτύωση (SDN).

- Με την NVF εξασφαλίζεται η μείωση των κεφαλαιακών και λειτουργικών δαπανών (Capital Expenses – CAPEX, Operational Expenses – OPEX) και επιταχύνεται η ανάπτυξη των δικτύων.
- Η συγκεκριμένη λειτουργία αποτέλεσε απαίτηση των τηλεπικοινωνιακών παρόχων που επιθυμούσαν να λειτουργούν απομακρυσμένα κέντρα δεδομένων (data centers) με στόχο τον αποδοτικότερο έλεγχο και την βελτίωση λειτουργίας των δικτύων τους.

Στην Εικόνα 29 βλέπουμε τα τμήματα από τα οποία αποτελείτε το πλαίσιο και τα οποία είναι: Εικονικές Μηχανές (Virtual Machines – VM) οι οποίες βρίσκονται στο κάτω τμήμα του πλαισίου. Το επίπεδο εικονικοποίησης το οποίο χρησιμοποιεί τις VM για την εκτέλεση των διαφορετικών λειτουργιών του δικτύου (Network Function – NF).Το υλισμικό του δικτύου το οποίο βρίσκεται κάτω από τις VM. Τους επιταχυντές (Accelerators – A) που εξασφαλίζουν την απαραίτητη υπολογιστική ισχύ για τις κρίσιμες λειτουργίες οι οποίες απαιτούν εξαιρετικά μικρούς χρόνους καθυστέρησης, και δεν είναι εφικτό να υποστηριχθούν αποτελεσματικά από την Ιδεατοποιημένη υποδομή.

Εικόνα 28. Οι ζώνες συχνοτήτων του 5G [74]



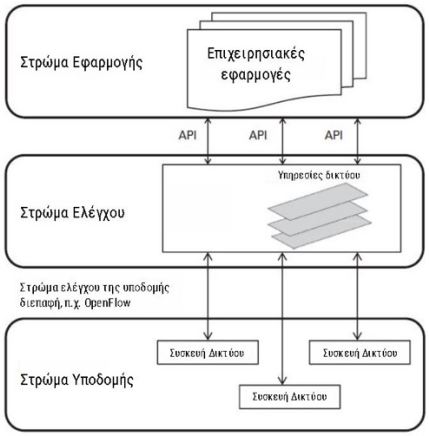
Εικόνα 29. NVF πλαίσιο [75]

4.4.2.6 Δικτύωση καθορισμένη με λογισμικό (SDN)

Οι κύριες λειτουργίες της SDN (Εικόνα 30) είναι:

- Να διαχωρίζει τις διαδικασίες ελέγχου (control) του δικτύου και των δεδομένων του χρήστη (data / user)
- Να ασκεί τον κεντρικό έλεγχο
- Να κάνει χρήση της αφαιρετικότητας (abstraction) του φυσικού εξοπλισμού από τις υπηρεσίες.
- Να επιτυγχάνει την αυτοματοποιημένη και προγραμματιζόμενη διαμόρφωση των στοιχείων δικτύου (infrastructure)

Αυτές οι δυο ανεξάρτητες διεργασίες, η NVF και η SDN έχουν τη δυνατότητα να λειτουργούν μεμονωμένα αλλά και συνδυαστικά, βελτιώνοντας με αυτόν τον τρόπο την αποδοτικότητα του συστήματος. Στον τομέα των PSN αυτή τεχνολογία έχει δοκιμαστεί με επιτυχία στο έργο SoftPSN [76] εξασφαλίζοντας την προτεραιότητα των κλήσεων των πρώτων ανταποκριτών την αξιοπιστία και την πολύ μικρή καθυστέρηση του συστήματος. Απέδειξε επίσης την ευκολία επανεγκατάστασης τομών στα μελλοντικά κυψελωτά δίκτυα γεγονός που μειώνει σημαντικά τόσο κεφαλαιακά όσο και τα λειτουργικά έξοδα των παρόχων.



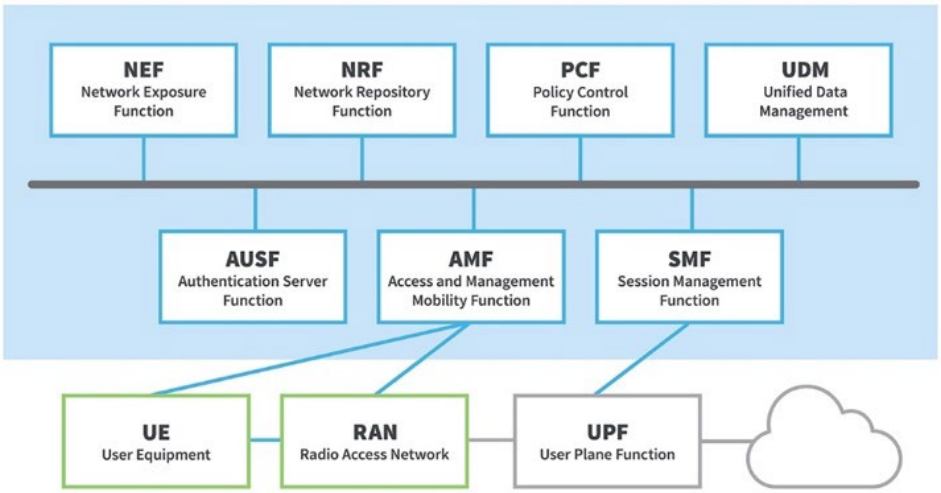
Εικόνα 30. Αρχιτεκτονική SDN [75]

4.4.2.7 Δίκτυο Πυρήνα

Ο πυρήνας του 5G σχεδιάστηκε από την αρχή με μια νέα φιλοσοφία ώστε οι λειτουργίες του δικτύου να μπορούν να τμηματοποιούνται ανά υπηρεσία. Αυτός είναι και ο λόγος για τον οποίο ονομάστηκε Αρχιτεκτονική Βασισμένη σε Υπηρεσίες (Service-Based Architecture – SBA). Στη νέα αυτή αρχιτεκτονική του πυρήνα (Εικόνα 31) διακρίνουμε:

- Εξοπλισμός Χρήστη (UE): Συσκευές όπως τα 5ης γενιάς κινητά και tablet έχουν τη δυνατότητα να συνδεθούν μέσω του Ραδιοδικτύου πρόσβασης (Radio Access Network – RAN) στον πυρήνα αρχικά, πριν τελικά αποκτήσουν πρόσβαση στο εξωτερικό Δίκτυο δεδομένων (Data Network – DN), πχ. διαδίκτυο.

- Τη Λειτουργία Διαχείρισης Πρόσβασης και Κινητικότητας (Access and Mobility Management Function – AMF). Η υπηρεσία αυτή λειτουργεί ως ενιαίο σημείο εισόδου πρόσβασης του UE. Είναι υπεύθυνη για τη διαχείριση εγγραφής (registration mgmt), διαχείριση προσιτότητας (reachability mgmt),υποστήριξη διαδικασιών πιστοποίησης αυθεντικότητας (authentication), ασφάλειας (security), σύνδεσης (connection mgmt). Με βάση την υπηρεσία που απαιτεί ο UE, η AMF επιλέγει την αντίστοιχη λειτουργία διαχείρισης συνεδρίας (Session Management Function – SMF). Η SMF αναλαμβάνει τη διαχείριση (εγκατάσταση, τροποποίηση, τερματισμό) των sessions, την εκχώρηση και διαχείριση διευθύνσεων IP στον UE, την διαχείριση και τον έλεγχο της κίνησης (User Plane – UP) καθώς και την λειτουργία επιπέδου χρήστη (User Plane Function – UPF), επίσης αναλαμβάνει και την συλλογή των δεδομένων χρέωσης.
- Η Λειτουργία επιπέδου χρήστη (User Plane Function – UPF) μεταφέρει τα IP δεδομένα (επίπεδο χρήστη) ανάμεσα στον εξοπλισμό του χρήστη και τα εξωτερικά δίκτυα. Εκτός από το ότι αποτελεί σημείο διασύνδεσης με εξωτερικά δίκτυα, ασχολείται επίσης με την δρομολόγηση και προώθηση πακέτων καθώς επίσης και με την διαχείριση QoS για το UP.
- Η Λειτουργία Πολιτικής Ελέγχου (Policy Control Function – PCF) Διαχειρίζεται την πολιτική των απαιτήσεων του QoS και των ροών της κίνησης από διαφορετικές υπηρεσίες ελέγχοντας ταυτόχρονα και τις πολιτικές χρεώσεων.
- Η Ενοποιημένη διαχείριση δεδομένων (Unified Data Management – UDM) αναλαμβάνει τη Δημιουργία των πιστοποιητικών της διαδικασίας πιστοποίησης αυθεντικότητας, την εξουσιοδότηση πρόσβασης των UE βάσει της συνδρομής, την διαχείριση των συνδρομών, τις χρεώσεις, καθώς επίσης και την αποθήκευση των AMF και SMF που εξυπηρετούν τους κινητούς σταθμούς.
- Η Λειτουργία Πιστοποίησης Αυθεντικότητας (Authentication Server Function – AUSF). Υποστηρίζει τη διαδικασία πιστοποίησης της αυθεντικότητας .
- Η Λειτουργία Εφαρμογής (Application Function – AF) Υποστηρίζει τις διαδικασίες που σχετίζονται με τις εφαρμογές όπως: η επίδραση των εφαρμογών στη δρομολόγηση της κίνησης, ή η συνεργασία με την PCF.
- Η Λειτουργία επιλογής τμηματοποίησης δικτύου (Network Slice Selection Function – NSSF), Πραγματοποιεί επιλογή των τμημάτων (slices) που εξυπηρετούν τον UE, καθορίζουν τις επιτρεπόμενες βοηθητικές πληροφορίες για την επιλογή του τμήματος δικτύου (Network Selection Assistance Information - NSAI) και του συνόλου των AME που εξυπηρετούν τον UE.



Εικόνα 31. Αρχιτεκτονική Πυρήνα Δικτύου 5G [75]

4.4.2.8 Δίκτυο Ραδιοπρόσβασης Επόμενης Γενιάς

Το Δίκτυο Ραδιοπρόσβασης Επόμενης Γενιάς (Next Generation Radio Access Network–NG-RAN) εξασφαλίζει την αμφίδρομη επικοινωνία των κινητών συσκευών με το κεντρικό δίκτυο 5G. Η νέα αυτή αρχιτεκτονική παρουσιάζει σημαντικά πλεονεκτήματα όπως ευελιξία, αποδοτικότητα, ενώ πλέον μπορεί να υποστηρίξει και ένα πλήθος νέων περιπτώσεων χρήσης και υπηρεσιών σε σύγκριση με την παραδοσιακή αρχιτεκτονική RAN.

Αποτελείται από δυο τμήματα: (α)το κεντροποιημένο και (β)το κατανεμημένο τμήμα [77], επιτυγχάνοντας έτσι οι λειτουργίες του δικτύου να εκτελούνται σε διαφορετικές τοποθεσίες. Το κεντροποιημένο τμήμα της αρχιτεκτονικής βρίσκεται στο κέντρο δεδομένων (Data Center – DC) και αποτελείται από την κεντρική μονάδα (Central Unit-CU) και την κατανεμημένη μονάδα (Distributed Unit - DU). Η DU βρίσκεται στο σταθμό βάσης και είναι υπεύθυνη για την εκτέλεση λειτουργιών που σχετίζονται με τις ραδιοεπικοινωνίες, όπως η διαμόρφωση δέσμης και η διαχείριση παρεμβολών. Η CU είναι υπεύθυνη για την εκτέλεση των λειτουργιών ελέγχου και διαχείρισης του δικτύου.

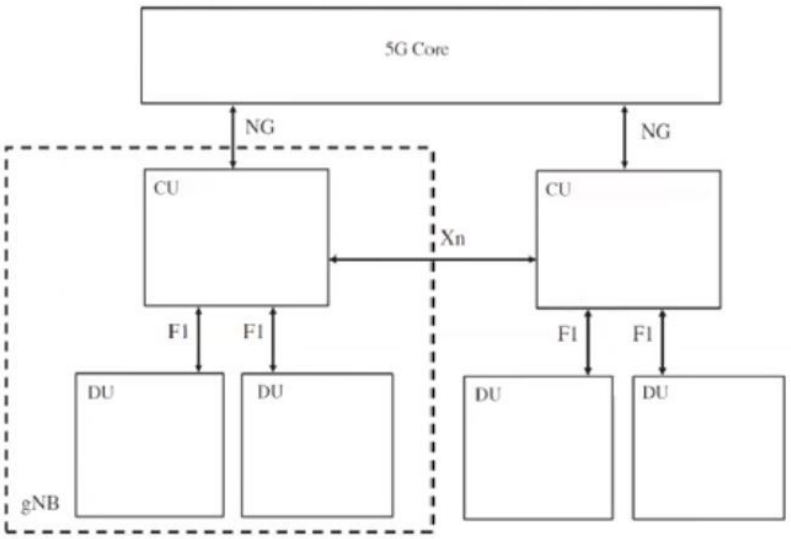
Αξιοποιώντας την NVF, η οποία επιτρέπει τη διαφορετική διαχείριση πολλαπλών ροών κίνησης, εξασφαλίζοντας χαμηλή καθυστέρηση για εφαρμογές πραγματικού χρόνου και μεγαλύτερη ευρυζωνικότητα για ροές βίντεο, αρκετές χώρες όπως το Βέλγιο και η Φινλανδία ανέπτυξαν τον δικό τους κορμό και αξιοποίησαν το ραδιοδίκτυο των παρόχων κινητής τηλεφωνίας για να καλύψουν τις τηλεπικοινωνιακές ανάγκες των υπηρεσιών δημόσιας ασφάλειας.

Ένα επίσης σημαντικό χαρακτηριστικό της νέας αρχιτεκτονικής είναι η χρήση της Υπολογιστικής Άκρων (Edge Computing – EC). Η EC επιτρέπει την εκτέλεση των λειτουργιών του δικτύου πιο κοντά στον χρήστη, μειώνοντας την καθυστέρηση και βελτιώνοντας τις επιδόσεις. Με την αποκέντρωση των λειτουργιών του δικτύου και τη μετακίνησή τους πιο κοντά στον χρήστη, εξασφαλίζεται η βελτίωση των επιδόσεων σε

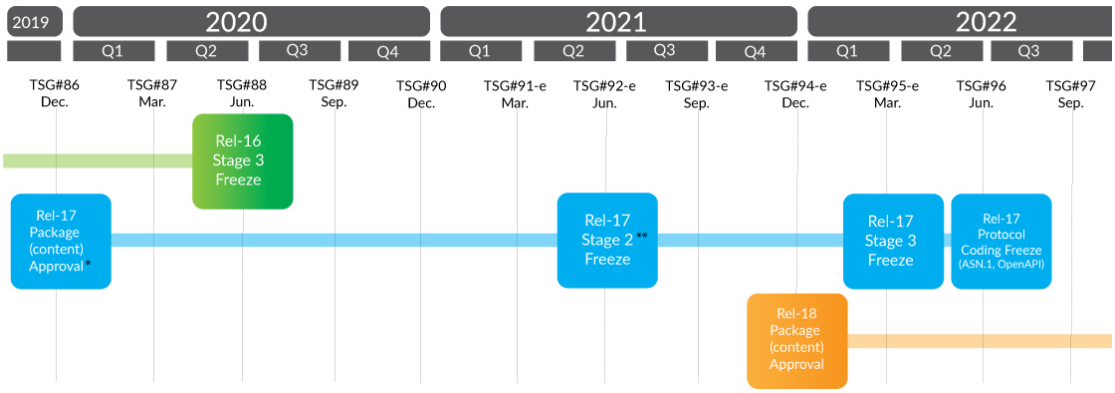
εφαρμογές πραγματικού χρόνου ενώ επιτρέπει και νέες περιπτώσεις χρήσης, όπως το IoT και τα ασύρματα δίκτυα αισθητήρων.

Εν κατακλείδι, το NG-RAN αποτελεί ένα ευέλικτο, κλιμακούμενο και αξιόπιστο δίκτυο ραδιοπρόσβασης. Με την χρήση προηγμένων τεχνικών, την υποστήριξη πολλαπλών ζωνών συχνοτήτων, την τμηματοποίηση του δικτύου και την υπολογιστική άκρων το καθιστούν απαραίτητο δομικό συστατικό της Πέμπτης γενιάς ραδιοεπικοινωνιών.

Οι δυο πιο σημαντικές προσθήκες της 17ης έκδοσης (Release 17) είναι η δυνατότητα απευθείας επικοινωνίας με μη επίγεια δίκτυα (Non-Terrestrial Networks - NTN) καθώς και η δυνατότητα αξιοποίησης μιας ελαφρύτερης έκδοσης για εφαρμογές του IoT. Η πρώτη σημαντική προσθήκη, εξασφαλίζει για πρώτη φορά στον τελικό χρήστη πρόσβαση με την τελική του συσκευή, σε μη επίγεια δίκτυα, γεγονός που επεκτείνει την κάλυψη της επικοινωνίας σε περιοχές χωρίς τηλεπικοινωνιακές υποδομές. Αντίστοιχα η δεύτερη προσθήκη εξασφαλίζει την διαχείριση και την επικοινωνία όλων των δικτύων αισθητήρων με αξιοπιστία και χαμηλή κατανάλωση. Στοιχεία που μπορούν να αξιοποιηθούν στην ανάπτυξη νέων φορητών συσκευών για τους πρώτους ανταποκριτές.



Εικόνα 32. NG-RAN κεντροποιημένο και κατανεμημένο σύστημα [77]



Εικόνα 33. Τα στάδια ολοκλήρωσης της 17ης έκδοσης. Πηγή: 3GPP [78]

Σύμφωνα με την 3GPP οι τομείς του 5G με τις οποίες οι ομάδες τεχνικών προδιαγραφών (Technical Specification Groups – TSG) ασχολήθηκαν για την ανάπτυξη και αναβάθμιση του προτύπου στην 17η έκδοση είναι οι παρακάτω (Εικόνα 33).

- Βελτιώσεις στην πλευρική σύνδεση (Sidelink) [79]
- Συσκευές μειωμένης ικανότητας (Reduced Capability - RedCap) για τη νέα ζώνη (New Radio – NR)
- Επέκταση της λειτουργίας NR στα 71GHz
- Περαιτέρω βελτιώσεις σε MIMO για NR
- NR σε μη επίγεια δίκτυα NTN
- IoT μέσω NTN
- Βελτιώσεις εξοικονόμησης ενέργειας του UE για NR
- Βελτιώσεις στην ολοκληρωμένη πρόσβαση και την οπισθοζεύξη για τη NR
- Βελτίωση του τεμαχισμού του Ραδιοδικτύου πρόσβασης (Radio Access Network – RAN) για το NR
- Βελτίωση των απαιτήσεων της Ραδιοσυχνότητας (Radio Frequency – RF) για NR ζώνη συχνοτήτων 1 (Frequency - FR1)

4.4.3 Συγκριτικά χαρακτηριστικά του 5G, με το 4G και 3G

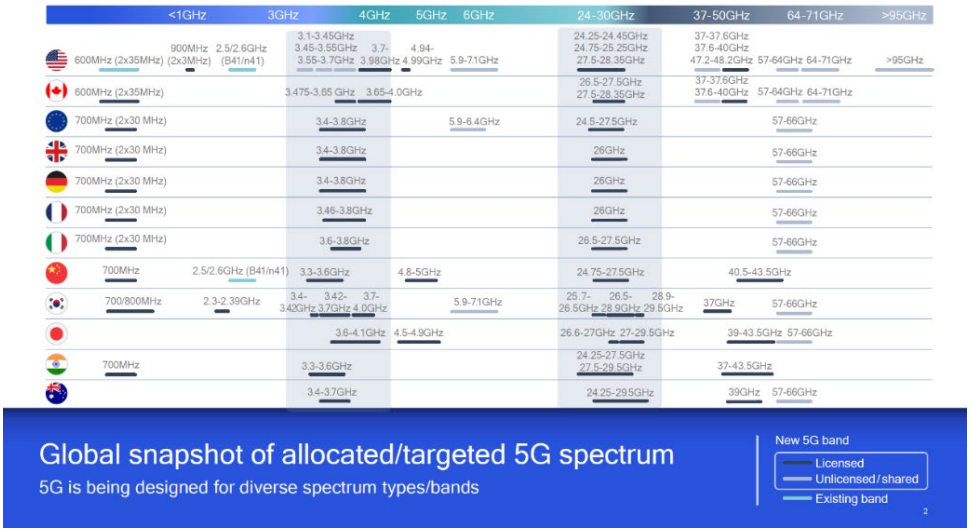
Το 5G περιλαμβάνει σημαντικές βελτιώσεις σε σχέση με το 3G και το 4G. Ορισμένες από τις βασικές διαφορές αναλύονται παρακάτω:

- Ταχύτητα: Το 5G προσφέρει σημαντικά υψηλότερες ταχύτητες λήψης και μεταφόρτωσης σε σύγκριση με το 3G και το 4G. Το 5G μπορεί να προσφέρει ταχύτητες λήψης έως και 20 Gbps, ενώ το 4G έως 1 Gbps και το 3G έως 42 Mbps.
- Καθυστέρηση: Το 5G έχει πολύ χαμηλότερη καθυστέρηση από το 4G ή το 3G. Το 5G έχει καθυστέρηση περίπου 1ms, ενώ το 4G έχει περίπου 50ms και το 3G έχει περίπου 100ms.
- Εύρος ζώνης: Το 5G μπορεί να υποστηρίξει εύρος ζώνης έως και 800 MHz, ενώ το 4G υποστηρίζει εύρος ζώνης έως και 100 MHz και το 3G υποστηρίζει εύρος ζώνης έως και 20 MHz.
- Χωρητικότητα: Τα δίκτυα 5G μπορούν να διαχειριστούν έως 1 εκατομμύριο συσκευές ανά τετραγωνικό χιλιόμετρο, την ίδια στιγμή που τα δίκτυα 4G έχουν τη δυνατότητα για 100.000 και τα δίκτυα 3G έως 16.000 συσκευές.
- Ενεργειακή απόδοση: Σύμφωνα με τους [80] [81] [82] [83] [84] τα δίκτυα 5G είναι πιο αποδοτικά από τα δίκτυα 4G και 3G, με ικανότητα μείωσης της κατανάλωσης ενέργειας έως 90%.Η ενεργειακή απόδοση αποτελεί σημαντική παράμετρος των κινητών δικτύων, καθώς μπορεί να συμβάλει στην παράταση της διάρκειας ζωής της μπαταρίας των κινητών συσκευών και στη μείωση της συνολικής κατανάλωσης

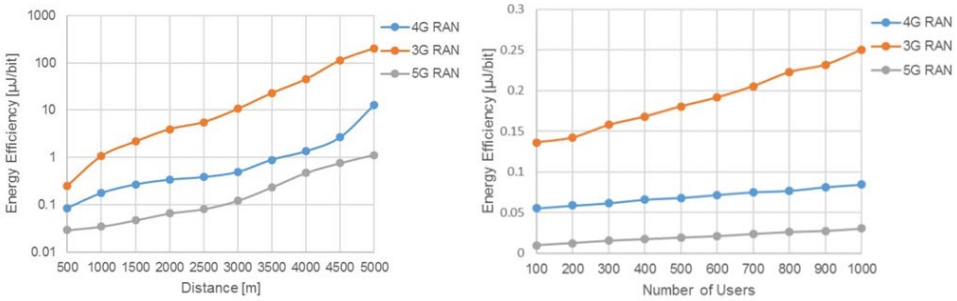
ενέργειας του δικτύου. Ειδικότερα για τους οργανισμούς PS και τα δίκτυα PSDR σε περιπτώσεις που έχουν καταστραφεί μερικώς ή ολικώς οι κρίσιμες υποδομές παροχής ενέργειας, η δυνατότητα λειτουργίας ad-hoc δικτύων με μειωμένη κατανάλωση αποτελεί σημαντικό κριτήριο για την πρόκριση της συγκεκριμένης τεχνολογίας στα PSDR δίκτυα επόμενης γενιάς. Ακολουθούν ορισμένες βασικές διαφορές στην ενεργειακή απόδοση μεταξύ των δικτύων 5G, 4G και 3G:

- Κατανάλωση ενέργειας BS: Οι 5G BSs καταναλώνουν λιγότερη ενέργεια από τους σταθμούς βάσης 4G και 3G. Για παράδειγμα, ένας BS 5G μπορεί να καταναλώνει το 50% της ενέργειας από έναν σταθμό βάσης 4G για τον ίδιο όγκο κίνησης.
- Κατανάλωση ενέργειας κινητής συσκευής (Mobile Device - MD): Οι 5G MDs καταναλώνουν λιγότερη ενέργεια από τις κινητές συσκευές 4G και 3G. Για παράδειγμα, ένα έξυπνο τηλέφωνο 5G μπορεί να καταναλώσει έως και 90% λιγότερη ενέργεια από το αντίστοιχο 4G για τις ίδιες εργασίες, χαρακτηριστικό ιδιαίτερα σημαντικό για την πολύωρη χρήση στο πεδίο όπου η δυνατότητες πρόσβασης σε πηγές τροφοδοσίας είναι περιορισμένες.
- Δυνατότητα αναστολής λειτουργίας: Τα δίκτυα 5G διαθέτουν δυνατότητα αναστολής λειτουργίας που επιτρέπει στις κινητές συσκευές να εξοικονομούν ενέργεια όταν δεν χρησιμοποιούνται. Αυτό μπορεί να μειώσει σημαντικά την κατανάλωση ενέργειας των κινητών συσκευών και να παρατείνει τη διάρκεια λειτουργίας των συσκευών.
- Ενεργειακά αποδοτικές κεραίες: Τα δίκτυα 5G χρησιμοποιούν ενεργειακά αποδοτικότερες κεραίες μικρότερης κατανάλωσης από τις αντίστοιχες των δικτύων 4G και 3G.
- Διαχείριση παρεμβολών: Τα δίκτυα 5G χρησιμοποιούν προηγμένες τεχνικές διαχείρισης παρεμβολών, όπως η διαμόρφωση δέσμης (Beam Forming – BF), επιτυγχάνοντας έτσι την μείωση της κατανάλωση ενέργειας των κινητών συσκευών.
- Τεμαχισμός δικτύου (Network Slicing): Τα δίκτυα 5G με δυνατότητες τεμαχισμού του δικτύου, μπορούν να επιτρέψουν διαφορετικές συμφωνίες επιπέδου υπηρεσιών (Service Level Agreement - SLA) για διαφορετικές υπηρεσίες έχοντας ως συνέπεια την μείωσης της κατανάλωσης ενέργειας.

Συμπερασματικά θα αναφέραμε πως τα δίκτυα 5G διαθέτουν καλύτερη ενεργειακή απόδοση [80] από τα αντίστοιχα 4G και 3G με σημαντικά οφέλη τόσο στην βελτίωση της διάρκειας ζωής της μπαταρίας των κινητών συσκευών όσο και στη μείωση της συνολικής κατανάλωσης ενέργειας του δικτύου.



Εικόνα 34. 5G Ζώνες λειτουργίας σε διαφορετικές χώρες. Πηγή: Devopedia [85]



Εικόνα 35. Ενεργειακή απόδοση ως συνάρτηση της (α) απόστασης μεταξύ κάθε RAN και της έξυπνης συσκευής του χρήστη και (β) αριθμό έξυπνων συσκευών [80]

- Ασφάλεια: Η ασφάλεια είναι μια κρίσιμη παράμετρος των PSDR, καθώς συμβάλλει στην προστασία από την παραβίαση δεδομένων καθώς και άλλων μορφών επιθέσεων του κυβερνοχώρου. Ακολουθούν ορισμένες βασικές διαφορές στην ασφάλεια [86] μεταξύ των δικτύων 5G, 4G και 3G:
  - ❖ Αυθεντικοποίηση και κρυπτογράφηση: Τα δίκτυα 5G χρησιμοποιούν ισχυρότερες μεθόδους ελέγχου ταυτότητας και κρυπτογράφησης από τα δίκτυα 4G και 3G, όπως η κρυπτογράφηση 128-bit Σύνθετου Πρότυπου Κρυπτογράφησης (Advanced Encryption Standard – AES). Αυτό συμβάλλει στην προστασία από επιθέσεις ενδιάμεσου (man-in-the-middle) ή άλλες μορφές επιθέσεων στον κυβερνοχώρο.
  - ❖ Ιδεατοποίηση (Virtualization): Τα δίκτυα 5G χρησιμοποιούν την (NFV) ενώ ο καθορισμός της δικτύωσης πραγματοποιείται με (SDN) το οποίο διαχειρίζεται τόσο την ιδεατοποίηση των λειτουργιών δικτύου όσο και τη βελτίωση της ασφάλειας. Έτσι εξασφαλίζεται η ανάπτυξη ευέλικτων πολιτικών ασφαλείας προσφέροντας ταυτόχρονα και καλύτερη προστασία από κυβερνοεπιθέσεις.

- ❖ Τεμαχισμός δικτύου (Network Slicing): Εξασφαλίζει τον σχεδιασμό διαφορετικών πολιτικών ασφαλείας για διαφορετικές υπηρεσίες, εξασφαλίζοντας με αυτό τον τρόπο την καλύτερη προστασία από κυβερνοεπιθέσεις.
- ❖ Εγγενή χαρακτηριστικά ασφαλείας 5G: Τα χαρακτηριστικά ασφαλείας του 5G αποτελούν αναπόσπαστα τμήματα του συστήματος, και παρέχουν ασφάλεια από άκρο σε άκρο (End-to-End) στο δίκτυο 5G.
- ❖ Ασφάλεια 4G: Το πρότυπο 4G διαθέτει χαρακτηριστικά ασφαλείας που μπορούν να εφαρμοστούν, αλλά δεν είναι εγγενή.
- ❖ Ασφάλεια 3G: Το πρότυπο 3G υποστηρίζει βασικά χαρακτηριστικά ασφαλείας, όπως πιστοποίηση ταυτότητας και κρυπτογράφηση, αλλά δεν είναι τόσο ισχυρά όσο αυτά των δικτύων 4G και 5G.

Θα πρέπει επίσης να θέσουμε υπόψη πως η ασφάλεια ενός δικτύου ασύρματης επικοινωνίας επηρεάζεται από πολλούς παράγοντες γεγονός που δεν επιτρέπει εύκολα την γενίκευση. Παρόλα αυτά, είναι ασφαλές να συμπεράνουμε, πως τα δίκτυα 5G διαθέτουν ισχυρότερους μηχανισμούς ασφαλείας από τα δίκτυα 4G και 3G, και αυτό μπορεί να συμβάλει στην προστασία από παραβιάσεις δεδομένων, ή άλλων μορφών επιθέσεων από τον κυβερνοχώρο.

- Διαθεσιμότητα: Η διαθεσιμότητα αναφέρεται στην ικανότητα ενός δικτύου να παρέχει υπηρεσίες στους χρήστες όταν και όπου χρειάζεται. Ένα χαρακτηριστικό που βρίσκεται στις πρώτες προτεραιότητες στη λίστα των απαιτήσεων των οργανισμών PS, με εφαρμογή σε σενάρια ή περιοχές όπου υπάρχει υπερβολικά πυκνή πληθυσμιακή σύνθεση. Για παράδειγμα σε γήπεδα όπου η πιθανότητα υπερφόρτωσης του δικτύου είναι υψηλή. Στην περίπτωση ενός μεγάλου σεισμού είναι πιθανόν το δίκτυο να αδυνατεί να ανταπεξέλθει στα μαζικά ταυτόχρονα αιτήματα των συνδρομητών, ιδιαίτερα αν ορισμένοι BS τεθούν εκτός λειτουργίας. Παρακάτω αναλύουμε ορισμένες βασικές διαφορές στη διαθεσιμότητα μεταξύ των δικτύων 5G, 4G και 3G:
  - ❖ Κάλυψη: Τα δίκτυα 5G έχουν ευρύτερη κάλυψη από τα δίκτυα 4G και 3G, χάρη στη χρήση ποικίλων ζωνών συχνοτήτων και της τεχνολογίας διαμόρφωσης δέσμης που χρησιμοποιούν, είναι αποδοτικότερα από τα παλαιότερα δίκτυα.
  - ❖ Κινητικότητα: Τα δίκτυα 5G παρέχουν μεγαλύτερη κινητικότητα από τα δίκτυα 4G και 3G, πράγμα που σημαίνει ότι οι χρήστες μπορούν να μετακινούνται πιο ελεύθερα χωρίς να χάνουν τη σύνδεση.
  - ❖ Ανθεκτικότητα: Τα δίκτυα 5G έχουν σχεδιαστεί για να είναι πιο ανθεκτικά από τα δίκτυα 4G και 3G, με μηχανισμούς αυτο-ίασης που μπορούν να αποκαθιστούν γρήγορα την υπηρεσία σε περίπτωση βλάβης.

- ❖ Ιδεατοποίηση: Εκτός από όλα τα παραπάνω οφέλη της ιδεατοποίησης ένα ακόμη σημαντικό πλεονέκτημα αποτελεί και η βελτίωση της διαθεσιμότητας του δικτύου. Το στοιχείο αυτό είναι ιδιαίτερα σημαντικό για τους πρώτους ανταποκριτές διότι θα πρέπει σε ποσοστό 99,999% των περιπτώσεων η κλήση τους να πραγματοποιείται και μάλιστα με προτεραιότητα έναντι των απλών συνδρομητών.

Αξίζει να σημειωθεί ότι η διαθεσιμότητα ενός δικτύου κινητής τηλεφωνίας μπορεί να διαφέρει ανάλογα με τη συγκεκριμένη υλοποίηση και το σενάριο χρήσης. Ωστόσο, σε γενικές γραμμές, τα δίκτυα 5G εξασφαλίζουν μεγαλύτερη διαθεσιμότητα από τα δίκτυα 4G και 3G, παρέχοντας ευρύτερη κάλυψη, μεγαλύτερη κινητικότητα, μεγαλύτερη ανθεκτικότητα, παράγοντες που έχουν ως αποτέλεσμα την υψηλότερη διαθεσιμότητα του δικτύου.

- Αξιοπιστία (Reliability): Τα δίκτυα 5G είναι πιο αξιόπιστα από τα δίκτυα 4G και 3G, διαθέτουν σημαντικά υψηλότερες επιδόσεις σε μια σειρά από τους τομείς που παρουσιάσαμε, οι οποίες αποτελούν απαραίτητη προϋπόθεση για την λειτουργία σε εφαρμογές όπως τα αυτόνομα οχήματα, οι απομακρυσμένες χειρουργικές επεμβάσεις καθώς και εφαρμογές στον τομέα της δημόσιας ασφάλειας.

4.4.4 Το 5G στα Δίκτυα Δημόσιας Ασφάλειας

Στον Πίνακας 8 βλέπουμε μια συνολική συνοπτική αποτύπωση των σημαντικότερων απαιτήσεων που έχουν καθορίσει οι οργανισμοί δημόσιας ασφάλειας σήμερα. Η έκδοση 17 του 5G καλύπτει σχεδόν το σύνολο αυτών των απαιτήσεων, λόγω της πλήρους υιοθέτησης των προτύπων MCX επικοινωνιών που σχεδιάστηκαν και αναπτύχθηκαν στα πλαίσια της συνεργασίας της TCCA και της 3GPP. Συγκεκριμένα οι υπηρεσίες κρίσιμων υπηρεσιών γνωστές και ως MCX όπου το X αναφέρεται σε: PTT, Video, Data, χωρίζονται σε τρείς κατηγορίες:

α. Κρίσιμη αποστολή φωνής με το πάτημα ενός πλήκτρου (MCPTT) [87]

β. Κρίσιμη Αποστολή Βίντεο (Mission Critical Video – MCVideo) [88]

γ. Κρίσιμη Αποστολή Δεδομένων (Mission Critical Data – MCData) [89]

Το MCPTT είναι μια υπηρεσία φωνής με ρυθμό δεδομένων 20 – 70kbps. Ο ρυθμός δεδομένων εξαρτάται από δυο παραμέτρους τον κωδικοποιητή ήχου και την υλοποίηση του συστήματος.

Το MCVideo είναι υπηρεσία που περιλαμβάνει τρείς διαφορετικές λειτουργίες βίντεο και συγκεκριμένα: (α)επείγον βίντεο σε πραγματικό χρόνο, (β)μη επείγον βίντεο με μετάδοση σε πραγματικό χρόνο και (γ)μετάδοση σε μη πραγματικό χρόνο. Ανάλογα με την απαιτούμενη ποιότητα του βίντεο ο ρυθμός μετάδοσης κυμαίνεται από 150kbps έως 5Mbps.

Το MCData είναι υπηρεσία μετάδοσης δεδομένων με ρυθμό που κυμαίνεται από 10kbps έως 1Mbps. Η QoS των MCX για κάθε χαρακτηριστικό ορίζονται από την 3GPP ως τυποποιημένα αναγνωριστικά QoS 5G (5 Quality Indentifiers - QI) [90], και συνοψίζονται στον Πίνακας 7. Μια τιμή 5QI αντιστοιχίζεται σε ένα σύνολο QoS χαρακτηριστικών, συμπεριλαμβανομένου του τύπου πόρου, του προεπιλεγμένου επιπέδου προτεραιότητας, τον προϋπολογισμό καθυστέρησης πακέτων και την απαίτηση ρυθμού σφάλματος πακέτων. Αυτά τα χαρακτηριστικά χρησιμοποιούνται ως οδηγοί QoS για την από άκρο σε άκρο εξασφάλιση της ομαλής ροής της κίνησης.

- Ο τύπος πόρου καθορίζει και τις απαιτούμενες ενέργειες που πρέπει να γίνουν για μια ροή QoS ώστε να εξασφαλιστεί η απαίτηση απόδοσης.
- Το επίπεδο προτεραιότητας υποδεικνύει την σημαντικότητα και την ιεράρχηση μιας ροής QoS, η οποία μπορεί να χρησιμοποιηθεί ως είσοδος για τον έλεγχο και τον προγραμματισμό των πόρων.
- Ο προϋπολογισμός καθυστέρησης πακέτων καθορίζει την επιτρεπόμενη καθυστέρηση, για την παράδοση των πακέτων, μεταξύ του εξοπλισμού χρήστη (UE) και του κεντρικού δικτύου.
- Ο ρυθμός σφάλματος πακέτων υπολογίζει τον αριθμό των πακέτων δεδομένων που μεταδίδονται εσφαλμένα ή χάνονται κατά τη μετάδοση σε ένα δίκτυο. Παρέχει πληροφορίες σχετικά με την απόδοση ενός δικτύου και χρησιμοποιείται για τον έγκαιρο εντοπισμό πιθανών προβλημάτων.

Υπηρεσία		5 τιμές QI	Τύπος πόρου	Επίπεδο προτεραιότητας (χαμηλότερη τιμή σημαίνει υψηλότερη προτεραιότητα)	Προϋπολογισμός καθυστέρησης πακέτου (συμπεριλαμβανομένης της καθυστέρησης βασικού δικτύου)	Προϋπολογισμός καθυστέρησης RAN	Ποσοστό σφάλματος πακέτου
MCPTT	Φωνητικό επίπεδο χρήστη	65	Εγγυημένος ρυθμός bit ροής (GBR)	7	75 ms	65 ms	10-2
	Σηματοδότηση	69	Μη - GBR	5	60 ms	50 ms	10-6
MCVideo επίπεδο χρήστη		67	GBR	15	100 ms	100 ms	10-3
MCData		70	Μη - GBR	55	200 ms	200 ms	10-6

Πίνακας 7. Χαρακτηριστικά Ποιότητας Υπηρεσιών QoS Κρίσιμης Αποστολής MC με βάση το πρότυπο 3GPP [69]

Τύπος υπηρεσίας	Διαδραστικότητα	Παραδείγματα	
Υπηρεσίες φωνής	Διαδραστικό: Αποστολή φωνητικών μηνυμάτων σε πολλές οντότητες και διαδραστικές κλήσεις μεταξύ πολλών οντοτήτων	Full - Duplex Κλήσεις	Κλήσεις μεταξύ δύο οντοτήτων όπου τα δεδομένα φωνής ανταλλάσσονται και προς τις δύο κατευθύνσεις ταυτόχρονα
		Half - Duplex PTT	Κλήσεις μεταξύ δύο οντοτήτων όπου τα δεδομένα φωνής ανταλλάσσονται προς μία κατεύθυνση κάθε φορά
		Ομαδικές κλήσεις	Κλήσεις πλήρους ή μισής διπλής όψης που περιλαμβάνουν περισσότερες από δύο οντότητες
		Κλήσεις έκτακτης ανάγκης	Επείγουσες κλήσεις που απαιτούν υψηλή αξιοπιστία και προτεραιότητα
	Μη διαδραστικά: ενημερωτικά φωνητικά μηνύματα από μια οντότητα σε άλλη χωρίς να απαιτείται άμεση απάντηση	Ακρόαση περιβάλλοντος	Ακρόαση εκπομπών φωνής κοντινών ανταποκριτών
		Φωνητικά μηνύματα ειδοποίησης	Ανταλλαγή φωνητικών ειδοποιήσεων και ειδοποιήσεων
		Αναγνωριστικό καλούντος	Αναγνώριση μελών κλήσεων κατά τη διάρκεια κλήσεων ένα - προς - ένα ή ομαδικές

Τύπος υπηρεσίας	Διαδραστικότητα	Παραδείγματα	(συνέχεια Πίνακα)
Υπηρεσίες δεδομένων	Διαδραστικό: Γίνονται ερωτήματα σχετικά με συγκεκριμένα κομμάτια δεδομένων και απαιτείται άμεση απάντηση	Συστήματα Real-Time Location System- RTLS	Προσδιορισμός και παρακολουθήση της θέσης των πρώτων αντοκριτών σε εσωτερικούς χώρους σε πραγματικό χρόνο
		Πρόσβαση σε διακομιστές PS	Δυνατότητα πρόσβασης σε βάσεις δεδομένων PS
		Πρόσβαση στον χάρτη	Παγκόσμιος εντοπισμός, ανάγνωση χαρτών και ανταλλαγή πληροφοριών θέσης.
		Βιομετρική ταυτότητα	Προσδιορισμός ατόμων με βάση τα βιομετρικά τους στοιχεία όπου χρειάζεται διαδραστική επικοινωνία με διακομιστές PS
	Μη διαδραστικό: κοινή χρήση δεδομένων χωρίς να απαιτείται απάντηση	Γραπτά μηνύματα	Αποστολή και λήψη μηνυμάτων κειμένου μεταξύ δύο ή περισσότερων οντοτήτων
		Παρακολούθηση δεδομένων Ασύρματων δικτύων αισθητήρων (Wireless Sensor networks - WSNs)	Δυνατότητα συλλογής πληροφοριών από τα WSNs που έχουν αναπτυχθεί σε περιοχές καταστροφών
		Παρακολούθηση ζωτικών σημείων	Παρακολούθηση ζωτικών σημείων των πρώτων ανταποκριτών χρησιμοποιώντας WSNs σώματος
Υπηρεσίες Πολυμέσων	Διαδραστικό: γίνονται ερωτήματα σχετικά με πληροφορίες τύπου πολυμέσων και απαιτείται άμεση απάντηση	Αναγνώριση προσώπου	Αναγνώριση ατόμων με βάση τις εικόνες του προσώπου τους
		Βιντεοκλήσεις	Ένας προς έναν ή ομαδικές βιντεοκλήσεις
	Μη διαδραστικό: πρόσβαση και κοινή χρήση πολυμέσων και ροής σε πραγματικό χρόνο	Επιτήρηση	Εγγραφή βίντεο με δυνατότητα πρόσβασης από συστήματα επιτήρησης
		Κοινή χρήση εικόνων	Κοινή χρήση εικόνων με άλλους πρώτους ανταποκριτές
		Ροή βίντεο	Πρόσβαση σε πραγματικό χρόνο σε ζωντανή ροή βίντεο

Πίνακας 8. Απαιτήσεις PSNs και είδη υπηρεσιών [91]

4.4.5 5G Μελέτες περίπτωσης

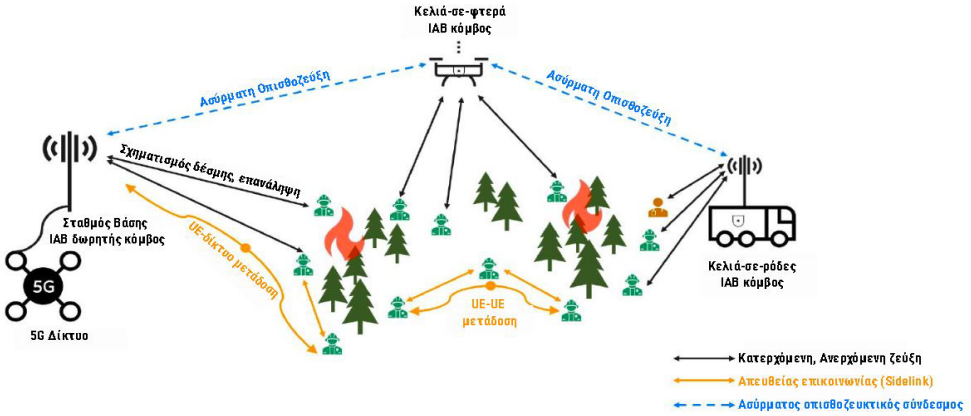
Η αξιοποίηση των τεχνολογιών της πέμπτης γενιάς επικοινωνιών στους τομείς της δημόσιας ασφάλειας έχει ήδη ξεκινήσει και οι εκτιμήσεις κάνουν λόγο για μια αγορά 700 εκ. δολάρια για την περίοδο 2022 - 2025 σύμφωνα με την συγκεκριμένη έρευνα [92]. Αυτό με τη σειρά του οδηγεί στην αναζήτηση λύσεων είτε με νέες αρχιτεκτονικές είτε με εφαρμογές για ένα πλήθος σεναρίων που οι αρμόδιοι οργανισμοί καλούνται να διαχειριστούν. Στην ενότητα αυτή θα αναδείξουμε τρείς ενδεικτικές μελέτες περίπτωσης που προϋποθέτουν την χρήση του 5G.

4.4.5.1 Δασοπυρόσβεση

Η αρχιτεκτονική 5G (Εικόνα 36) μπορεί να αναπτυχθεί σε περιπτώσεις δασικών πυρκαγιών [69]. Σε αυτή την περίπτωση χρησιμοποιείται η εναέρια ασύρματη οπισθοζεύξη με χρήση UAV για την επέκταση του σήματος στην δασική περιοχή. Οι λύσεις κάλυψης περιλαμβάνουν τους παρακάτω τρόπους:

1) UAV(κελιά-σε-φτερά) με ασύρματη οπισθοζεύξη με τον Σταθμό Βάσης
2) Κινητός σταθμός (κελιά-σε-ρόδες) με UAV (για επέκταση του σήματος
3) Απευθείας επικοινωνία UE προς UE μεταξύ των πυροσβεστών χωρίς χρήση οπισθοζεύξης

4) Κινητός σταθμός με UE (πυροσβέστες)
5) Σταθμός Βάσης με UE
6) UAV με UE



Εικόνα 36. Λύσεις κάλυψης 5G NR για την παροχή απεριόριστης συνδεσιμότητας για τις επικοινωνίες MC δημόσιας ασφάλειας [69]

4.4.5.2 Εκπαίδευση σε εικονικό περιβάλλον

Η εκπαίδευση των πρώτων ανταποκριτών μπορεί πλέον να επιτευχθεί σε εικονικό περιβάλλον απτικού διαδικτύου. Αυτό θα εξασφαλίσει την εκπαίδευση σε πλήθος διαφορετικών σεναρίων που σε πολλές περιπτώσεις δεν θα ήταν εφικτό να πραγματοποιηθούν σε συνθήκες κανονικότητας. Επίσης με αυτό τον τρόπο μπορεί να υπάρξει μεγαλύτερη συμμετοχή του προσωπικού των οργανισμών PS ακόμη και απομακρυσμένα, γεγονός που οδηγεί στην εξοικονόμηση επιπλέον πόρων.Είναι σημαντικό επίσης να τονίσουμε πως στη διάρκεια της εκπαίδευσης οι εκπαιδευτές μπορούν σε πραγματικό χρόνο να καθοδηγούν τους εκπαιδευόμενους ώστε να υιοθετούνται η βέλτιστες πρακτικές για κάθε πιθανό σενάριο.

Τον Μάιο του 2022 το NIST δημιούργησε το πρώτο εκπαιδευτικό κέντρο στον κόσμο για τη δημόσια ασφάλεια (Immersive Virtual Experience Center for Public Safety) [93] που προσφέρει εμπειρίες εικονικής πραγματικότητας. Σε συνεργασία με το First Net στο κέντρο αυτό θα μπορούν να εκπαιδευτούν δωρεάν οι πρώτοι ανταποκριτές από όλες τις υπηρεσίες των ΗΠΑ ενώ οι εταιρείες θα μπορούν δοκιμάζουν εξοπλισμό και εφαρμογές για τους πρώτους ανταποκριτές σε μια σύμπραξη με αμοιβαία οφέλη [94], Είναι σημαντικό να τονίσουμε πως στο συγκεκριμένο κέντρο η εμπειρία θα είναι πρωτόγνωρη γιατί οι εκπαιδευόμενοι θα μπορούν να κινηθούν ή ακόμη και να έρπουν μέσα στο χώρο, να κρατούν αντικείμενα όπως πυροσβεστήρες και να αγγίζουν τοίχους και έπιπλα χωρίς τη χρήση ελεγκτών που ήταν απαραίτητοι στους παραδοσιακούς εξομοιωτές εικονικής πραγματικότητας. Συνεπώς αυτή η προσέγγιση θα προετοιμάσει καλύτερα τους πρώτους ανταποκριτές στην αντιμετώπιση σεναρίων όταν κληθούν να τα διαχειριστούν σε ρεαλιστικές συνθήκες.

Εικόνα 37. NIST Κέντρο Δοκιμών Δημόσιας Ασφάλειας Καθηλωτικής Εμπειρίας[7] [95]

4.4.5.3 Εντοπισμός στίγματος σε εσωτερικό χώρο με χρήση 5G και UAVs

Ο ακριβής εντοπισμός θέσης [69] διαδραματίζει ζωτικό ρόλο στη βελτίωση της ασφάλειας και της επίγνωσης της κατάστασης των πρώτων ανταποκριτών. Συγκριτικά με τις προηγούμενες γενιές 4G και 3G, στο 5G NR, τα σήματα εντοπισμού θέσης και οι μετρήσεις έχουν ενισχυθεί για να παρέχουν μεγαλύτερη ακρίβεια εντοπισμού θέσης τόσο σε εσωτερικούς όσο και σε εξωτερικούς χώρους.

Το 5G NR υποστηρίζει δύο νέα σήματα αναφοράς για τον εντοπισμό θέσης και δυο νέων μεθόδων εντοπισμού. Αξιοποιώντας επίσης τα πλεονεκτήματα των χαρακτηριστικών διαμόρφωσης δέσμης πολλαπλών κεραιών στα mmWave, τα σήματα αναφοράς εντοπισμού θέσης μπορούν να μεταδοθούν σε δέσμες. Η μετάδοση αυτή επιτρέπει την καλύτερη εκτίμηση των αποστάσεων βελτιώνοντας επίσης και την εμβέλεια αυτών των σημάτων.

Ένα δύσκολο σενάριο για τον εντοπισμό θέσης των πρώτων ανταποκριτών είναι η αποτύπωση της τρισδιάστατης θέσης των πυροσβεστών σε ένα φλεγόμενο κτίριο στο οποίο υπάρχει διακοπή παροχής ρεύματος. Η λύση που προτείνεται [69] για αυτό το σενάριο είναι η χρήση UAVs ως κινητών BS για την παροχή πρόσθετων συνδέσεων επικοινωνίας, εξασφαλίζοντας ταυτόχρονα και με ακρίβεια τον εντοπισμό της θέσης των πυροσβεστών εντός του κτιρίου. Με αυτή την ανάπτυξη (Σχ.9) είναι επίσης δυνατό ο εντοπισμός οποιουδήποτε ατόμου που φέρει συσκευή 5G NR και βρίσκεται παγιδευμένο σε άγνωστη τοποθεσία εντός του κτιρίου.

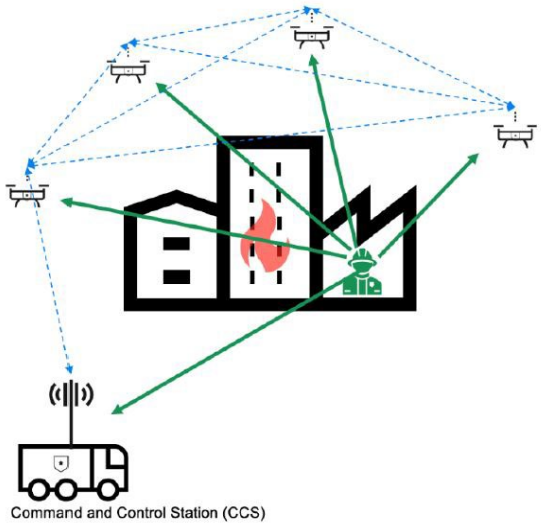
Η ανάπτυξη UAVs ως κινούμενων BS προσφέρει μια σειρά από πλεονεκτήματα.

- Εξασφαλίζει την αδιάλειπτη επικοινωνία των πυροσβεστών
- Η δυνατότητα μετακίνηση των UAVs σε καλύτερη θέση παρέχει μεγαλύτερη ακρίβεια στίγματος και κάνει ευκολότερη την 3 διάστατη αποτύπωση των θέσεων τόσο των πυροσβεστών αλλά και όλων όσων διαθέτουν συσκευή 5GNR.

[7] https://www.theasys.io/viewer/4ciiGJMYYfxYNZrZOjX8IQ5utt0c6R/

- Με την χρήση και των καμερών από τα UAVs εξασφαλίζεται καλύτερη επίγνωση της κατάστασης, γεγονός που οδηγεί στη λήψη ορθότερων αποφάσεων για τον αποδοτικότερο συντονισμό των ομάδων, ένας παράγοντας κρίσιμος για την έκβαση κάθε αποστολής.

Συνοψίζοντας εκτιμούμε πως η Πέμπτη γενιά επικοινωνιών με τα τεχνολογικά χαρακτηριστικά που διαθέτει θα αποτελέσει τη βάση των μελλοντικών δικτύων ασφαλείας. Είναι επίσης σημαντικό να αναφέρουμε το γεγονός της στενής συνεργασίας των δυο σημαντικότερων οργανισμών του TCCA και της 3GPP που ουσιαστικά καθορίζουν τα μελλοντικά πρότυπα στον συγκεκριμένο τομέα σχεδιάζοντας με πολύ προσοχή τα βήματα της μετάβασης από τις τεχνολογίες στενής ζώνης στις ευρυζωνικές επικοινωνίες. Μέσα από αυτή τη συνεργασία χώρες όπως η Φινλανδία το Ηνωμένο Βασίλειο αλλά και οι ΗΠΑ έχουν ήδη δρομολογήσει την ανάπτυξη των δημόσιων ευρυζωνικών δικτύων της επόμενης γενιάς. (η Φινλανδία έχει σχεδιάσει την ολοκλήρωση του δικτύου της το 2025). Το γεγονός αυτό οδηγεί σε περαιτέρω μείωση και του κόστους του τηλεπικοινωνιακού εξοπλισμού αλλά και των συσκευών, του πιο σημαντικού παράγοντα για την υλοποίηση αυτών των δικτύων. Τα μειωμένα CAPEX και OPEX σε συνδυασμό με την δυνατότητα εμπορικής εκμετάλλευσης αυτών των δικτύων σε συνθήκες κανονικότητας θα εξασφαλίσουν την μελλοντική βιωσιμότητα αλλά και συνεχή αναβάθμιση των υποδομών.



Εικόνα 38. Σενάριο 3D αποτύπωσης θέσης σε εσωτερικό χώρο με τη χρήση UAVs [69]

4.5 Software Defined Radio

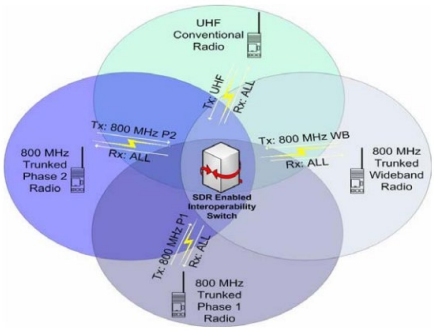
Το SDN προτείνεται ως βασικός ενεργοποιητής για δυναμική διαχείριση προτεραιότητας στα PSNs. Στα Δίκτυα που Βασιζονται στο Λογισμικό (Software Defined Networks – SDNs), οι

αποφάσεις λαμβάνονται με βάση τη ροή και εφαρμόζονται με τη μορφή κανόνων. Η ροή των δεδομένων ελέγχεται με βάση τις πολιτικές και τους κανόνες που ορίζονται σε έναν ελεγκτή SDN. Ως εκ τούτου, ένα σχήμα διαχείρισης προτεραιότητας μπορεί να εφαρμοστεί αποτελεσματικά χρησιμοποιώντας την τεχνολογία SDR [49]. Ουσιαστικά, η ιδέα του ράδιο-πομποδέκτη που καθορίζεται από λογισμικό γεννήθηκε από την ανάγκη να ξεπεραστεί το πρόβλημα της αδυναμίας περαιτέρω κλιμάκωσης της προσθήκης νέων ζωνών, λειτουργιών και υπηρεσιών σε φορητές ασύρματες συσκευές [96]. Αυτό που συνέβη στις ραδιοεπικοινωνίες μέσω του λογισμικού Επεξεργασίας Ψηφιακού Σήματος (Digital Signal Processing – DSP) για την εκτέλεση των περισσότερων λειτουργιών ράδιο-εκπομπής/λήψης

σε επίπεδα απόδοσης που προηγουμένως θεωρούνταν ανέφικτα, παραλληλίζεται με αυτό που κατάφεραν τα modem στην επέκταση και εξάπλωση του διαδικτύου. Ένας ραδιο-πομποδέκτης που καθορίζεται από λογισμικό χαρακτηρίζεται από ευελιξία, καθώς τροποποιώντας απλώς, ή αντικαθιστώντας προγράμματα λογισμικού μπορεί να αλλάξει εντελώς τη λειτουργικότητά του. Έτσι επιτυγχάνεται εύκολη αναβάθμιση σε νέες λειτουργίες και βελτιωμένη απόδοση χωρίς την ανάγκη αντικατάστασης υλικού [97].

Πως όμως η τεχνολογία SDR εμπλέκεται στη δημιουργία δικτύων PSNs; Η κοινότητα της δημόσιας ασφάλειας οδηγήθηκε σταδιακά να διερευνήσει τους τρόπους αξιοποίησης της εξελισσόμενης τεχνολογία SDR και ένταξης αυτής στις λύσεις στενής ζώνης για τη βελτιστοποίηση αντιμετώπισης κρίσιμων προκλήσεων επικοινωνίας στη δημόσια ασφάλεια. Μια από τις πρωταρχικές αλλά και βασικές προκλήσεις που έπρεπε να αντιμετωπιστεί ήταν η διαλειτουργικότητα [98].

Για τους σκοπούς προώθησης αυτής της προσπάθειας, το 2004 το SDR Forum δημιούργησε μια Ειδική Ομάδα Ενδιαφέροντος για τη Δημόσια Ασφάλεια (Public Safety Special Interest Group - SIG) με σκοπό να προωθήσει τις λύσεις που προκρίνονται με SDR. Η ομάδα αυτή δημοσίευσε το 2006 την Έκθεση με τίτλο «Τεχνολογία SDR για τη δημόσια ασφάλεια» [99], όπου περιγράφονται οι τρόποι βελτίωσης της διαλειτουργικότητας μεταξύ των πρώτων ανταποκριτών και προσδιορίζονται περαιτέρω πιθανά οφέλη της. Από την ίδια Έκθεση συνάγεται ότι το SDR παρέχει μια αποτελεσματική και σχετικά φθηνή λύση στο πρόβλημα της κατασκευής ασύρματων συσκευών πολλαπλών λειτουργιών και πολλαπλών ζωνών, που μπορούν να βελτιωθούν χρησιμοποιώντας αναβαθμίσεις λογισμικού. Υπό την έννοια αυτή και ως αρχικώς αναφέρθηκε, το SDR χαρακτηρίστηκε ως ενεργοποιητής. Οι συσκευές με SDR (π.χ. φορητές συσκευές χειρός) και ο εξοπλισμός (π.χ. υποδομή ασύρματου δικτύου) μπορούν να προγραμματιστούν δυναμικά και να τροποποιηθούν αναλόγως για να εκτελούν διαφορετικές λειτουργίες σε διαφορετικούς χρόνους [99]. Επιπλέον, η τεχνολογία SDR μπορεί να βελτιώσει τη διαλειτουργικότητα των επικοινωνιών δημόσιας ασφάλειας, επιτρέποντας την επικοινωνία μεταξύ διαφορετικών συστημάτων (Εικόνα 39).

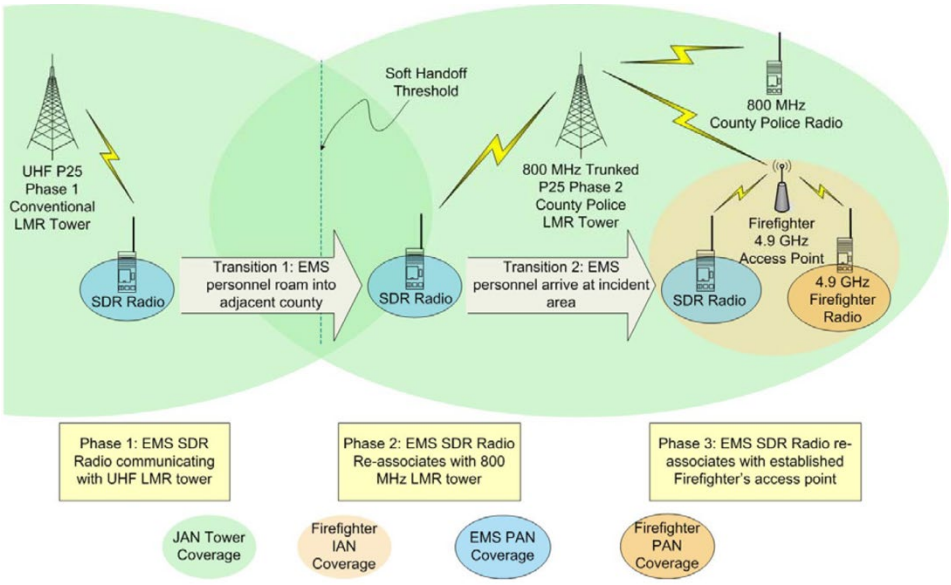


Εικόνα 39. Διεπαφές διαλειτουργικότητας SDR [99]

Όπως πολλές άλλες τεχνολογίες, το SDR θα μπορούσε να διαδραματίσει σημαντικό ρόλο στη βελτίωση των επικοινωνιών δημόσιας ασφάλειας, καθώς τα οφέλη μπορούν να είναι πολλαπλά και συγκεκριμένα:

- Μείωση του κόστους που σχετίζεται με την αναβάθμιση και τροποποίηση του κατεχόμενου εξοπλισμού.
- Ικανότητα προσαρμογής σε εξελισσόμενες τεχνολογίες και πρότυπα.
- Ευκολία στη λειτουργία. Είναι χαρακτηριστικό ότι ο χρήστης θα πρέπει να απαλλάσσεται από την υποχρέωση διαχείρισης πληροφοριών που δεν διαφοροποιούν το επίπεδο ανταπόκρισής του. Για παράδειγμα, ο πρώτος ανταποκριτής αρκεί μόνο να γνωρίζει ότι το τακτικό κανάλι επικοινωνίας είναι το 2ο, χωρίς να ανησυχεί αν αυτό αφορά σε VHF, UHF, ή άλλης συχνότητας επικοινωνία.
- Βελτιστοποίηση απόδοσης. Αυτό επιτυγχάνεται από την αποτελεσματική αξιοποίηση του φάσματος, μέσω δυναμικής κατανομής.

Στην ίδια έκθεση του SIG αναφέρεται ότι ουσιαστικά οι μελλοντικές υλοποιήσεις εφαρμογών για τη δημόσια ασφάλεια θα αποτελούν έναν συνδυασμό συστημάτων που θα είναι αλληλοσυνδεδεμένα και θα αλληλεπιδρούν μεταξύ τους. Αυτή η υβριδική αρχιτεκτονική θα μπορούσε να ενσωματώσει την τεχνολογία SDR για την υλοποίηση των δικτύων, των προτύπων και πρωτοκόλλων που θα αναλάμβαναν την επικοινωνία μικρών ή μεγάλων αποστάσεων σε πολλαπλές συχνότητες και σε πλήρη διαλειτουργικότητα [99]. Ένα χαρακτηριστικό παράδειγμα του συγκεκριμένου μοντέλου φαίνεται στην Εικόνα 40, το οποίο μάλιστα στη σχετική έκθεση του SIG περιγράφεται ως το σύστημα των συστημάτων. Όπως είδαμε ήδη, το SDR είναι μια τεχνολογία που επιτρέπει στις συσκευές δικτύωσης να συνδέονται απευθείας με τις εφαρμογές με τη χρήση μια Διεπαφής Προγραμματισμού Εφαρμογών (Application Programming Interface – API), ώστε η συνολική διαχείριση του υλικού και των συσκευών που συνθέτουν αυτό να γίνεται διαμέσου του λογισμικού. Αυτό επιτυγχάνεται βέλτιστα με το διαχωρισμό του συνολικού δικτύου σε μικρότερα τμήματα.



Εικόνα 40. Το σύστημα των συστημάτων με υλοποίηση τεχνολογία SDR [99]

Τα βασικότερα πλεονεκτήματα ενός SDN συνοψίζονται στα ακόλουθα [100]:

- Κόστος. Η δυνατότητα πολλαπλής εκτέλεσης εργασιών, το σχετικά φτηνό υλικό που απαιτείται και η συγκεντρωτική και αυτοματοποιημένη διαχείριση του δικτύου έχει ως αποτέλεσμα αισθητά μειωμένο κόστος.
- Ασφάλεια. Υφίσταται ενιαίο σύστημα διαχείρισης, που λειτουργεί ελεγκτής σωστής εφαρμογής πολιτικών ασφάλειας του SDN. Οι απειλές ασφαλείας που αντιμετωπίζει το SDN αναλύονται στο [101], στο οποίο μάλιστα γίνεται μια προσέγγιση για την πρόληψη και μετριασμό αυτών.
- Συγκέντρωση – κεντρικοποίηση. Το SDN επιτρέπει την κεντρική διαχείριση του δικτύου και των συσκευών που ανήκουν σ` αυτό από μια κεντρική τοποθεσία.
- Επεκτασιμότητα. Η υποδομή του SDN μπορεί ν` αλλάξει χωρίς να υφίσταται ανάγκη νέων πόρων.
- Βελτιστοποίηση. Και στην περίπτωση αυτή η χρήση των ελεγκτών του δικτύου SDN παρέχουν τη δυνατότητα βελτιστοποιημένης χρήσης των συσκευών, καθώς αυτές δεν είναι αφιερωμένες μόνο σε έναν σκοπό.

Τα μειονεκτήματα των δικτύων SDNs συνοψίζονται στ` ακόλουθα [102]:

- Καθυστέρηση. Προκύπτει λόγω του αριθμού των εικονικών πόρων από τους οποίους εξαρτάται η ταχύτητα αλληλεπίδρασης των συσκευών του δικτύου.
- Συντήρηση. Η διαχείριση των πραγματικών πόρων του δικτύου SDN καθίσταται πραγματικά αδύνατη και ως εκ τούτου δημιουργούνται προβλήματα στη συντήρηση.

- Πολυπλοκότητα. Προϋποθέτει πολύ καλή γνώση του χειρισμού των συστημάτων του δικτύου SDN ώστε να περιορίσει ζητήματα ασφάλειας. Επιπλέον, δεν υπάρχουν τυποποιημένα πρωτόκολλα ασφάλειας για ένα SDN δίκτυο.
- Διαμόρφωση. Η επαναδιαμόρφωση ενός δικτύου SDN δεν είναι απλή υπόθεση, καθώς σε πολλές περιπτώσεις απαιτείται η εκ νέου ρύθμιση ολόκληρου του δικτύου.
- Ασφάλεια συσκευής. Με δεδομένο ότι από ένα SDN δίκτυο απουσιάζουν οι συμβατικοί δρομολογητές, απουσιάζουν ταυτόχρονα και τα τείχη προστασίας που αυτά περιλαμβάνουν, με ό,τι αυτό συνεπάγεται για την ασφάλεια του δικτύου σε εξωτερικές απειλές.

Εν κατακλείδι, παρά το γεγονός ότι προκύπτει δυνητικά η δυνατότητα το SDR να συνεισφέρει στη δημόσια ασφάλεια, υπάρχουν ακόμη σημαντικά ζητήματα που θα πρέπει να αντιμετωπιστούν, ώστε να γίνει κάτι τέτοιο πραγματικότητα. Το σημαντικότερο εξ αυτών αποτελεί η προτυποποίηση στη διεπαφή, στο μοντέλο που λειτουργεί για τα αντίστοιχα πρότυπα του TETRA και P25, ώστε να επιταχυνθεί η ενσωμάτωση της τεχνολογίας SDR στα συστήματα επικοινωνιών δημόσιας ασφάλειας [99].

4.6 Cognitive Radio

Η γνωσιακή ραδιοεπικοινωνία (Cognitive Radio – CR) είναι μια μορφή ασύρματης επικοινωνίας στην οποία ένας πομποδέκτης μπορεί να ανιχνεύσει έξυπνα ποια κανάλια επικοινωνίας χρησιμοποιούνται και ποια όχι, ώστε ακολούθως να μετακινείται σε μη κατειλημμένα κανάλια και να βελτιστοποιείται με τον τρόπο αυτό η χρήση του διαθέσιμου φάσματος, το οποίο αποτελεί έναν περιορισμένο και συνάμα πολύτιμο πόρο [103]. Υπό την έννοια αυτή, το CR μπορεί να παρατηρήσει το λειτουργικό περιβάλλον, να λαμβάνει αποφάσεις και να προχωρά σε αναδιαμόρφωση με βάση τις παρατηρήσεις αυτές. Ένα Δίκτυο Γνωσιακής Ραδιοεπικοινωνίας (Cognitive Radio Network - CRN) σχηματίζεται από πολλαπλά CR. Τα CRNs προσφέρουν υποστήριξη για ετερογένεια, δυνατότητα αναδιαμόρφωσης, αυτοοργάνωση, και διαλειτουργικότητα με τα υπάρχοντα δίκτυα, και έτσι προσφέρουν μια πολλά υποσχόμενη λύση για αντιμετώπιση καταστροφών και σοβαρών ζητημάτων δημόσιας ασφάλειας [37]. Σύμφωνα με την ίδια πηγή, η επόμενη γενιά ετερογενών ασύρματων δικτύων παρουσιάζει κάποια βασικά γνωρίσματα και συγκεκριμένα: (α)υψηλό ρυθμό μετάδοσης δεδομένων, (β)υποστηρίζει QoS, (γ)αρχιτεκτονική πολλαπλών επιπέδων, (δ)ενσωματώνει διαφορετικές ασύρματες τεχνολογικές λύσεις, (ε)SDR και τέλος (στ)CR.

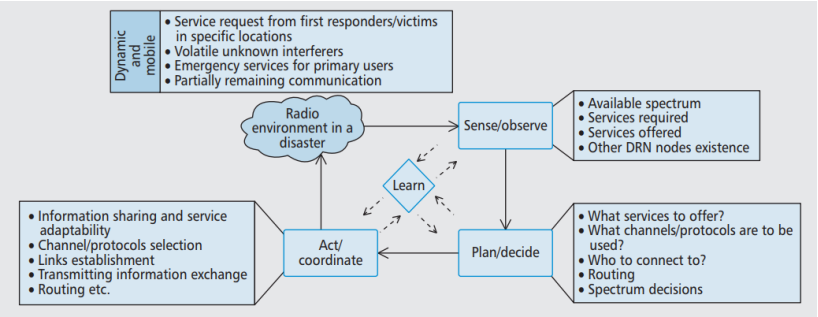
Ποιος είναι όμως ο τρόπος που το CR συνεισφέρει στα δίκτυα δημόσιας ασφάλειας; Από το 1999, που γεννήθηκε η ιδέα του CR έως σήμερα έχει σημειώσει σημαντική πρόοδο. Ουσιαστικά, αποτελεί μια υβριδική τεχνολογική λύση που βασίζεται στο SDR [103]. Το CR μπορεί να αλλάξει τις παραμέτρους του πομπού ή του δέκτη του, που βασίζονται στην αλληλεπίδραση με το περιβάλλον και μπορεί να λαμβάνει αποφάσεις με βάση τις διαθέσιμες πληροφορίες και τους προκαθορισμένους στόχους [37]. Από το ίδιο άρθρο προκύπτει ότι υπάρχουν βασικοί μηχανισμοί που λειτουργούν στο πλαίσιο του CR και καθορίζουν τη σχέση του με τα δίκτυα δημόσιας ασφάλειας. Οι λειτουργίες αυτές παράγουν αποτελέσματα ταυτόχρονα και παράλληλα και αλληλοτροφοδοτούνται για να επιτύχουν τη ζητούμενη προσαρμογή με το περιβάλλον. Οι βασικές λειτουργίες είναι (Εικόνα 41):

- Αίσθηση και παρατήρηση (Sense / Observe): Η παρατήρηση του περιβάλλοντος λειτουργίας οδηγεί σε εντοπισμό διαθέσιμου φάσματος. Μια μέθοδος ανίχνευσης του φάσματος αναλύεται στην εργασία των [104]. Πληροφορίες για το σύστημα λαμβάνονται με διάφορους τρόπους και συγκεκριμένα μέσω τοπικής ανίχνευσης, από μεμονωμένες συσκευές, συνεργατικά από δίκτυο συσκευών, από βάσεις δεδομένων, απομακρυσμένα μέσω σύνδεσης δικτύου. Η αίσθηση θεωρείται κρίσιμης σημασίας, καθώς μπορεί να συνεισφέρει την πολύτιμη πληροφόρηση σχετικά με τη διαθεσιμότητα του φάσματος.
- Σχεδιασμός και απόφαση (Plan / Decide): Με βάση τις πληροφορίες που ελήφθησαν από τη διαδικασία αίσθησης και παρατήρησης, το CR πρέπει στη συνέχεια να σχεδιάσει μια πορεία δράσης. Η απόφαση περιλαμβάνει την επιλογή κατάλληλης δρομολόγησης, ζώνης συχνοτήτων, πρωτοκόλλων διασύνδεσης, καναλιών, κ.λπ., ώστε ν` αποφασιστεί ποιες υπηρεσίες από τις διαθέσιμες πρέπει να έχουν προτεραιότητα στο πλαίσιο μιας καταστροφής.
- Πράξη και συντονισμός (Act / Coordinate): Μόλις ληφθούν οι αποφάσεις και ένα σχέδιο δράσης το σύστημα CR πρέπει να εκτελέσει με βάση αυτό το σχέδιο μοιράζοντας και ανταλλάσσοντας πληροφορίες.

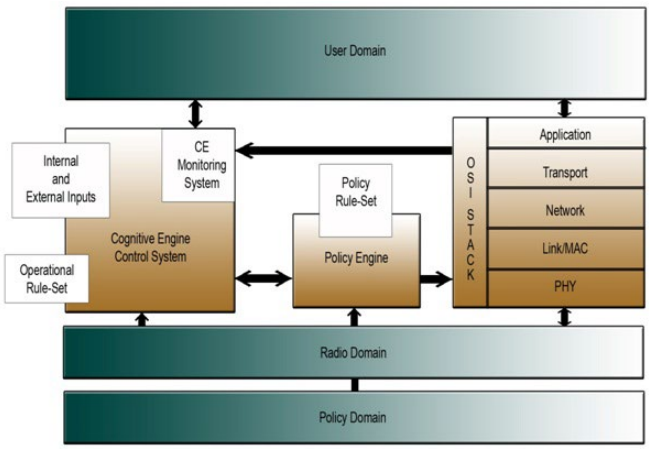
Καθ` όλη τη διάρκεια των ενεργειών – σταδίων που περιγράφηκαν, το σύστημα παράγει γνώση που τελεί σε διαρκή αλληλεπίδραση μ` αυτό, ανατροφοδοτώντας τη βέλτιστη λήψη αποφάσεων. Η τεχνολογία CR εξελίσσεται ήδη για χρήση σε στρατιωτικούς και εμπορικούς τομείς. Ωστόσο, σημαντικές από τις δυνατότητες που προσφέρει έχουν εφαρμογή στις κρίσιμες επικοινωνίες, τα δίκτυα δημόσιας ασφάλειας και αντιμετώπισης καταστροφών. Αυτό αποδεικνύεται εμπράκτως, καθώς σύμφωνα με την έρευνα που έκαναν οι [37], στο πλαίσιο του 7ου Πακέτου Στήριξης (FP-7) της Ευρωπαϊκής Ένωσης, αλλά και του Εθνικού Ιδρύματος Επιστημών (National Science Foundation – NSF) έχουν σχεδιαστεί και αναπτυχθεί

σημαντικά έργα και ειδικότερα αυτά που περιλαμβάνονται στον Πίνακας 9. Οι τρεις βασικές δυνατότητες που διαφοροποιούν το γνωστικό ραδιόφωνο είναι [103] (α) η γνώση, σύμφωνα με την οποία το CR κατανοεί το γεωγραφικό και επιχειρησιακό του περιβάλλον, (β) η αναδιαμόρφωση, σύμφωνα με την οποία το CR προσαρμόζει δυναμικά και αυτόνομα τις παραμέτρους του και (γ) η μάθηση, σύμφωνα με την οποία το CR μαθαίνει από την εμπειρία και πειραματίζεται με νέες διαμορφώσεις σε νέες καταστάσεις.

Σύμφωνα με την προσέγγιση που επιχειρείται από το [105], η αρχιτεκτονική του CR περιλαμβάνει δύο κύρια υποσυστήματα. Μια μονάδα που λαμβάνει αποφάσεις βασιζόμενη στις εισροές πληροφοριών που δέχεται και μια ευέλικτη μονάδα SDR. Βέβαια, είναι σημαντικό να σημειωθεί ότι αυτά τα υποσυστήματα δεν ορίζουν απαραιτήτως ένα μόνο τμήμα του εξοπλισμού, αλλά αντίθετα μπορούν να ενσωματώνουν στοιχεία που είναι κατανεμημένα σε ένα ολόκληρο δίκτυο. Η γνωστική μονάδα, χωρίζεται περαιτέρω σε δύο μέρη όπως φαίνεται στην Εικόνα 42. Στον «γνωστικό κινητήρα» που προσπαθεί να βρει μια λύση, ή να βελτιστοποιήσει έναν στόχο απόδοσης με βάση τις εισόδους που λαμβάνονται και καθορίζουν την τρέχουσα εσωτερική κατάσταση και το περιβάλλον λειτουργίας του ραδιοφώνου. Στη «μηχανή πολιτικής» που χρησιμοποιείται για να διασφαλιστεί ότι η λύση που παρέχεται από τη «γνωστική μηχανή» είναι σύμφωνη με τους ρυθμιστικούς κανόνες και άλλες πολιτικές εκτός του ραδιοφώνου.



Εικόνα 41. Βασικοί ραδιομηχανισμοί για δίκτυο αντιμετώπισης καταστροφών [37]



Εικόνα 42. Αρχιτεκτονική CRN [105]

Έργο	Διάρκεια	Πηγή	Στόχοι - Παρατηρήσεις
ABSOLUTE	2012-2015	[106]	Στόχος του προγράμματος ήταν η παροχή εφαρμογών για διαλειτουργική και συμβατή προς τα πίσω λύση επικοινωνίας, στο πλαίσιο μιας προσπάθειες τυποποίησης, επιτρέποντας τη γρήγορη υιοθέτηση των τεχνολογιών επικοινωνίας 4G για να βελτιωθεί η ετοιμότητα αποκατάστασης καταστροφών και διαχείρισης κρίσεων όλων των φορέων δημόσιας ασφάλειας στην Ευρώπη, αλλά και παγκοσμίως. Τα λειτουργικά στοιχεία και οι αντίστοιχες βελτιώσεις της αρχιτεκτονικής δικτύου βασίζονται στην ανάλυση των απαιτήσεων χρήστη / ενδιαφερομένων και στην υιοθέτηση ευρυζωνικού φάσματος για τη δημόσια ασφάλεια.
CORASAT[8]	2012-2015	[107]	Το έργο επιχείρησε να πετύχει τη διερεύνηση, ανάπτυξη και επίδειξη γνωστικών ραδιοφωνικών τεχνικών σε συστήματα δορυφορικής επικοινωνίας για κοινή χρήση φάσματος μεταξύ δορυφορικών και επίγειων συστημάτων. Στο πλαίσιο του έργου έγιναν 25 δημοσιεύσεις σε επιστημονικά συνέδρια, 6 δημοσιεύσεις σε περιοδικά και ένα κεφάλαιο βιβλίου, με αξιοσημείωτη την εργασία [108]. Επίσης, ο ETSI δημοσίευσε την τεχνική έκθεση [109], η οποία θεωρείται ένα σημαντικό ορόσημο στην τυποποίηση των σχετικών δραστηριοτήτων CR SatCom.
CREW	2010-2015	[110]	Το έργο στόχευσε στη δημιουργία μιας ανοιχτής ομοσπονδιακής πλατφόρμας δοκιμαστικής βάσης, η οποία διευκολύνει την πειραματική έρευνα για προηγμένες στρατηγικές ανίχνευσης φάσματος, γνωστικού ραδιοφώνου και γνωστικής δικτύωσης σε ζώνες με άδεια και χωρίς άδεια.
EULER	2009-2012	[111], [112], [113]	Το έργο είναι μια υλοποίηση με τεχνολογία SDR, το οποίο χρησιμοποιείται για την υποστήριξη της διαλειτουργικότητας μεταξύ συμβατικών τεχνολογιών ασύρματης επικοινωνίας όπως TETRA, WiMAX και δορυφορικών επικοινωνιών. Η κύρια πτυχή που διερευνήθηκε στο EULER είναι ο ορισμός μιας κοινής κυματομορφής που σέβεται τους περιορισμούς της αρχιτεκτονικής επικοινωνιών λογισμικού και εγγυάται τη μέγιστη φορητότητα στις πλατφόρμες SDR.
DITSEF[9]	2010-2013	[114]	Ένα ακόμη έργο που χρηματοδοτήθηκε από την Ευρωπαϊκή Ένωση με τίτλο «Ψηφιακές και καινοτόμες τεχνολογίες για την ασφάλεια και την αποτελεσματικότητα της λειτουργίας των πρώτων ανταποκριτών» (Ditsef). Ουσιαστικά, η προσπάθεια έγινε για την υποστήριξη των πρώτων ανταποκριτών μέσω ενός δικτύου αισθητήρων, συστημάτων εντοπισμού και επικοινωνίας, ιδιαίτερα σε περίπτωση μεγάλων πυρκαγιών. Η τεχνολογία αισθητήρων μπορεί να βοηθήσει στην προειδοποίηση έναντι κινδύνων όπως αέρια και τοξικές χημικές ουσίες, καθώς και σε σενάρια χαμηλής ορατότητας. Αυτό μπορεί στη συνέχεια να βελτιωθεί μέσω δικτύου εντοπισμού εσωτερικών χώρων, βελτιωμένης μετάδοσης δεδομένων ραδιοφώνου και τεχνολογίας διασύνδεσης ανθρώπου-μηχανής για τη βελτίωση της αποτελεσματικότητας και της ασφάλειας των πρώτων ανταποκριτών.
SALICE	2008-2010	[115]	Το έργο είχε ως στόχο να εντοπίσει τις λύσεις που μπορούν να υιοθετηθούν σε μια ενσωματωμένη επαναδιαμορφώσιμη συσκευή NAV/COM και να μελετήσει τη σκοπιμότητά της σε ρεαλιστικά σενάρια. Ο πρώτος στόχος του έργου SALICE είναι να ορίσει τα βασικά σενάρια και την αρχιτεκτονική του συστήματος για ολοκληρωμένα τεχνικές επικοινωνίας και εντοπισμού, συσκευές SDR NAV/COM, ενσωμάτωση HAPS στις υπηρεσίες διάσωσης, ετερογενείς λύσεις στον τομέα της επέμβασης.
EMPhAtiC[10]	2012-2015	[116]	Το έργο είχε ως στόχο την ανάπτυξη και επίδειξη της ικανότητας βελτιωμένων τεχνικών πολλαπλών φορέων για καλύτερη χρήση των υφιστάμενων ζωνών ραδιοσυχνοτήτων για την παροχή ευρυζωνικών υπηρεσιών δεδομένων σε συνύπαρξη με υπηρεσίες παλαιού τύπου στενής ζώνης. Σε αυτό θα αναπτυχθούν λύσεις βασισμένες σε κυψέλες και ad-hoc για PPDR.
CNS/EARS	Έως 2014	[117]	Ένα έργο του NSF, το οποίο είχε ως στόχο την ενίσχυση της πρόσβασης σε ραδιοφάσμα από γνωστικά και επαναδιαμορφώσιμα ασύρματα συστήματα. Συμπεριλαμβανομένης της φασματικής απόδοσης, των αναδιαμορφώσιμων ασύρματων συστημάτων, της ασφάλειας των ασύρματων σημάτων και των συστημάτων, της συνύπαρξης με παλαιού τύπου συστήματα, των ασύρματων συστημάτων ειδικού σκοπού με δοκιμές και των μετρήσεων, του οικονομικού μοντέλου για κοινή χρήση φάσματος, των τεχνικών διαχείρισης φάσματος, της αρχιτεκτονικής ραδιοφώνου δικτύου και της ενεργειακής απόδοσης και ισχυρές τεχνικές ανίχνευσης και κατανομής φάσματος. Πολλά έργα σε αυτό το σχήμα στοχεύουν σε ετερογενή σενάρια μεγάλης κλίμακας.
CNS/RSCRN	2011-2014	[118]	Το ακόμη έργο του NSF με τίτλο Robust and Secure Cognitive Radio Network - RSCRN εστιάζει στην αποτελεσματική συνύπαρξη δευτερευόντων χρηστών που κρίνονται απαραίτητοι για την επιτυχία των μελλοντικών γνωστικών δικτύων, με τους πρωτεύοντες χρήστες σε ίδιες ζώνες συχνοτήτων. Επιπλέον, αναφέρεται σε σχήματα διαχείρισης ραδιοφωνικών πόρων και στο σχεδιασμό χαμηλών κατανεμημένων αλγορίθμων για την αντιμετώπιση ζητημάτων ασφάλειας.

Πίνακας 9. Προγράμματα – έργα που σχετίζονται με το CR και το PPDR [37]

[8] https://cordis.europa.eu/project/id/316779

[9] https://cordis.europa.eu/project/id/225404

[10] https://cordis.europa.eu/project/id/318362

Οι εφαρμογές στις οποίες απαντάται το CR, ως ανατρεπτική τεχνολογία επόμενης γενιάς, είναι πολλές. Το CR μπορεί να βοηθήσει στην αντιμετώπιση προβλημάτων συνδεσιμότητας σε αγροτικές περιοχές, να βελτιστοποιήσει τις λειτουργίες RF για smartphone και συσκευές IoT, δίκτυα παράδοσης περιεχομένου, γνωστά και ως δίκτυα διανομής περιεχομένου, και γιγάντια ασύρματα hotspots. Κάλυψη δικτύου ραδιοσυχνοτήτων μεγάλου γεωγραφικού πλάτους, δίκτυα έκτακτης ανάγκης, ιατρικές εφαρμογές, πρόγνωση καιρού, έλεγχο κυκλοφορίας, κ.λπ. [103].

4.7 Device to Device

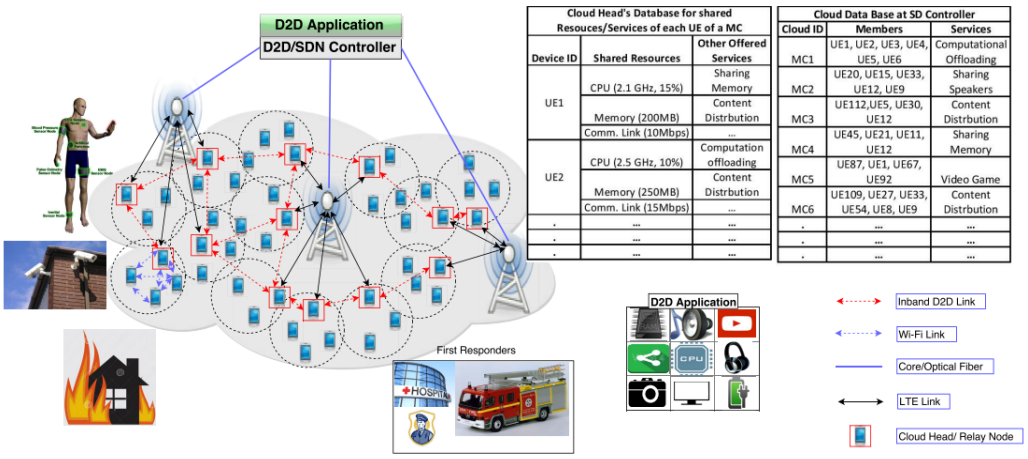
Στο 3GPP η επικοινωνία συσκευή προς συσκευή (Device to Device – D2D) ορίζεται ως επικοινωνία μεταξύ δύο UE σε φυσική εγγύτητα χρησιμοποιώντας διεπαφή αέρα 4G LTE για τη δημιουργία μιας άμεσης σύνδεσης χωρίς δρομολόγηση μέσω σταθμού βάσης (BS) και δικτύου πυρήνα (CN). Η επικοινωνία που βασίζεται στην εγγύτητα προσδιορίζει τις συσκευές που βρίσκονται στην περιοχή και επιτρέπει τη βελτιστοποιημένη επικοινωνία μεταξύ τους. Η συγκεκριμένη λειτουργία είναι αδιαπραγμάτευτη απαίτηση για δίκτυα δημόσιας ασφάλειας, καθώς υλοποιεί την επικοινωνία μεταξύ των επαγγελματιών χρηστών της δημόσιας ασφάλειας ακόμη και όταν η κάλυψη του δικτύου είναι μειωμένη, ή η συσκευή είναι εκτός δικτύου [53]. Μάλιστα, το 3GPP τυποποίησε τη συγκεκριμένη επικοινωνία ως υπηρεσία εγγύτητας (ProSe) [119], [120] η οποία σχεδιάστηκε για να καλύψει τόσο τις κρίσιμες όσο και τις εμπορικές απαιτήσεις. Σύμφωνα με την προσέγγιση των [53] τα χαρακτηριστικά υψηλού επιπέδου του δικτύου ProSe αποτελούνται από την ανακάλυψη ProSe και τη ρύθμιση άμεσης επικοινωνίας ProSe:

1) Η λειτουργία εντοπισμού ProSe προσδιορίζει συσκευές με δυνατότητα ProSe σε κοντινή απόσταση είτε στο επίπεδο του δικτύου ραδιοπρόσβασης (ανακάλυψη άμεσης εγγύτητας) είτε σε επίπεδο EPC. Στην άμεση ανακάλυψη εγγύτητας, το UE αναζητά αυτόνομα κοντινές συσκευές UE και απαιτεί να συμμετάσχουν στον εντοπισμό συσκευών μέσω μιας διαδικασίας περιοδικής μετάδοσης και λήψης σημάτων ανακάλυψης. Η άμεση ανακάλυψη μπορεί να λειτουργήσει τόσο υπό κάλυψη δικτύου όσο και εκτός κάλυψης και δεν αποκλείει τη βοήθεια δικτύου όταν είναι διαθέσιμη με διάφορους μηχανισμούς (ώθηση ή έλξη). Σε μια ανακάλυψη που βασίζεται στην ώθηση, το UE εκπέμπει την παρουσία του, ενώ αντίστοιχα στην έλξη το UE ζητά πληροφορίες σχετικά με συσκευές εγγύτητας με δυνατότητα εντοπισμού. Όταν ο εντοπισμός λαμβάνει χώρα σε επίπεδο EPC, το EPC είναι αυτό που καθορίζει την εγγύτητα των συσκευών UE και μια συσκευή UE επιτρέπεται να ξεκινήσει τη διαδικασία εντοπισμού αφού λάβει τις πληροφορίες στόχου της από το δίκτυο. Αυτό το σχήμα απαιτεί από το δίκτυο

να παρακολουθεί τις υποψήφιες συσκευές D2D UE, επωμιζόμενο τον φόρτο εντοπισμού και μειώνοντάς το αντίστοιχα από τα κινητά τερματικά.

2)Αφού ολοκληρωθεί η φάση της λειτουργίας που περιγράψαμε ήδη, η ρύθμιση άμεσης επικοινωνίας ProSe επιτρέπει τη δημιουργία μονοπατιών επικοινωνίας μεταξύ δύο ή περισσότερων UE με δυνατότητα ProSe που βρίσκονται σε εύρος άμεσης επικοινωνίας. Η διαδρομή άμεσης επικοινωνίας ProSe θα μπορούσε να χρησιμοποιεί E-UTRAN ή WLAN.

Η διαδικασία για τη ρύθμιση άμεσης επικοινωνίας δεν είναι τυποποιημένη από το 3GPP, ωστόσο στη βιβλιογραφία προτείνονται διάφορες διαδικασίες. Στο [121] προτείνεται η επικοινωνία D2D μέσω ενός πρωτοκόλλου, ενεργοποίησης των συσκευών των χρηστών με «φάρους» (beacon) και απλά τερματικά LTE που είναι διάσπαρτα στην περιοχή ενός μεγάλου γεγονότος, το οποίο βρίσκει εφαρμογή στην προσέγγιση που προτάθηκε στο πλαίσιο του έργου ABSOLUTE. Στο πλαίσιο του ίδιου έργου, οι [122] προτείνουν η κατεστραμμένη υποδομή να αντικατασταθεί από ένα 4G eNB (AeNB) το οποίο θα υποστηρίξει το δίκτυο από αέρα, καθώς θα βρίσκεται προσαρτημένο σε ένα μπαλόνι. Επίσης, στο [123] επιχειρείται μια προσπάθεια βελτίωσης των κενών κάλυψης που δημιουργούνται στις περιοχές των άκρων του κάθε κελιού ή εντός κτηρίων. Μάλιστα, στις δοκιμές που έγιναν το 99% των χρηστών που βρισκόταν εκτός κάλυψης επέτυχαν τη ζητούμενη απόδοση μετάδοσης εικόνας με επικοινωνία D2D. Στο [124] προτείνεται μια αρχιτεκτονική επικοινωνίας D2D, με χρήση κεντρικού ελεγκτή που επιτρέπει τη συνέχιση της απρόσκοπτης λειτουργία του δικτύου ακόμη και σε περίπτωση που η υποδομή του έχει υποστεί ζημία ή καταστραφεί ολοσχερώς. Στη συγκεκριμένη αρχιτεκτονική (Εικόνα 43) κάθε UE εκτελεί μια εφαρμογή D2D, χρησιμοποιώντας μια ιεραρχική προσέγγιση για τη δημιουργία cloud για κινητά. Ο κεντρικός ελεγκτής D2D/SDN «βλέπει» όλα τα mobile cloud της εμβέλειάς του, ενώ οι τοπικοί ελεγκτές (κεφαλές σύννεφων) γνωρίζουν τα UE της γειτονιάς τους.



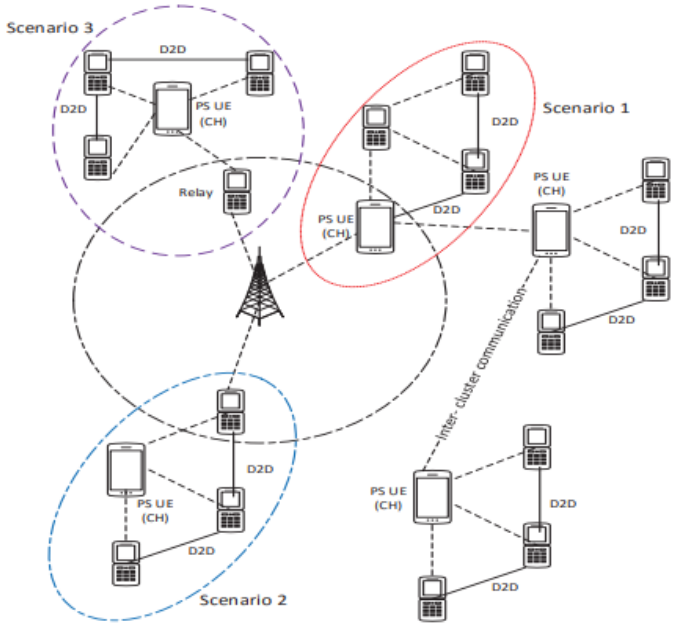
Εικόνα 43. Αρχιτεκτονική PSN βασισμένη σε D2D επικοινωνίες [124]

Συνάγεται λοιπόν ότι οι επικοινωνίες D2D μπορούν να χρησιμοποιηθούν για τη βελτίωση της απόδοσης των δικτύων δημόσιας ασφάλειας, καθώς τα UE που αναπτύσσονται επεκτείνουν την κάλυψη του δικτύου. Στο πλαίσιο αυτό στο [125] αναλύονται τρία διαφορετικά σενάρια, σε σχέση πάντοτε με τη θέση των UE ως προς την κυψέλη, όπως προκύπτει και στην Εικόνα 44. Στο [126] παρουσιάζεται μια κατηγοριοποίηση του D2D από την πλευρά του χρήστη, που περιλαμβάνει δύο σκέλη: (α)σε κάλυψη (In-coverage) και (β)εκτός κάλυψης (Out-of-coverage), όπως φαίνεται και στην Εικόνα 45. Στην ίδια βιβλιογραφική επισκόπηση και για κάθε μια από τις δύο αναφερόμενες ως άνω υποπεριοχές εξετάζεται το ζήτημα της ανακάλυψης συσκευών και της D2D επικοινωνίας. Όπως ήδη αναφέρθηκε, η ανακάλυψη συσκευών υποδηλώνει την ανακάλυψη κοντινών συσκευών για τη δημιουργία απευθείας συνδέσεων επικοινωνίας. Σε ένα κυψελοειδές δίκτυο τρεις παράγοντες καθορίζουν τα σχήματα ανακάλυψης συσκευών: (α) η αποτελεσματικότητα, η οποία δύναται να ορισθεί ως η πιθανότητα ανακάλυψης, (β) η ενεργειακή απόδοση και (γ) ο συντονισμός παρεμβολών που αφορά ουσιαστικά στη διαχείριση των πόρων του φάσματος. Αναφορικά δε με τις D2D επικοινωνίες, αυτές διακρίνονται σε δύο κύρια στοιχεία: (α) στη φασματική απόδοση, που περιλαμβάνει την κατανομή πόρων και την επιλογή D2D ή κυψελοειδούς επικοινωνίας, και (β) στην ενεργειακή απόδοση, η οποία με τη σειρά της περιλαμβάνει στοιχεία που αφορούν στον έλεγχο και κατανομή των πόρων, στη βελτιστοποίηση και στη μεταφορά ενέργειας.

Από την άλλη, χωρίς την παρουσία υποδομής δικτύου, η συσκευή έχει βασικό ρόλο. Τα συστήματα ανακάλυψης των συσκευών που γειτνιάζουν υφίστανται και στην περίπτωση αυτή, ωστόσο μπορούν να δημιουργηθούν προβλήματα που αφορούν σε παρεμβολές σε σύγκριση με τα δικτυοκεντρικά σχήματα. Το D2D UE στην περίπτωση αυτή και για την ανακάλυψη εγγύτητας έχει διττό ρόλο: (α) την αναγγελία και (β) την παρακολούθηση. Για την αναγγελία μεταδίδει περιοδικά μηνύματα εντοπισμού εγγύτητας, ενώ για την παρακολούθηση ακούει τα μηνύματα από τις ανακοινώσεις και απαντά σε αυτές.

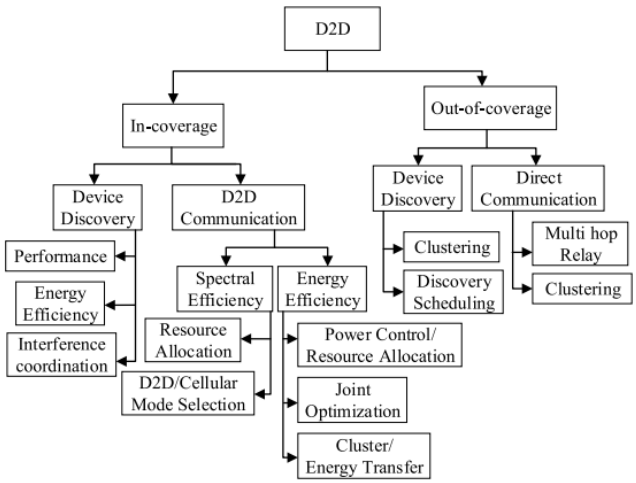
Στη μελέτη των [127] εξετάσθηκαν διεξοδικά ορισμένες από τις βασικές απαιτήσεις και τεχνολογικές προκλήσεις για τις προσεγγίσεις λύσεων που πρέπει να υπάρχουν προκειμένου να επιτραπεί στα δίκτυα LTE και ειδικότερα στις επικοινωνίες D2D ν` ανταποκρίνονται στο PPDR και στην Εθνική και Δημόσια Ασφάλεια (National Security and Public Safety – NSPS). Προτείνεται μια αρχιτεκτονική που βασίζεται στη διαδικασία ομαδοποίησης για το σχεδιασμό ενός συστήματος που ενσωματώνει κυψελοειδείς και ad hoc λειτουργίες, ανάλογα με τη διαθεσιμότητα των κόμβων υποδομής. Η αρχιτεκτονική αυτή προσέγγιση αποτέλεσε ένα τεχνολογικό στοιχείο της εξελισσόμενης τότε (2015) ιδέας του 5G στο πλαίσιο του ερευνητικού έργου METIS [11].

[11] https://metis-ii.5g-ppp.eu/index.html



Εικόνα 44. Μοντέλο δικτύου που εξετάζει 3 διαφορετικά σενάρια D2D επικοινωνίας [125]

Όπως αναφέρθηκε ήδη, το 3GPP, στις εκδόσεις 12 και 13 (Releases 12,13), ανάμεσα στα άλλα, επέτυχε βελτιώσεις στον τομέας των υπηρεσιών εγγύτητας, που επιτρέπουν την άμεση επικοινωνία D2D μεταξύ τερματικών σε κοντινή απόσταση μεταξύ τους, αλλά και στην ομαδική επικοινωνία, συμπεριλαμβανομένης της επικοινωνίας ένας προς πολλούς. Οι υπηρεσίες ProSe προσφέρουν σημαντικά πλεονεκτήματα. Κύριο εξ αυτών είναι η βελτιωμένη φασματική απόδοση, αφού ορισμένα κανάλια κυψελοειδούς συχνότητας αντικαθίστανται από άμεσες ζεύξεις. Περαιτέρω δε, η επικοινωνία D2D παρέχει υψηλότερο ρυθμό μεταφοράς δεδομένων με χαμηλότερες καθυστερήσεις από άκρο σε άκρο. Επίσης εξοικονομείται ενέργεια και ενισχύεται την αξιοποίηση των ραδιοφωνικών πόρων.



Εικόνα 45. Κατηγοριοποίηση επικοινωνιών D2D από την πλευρά του χρήστη [126]

Οι λειτουργίες, τα ενδεχόμενα, οι αρχιτεκτονικές, τα πρωτόκολλα επικοινωνίας στα διάφορα επίπεδα των υπηρεσιών εγγύτητας (ProSe) αναλύονται διεξοδικά στο 4ο κεφάλαιο του [58]. Όπως ήδη διεξοδικά έχει αναφερθεί, οι επικοινωνίες D2D εμπλέκονται ενεργά στα πέμπτης γενιάς δίκτυα κινητής τηλεφωνίας (5G) και σίγουρα αυτό έχει ως αποτέλεσμα υψηλή απόδοση, λιγότερη κατανάλωση ενέργειας και μείωση της καθυστέρησης [128]. Στο πλαίσιο της αναφερόμενης βιβλιογραφικής επισκόπησης έγινε συγκριτική μελέτη των προτεινόμενων τεχνικών ανακάλυψης συσκευών στις επικοινωνίες D2D και των προκλήσεων που το συγκεκριμένο ερευνητικό πεδίο εμφανίζει ειδικότερα αναφορικά με τα ζητήματα ασφάλειας και ιδιωτικότητας.

Σε κάθε περίπτωση, το πεδίο των τεχνολογιών επικοινωνίας D2D είναι ευρύτατο και παρουσιάζει σημαντικό ερευνητικό ενδιαφέρον. Απόδειξη αυτού είναι ότι πλείστες ερευνητικές προσπάθειες, που αναφέρθηκαν ήδη, αλλά και άλλες τόσες που δεν αποτυπώθηκαν στην παρούσα εργασία πραγματεύονται τα ζητήματα της επικοινωνίας συσκευής προς συσκευή και τις υπηρεσίες εγγύτητας των δικτύων δημόσιας ασφάλειας. Χαρακτηριστικό παράδειγμα δε αποτελεί το γεγονός ότι στο [126] προτείνεται ως λύση της υπερφόρτωσης του δικτύου, ή της βλάβης που έχει υποστεί η υποδομή του, από την πλευρά του χρήστη, η επικοινωνία D2D και από την πλευρά του δικτύου η ανάπτυξη των δυναμικών ασύρματων δικτύων (Dynamic Wireless Networks - DWNs).

4.8 M-MIMO

Η τεχνολογία Πολλαπλών Εισόδων – Πολλαπλών Εξόδων (Multiple Input Multiple Output - MIMO) σε ασύρματα δίκτυα επικοινωνίας ξεκίνησε από τη δεκαετία του 1990 και έφερε μια σημαντική αλλαγή στη φιλοσοφία της σχεδίασης των δικτύων αυτών. Το 3GPP πρόσθεσε για πρώτη φορά το MIMO στην 8η έκδοσή του (Release 8), η οποία αναφέρεται στο σχήμα κεραιών του MIMO και τους αυξημένους ρυθμούς μετάδοσης δεδομένων (ως 300 Mbps σε κατερχόμενη ζεύξη και 75 Mbps σε ανερχόμενη ζεύξη) όταν χρησιμοποιείται εύρος ζώνης 4×4 MIMO και 20 MHz [129].

Σύμφωνα με την ίδια πηγή, στις εκδόσεις 9 και 10 του 3GPP, έγιναν περαιτέρω βελτιώσεις της τεχνολογίας MIMO. Συγκεκριμένα, στην 9η έκδοση (Release 9) η διαμόρφωση δέσμης MIMO χρησιμοποιείται για την αύξηση της απόδοσης ακμών κυψέλης κατευθύνοντας τη δέσμη προς συγκεκριμένο UE με εκτίμηση θέσης στο eNB. Αντίστοιχα, στη 10η έκδοση (Release 10), επήλθαν βελτιώσεις της τεχνολογίας MIMO, καθώς πλέον το LTE-Advanced επιτρέπει έως και 8×8 MIMO σε κατερχόμενη ζεύξη και στην πλευρά UE επιτρέπει 4X4 στην κατεύθυνση ανοδικής ζεύξης. Περαιτέρω βελτιώσεις καταγράφηκαν στην 13η έκδοση

(Release 13), όπου εξετάσθηκε η χρήση συστημάτων MIMO υψηλής τάξης με έως και 64 θύρες κεραίας.

Επιπλέον, η τεχνολογία MIMO χρησιμοποιείται για δίκτυα Wi-Fi και την κινητή τηλεφωνία 4G, LTE και 5G σε ένα ευρύ φάσμα περιπτώσεων που περιλαμβάνει και τη δημόσια ασφάλεια. Μάλιστα, χρησιμοποιείται συχνά για επικοινωνίες υψηλού εύρους ζώνης όπου είναι σημαντικό να μην υπάρχουν παρεμβολές από συστήματα μικροκυμάτων ή ραδιοσυχνοτήτων. Τα συγκεκριμένα οφέλη το καθιστούν ιδανικό εργαλείο για τους πρώτους ανταποκριτές, που δεν μπορούν πάντα να βασίζονται σε δίκτυα κινητής τηλεφωνίας, τα οποία είναι ευάλωτα κατά τη διάρκεια μιας καταστροφής, είτε από διακοπές ρεύματος, είτε από βλάβες στην υποδομή, είτε από υπερφόρτωση [130].

Ως προς τα τεχνικής φύσεως θέματα, η τεχνολογία MIMO κατάφερε να εξασφαλίσει μεγαλύτερη αξιοπιστία και ταχύτητα στα ασύρματα δίκτυα επικοινωνίας, καθώς στηρίχθηκε στο φαινόμενο της πολυόδευσης του σήματος, που ουσιαστικά εξηγείται ως η ύπαρξη πολλών διαφορετικών καναλιών δια των οποίων μεταδίδεται η πληροφορία, η οποία αποδίδει μεγαλύτερη συνολική χωρητικότητα. Η τεχνολογία MIMO χρησιμοποιείται σε ασύρματα τοπικά δίκτυα (WLAN) και υποστηρίζεται από όλα τα ασύρματα προϊόντα με 802.11n. Μάλιστα, το πρωτόκολλο επικοινωνίας 802.11ax (Wi-Fi 6), έκανε ένα επιπλέον τεχνολογικό βήμα στην ασύρματη συνδεσιμότητα με τεχνολογικές λύσεις που θα βοηθήσουν στην εξάλειψη των περιορισμών που σχετίζονται με την προσθήκη περισσότερων συσκευών Wi-Fi σε ένα δίκτυο. Το Wi-Fi 7 βρίσκεται επί του παρόντος σε ανάπτυξη και αναμένεται να βγει στην κυκλοφορία το 2024.

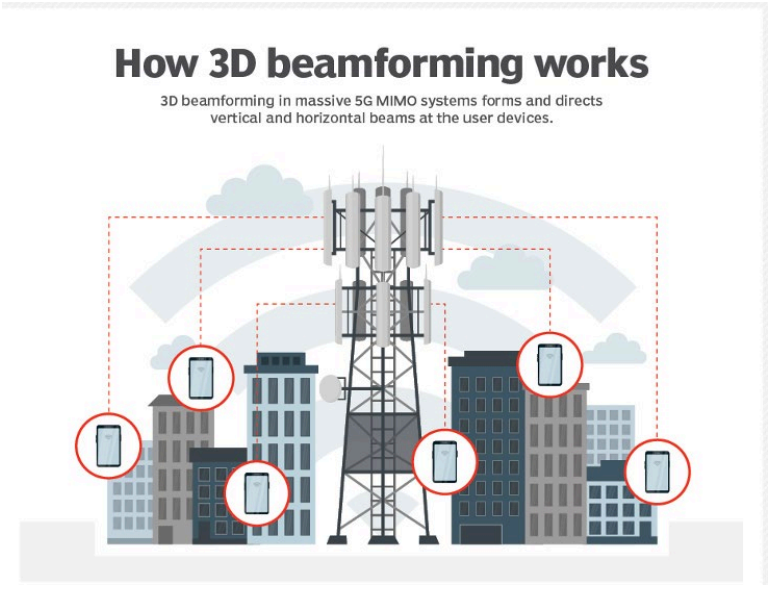
Η τεχνολογία MIMO βασίστηκε στην τεχνολογία κεραιών με διαφορετικές διαμορφώσεις και συγκεκριμένα:

- Πολλαπλή είσοδος, μονή έξοδος (Multiple Input Single Output - MISO)
- Μία είσοδος, πολλαπλή έξοδος (Single Input Multiple Output – SIMO)

Οι MISO και SIMO θεωρούνται τεχνολογικοί προκάτοχοι και σ` αυτές στηρίχθηκε η τεχνολογία MIMO. Επιπλέον, το MIMO λογίζεται ως μια ασύρματη τεχνολογία που έχει σχεδιαστεί να παρέχει καλύτερη εμπειρία επικοινωνίας σε περίπτωση υψηλής κινητικότητας των χρηστών εντός του δικτύου. Αποτελείται από πολλαπλές συστοιχίες κεραιών συνδεδεμένες με BS, οι οποίες μπορούν να εξυπηρετήσουν πολλούς χρήστες ταυτόχρονα. Το MIMO συνεχίζει να εξελίσσεται και αναβαθμίζεται μέσω της χρήσης του σε πολύ μεγάλες και σύνθετες νέες εφαρμογές, καθώς η σύγχρονη ασύρματη επικοινωνία φιλοξενεί περισσότερες κεραίες, δίκτυα και συσκευές. Ένα από τα χαρακτηριστικότερα τέτοια παραδείγματα είναι η ανάπτυξη της τεχνολογίας 5G. Αυτά τα τεράστια μαζικά συστήματα (massive 5G MIMO – M-MIMO) χρησιμοποιούν πολυάριθμες μικρές κεραίες για να

ενισχύσουν το εύρος ζώνης στους χρήστες και υποστηρίζουν περισσότερους χρήστες ανά κεραία [130]. Επιπλέον, για βέλτιστα αποτελέσματα εφαρμόζεται μια τεχνική διαχείρισης ραδιοσυχνοτήτων που μεγιστοποιεί την ισχύ του σήματος στον δέκτη εστιάζοντας τα δεδομένα εκπομπής σε συγκεκριμένους χρήστες, αντί για μια μεγάλη περιοχή. Με το 5G, η τρισδιάστατη (3D) διαμόρφωση δέσμης σχηματίζει και κατευθύνει κάθετες και οριζόντιες δοκούς στον χρήστη, όπως φαίνεται στην Εικόνα 46 [130]. Όπως αναφέρθηκε ήδη, η τεχνολογία MIMO βασίζεται σε πολλαπλές κεραίες για την ταυτόχρονη μετάδοση πολλαπλών ροών δεδομένων σε συστήματα ασύρματων επικοινωνιών. Όταν το MIMO χρησιμοποιείται για την επικοινωνία με πολλά τερματικά ταυτόχρονα, αναφερόμαστε σε MIMO πολλαπλών χρηστών, ή όπως αλλιώς το ονομάζουμε (Multiuser MIMO - MU-MIMO). Το MU-MIMO στα κυψελωτά συστήματα φέρνει βελτιώσεις και συγκεκριμένα [131]:

- αυξημένο ρυθμό δεδομένων, επειδή όσο περισσότερες κεραίες, τόσο περισσότερες ανεξάρτητες ροές δεδομένων αποστέλλονται και περισσότερα τερματικά εξυπηρετούνται ταυτόχρονα.
- ενισχυμένη αξιοπιστία, γιατί όσο περισσότερες κεραίες τόσο πιο ευδιάκριτες διαδρομές έχει το ραδιοφωνικό σήμα.
- βελτιωμένη ενεργειακή απόδοση, εκ της δυνατότητας που έχει ο BS να εστιάζει την ενέργεια που εμπέμπει στις περιοχές που γνωρίζει ότι βρίσκονται οι τερματικές συσκευές.
- μειωμένες παρεμβολές, επειδή ο σταθμός βάσης μπορεί σκόπιμα να αποφύγει τη μετάδοση σε κατευθύνσεις όπου οι παρεμβολές θα ήταν επιβλαβείς.



Εικόνα 46. Τρισδιάστατη διαμόρφωση δέσμης σε M-MIMO 5G [130]

Τα ως άνω αποτελούν τα γενικά οφέλη της τεχνολογίας MU-MIMO για τις ασύρματες επικοινωνίες, η οποία ωριμάζει και ενσωματώνεται στα πρότυπα ασύρματης ευρυζωνικότητας όπως το 4G, LTE και το LTE-A, στα οποία ήδη αναφερθήκαμε. Με όσες περισσότερες κεραίες είναι εξοπλισμένος ο σταθμός βάσης (ή τα τερματικά), τόσο καλύτερη απόδοση θα έχουν [131]. Μάλιστα, η απόδοση αυτή βελτιστοποιείται για τη λειτουργία διπλής όψης διαίρεσης χρόνου (Time Division Duplex - TDD), που χρησιμοποιείται στην τεχνολογία M-MIMO, σε αντίθεση με το σύστημα διαίρεσης συχνότητας (Frequency Division Duplex – FDD) που χρησιμοποιείται στο 4G MIMO [130].

Στη βιβλιογραφία, η τεχνολογία M-MIMO απαντάται με πολλά διαφορετικά ονόματα και συγκεκριμένα: Συστήματα Κεραίας Μεγάλης Κλίμακας (Large-Scale Antenna Systems), Πολύ Μεγάλο MIMO (Very Large MIMO), Υπερ MIMO (Hyper MIMO) και MIMO Πλήρων Διαστάσεων (Full-Dimension MIMO). Όλα είναι προσδιοριστικά του ρόλου της αναφερόμενης τεχνολογίας, καθώς η βασική ιδέα πίσω από το M-MIMO είναι να αποκομίσουμε όλα τα οφέλη του συμβατικού MIMO, αλλά σε πολύ μεγαλύτερη κλίμακα. Με τον τρόπο αυτό υφίσταται δυνατότητα ανάπτυξης μελλοντικών ευρυζωνικών δικτύων (σταθερών και κινητών) που θα είναι ενεργειακά αποδοτικά, ασφαλή και στιβαρά και θα χρησιμοποιούν αποτελεσματικά το φάσμα. Ως εκ τούτου, αποτελεί ένα εργαλείο για τη μελλοντική υποδομή της ψηφιακής κοινωνίας που θα συνδέει το IoT, το Cloud, ή άλλες υποδομές δικτύου και δυνητικά θα υποστηρίξει δίκτυα δημόσιας ασφάλειας ή κρίσιμων επικοινωνιών.

Τα M-MIMO έχουν πλήθος πλεονεκτημάτων, που έπειτα από όσα αναφέρθηκαν ήδη συνοψίζονται στ` ακόλουθα:

- Υψηλότερος ρυθμός δεδομένων, υψηλή QoS, δέκα φορές υψηλότερη χωρητικότητα και εκατό φορές βελτιωμένη ενεργειακή απόδοση, καθώς η ευρεία κάλυψη που υποστηρίζεται βοηθά στην υποστήριξη μεγάλου αριθμού συνδρομητών ανά κελί, ενώ σημαντικό ρόλο διαδραματίζουν η ύπαρξη πολλαπλών κεραιών και η τεχνική της Χωρικής Πολυπλεξίας (Spatial Multiplexing).
- Λόγω της εφαρμογής προηγμένων αλγορίθμων στην επεξεργασία σήματος που λαμβάνεται από πολλαπλές κεραίες, αλλά και της τεχνικής BF στην οποία αναφερθήκαμε ήδη, επιτυγχάνεται μείωση του ποσοστού εσφαλμένων bit (Bit Error Rate - BER) και επέκταση κάλυψης, αντίστοιχα.
- Δυνατότητα κατασκευής υποδομής του με φθηνά εξαρτήματα χαμηλής κατανάλωσης
- Σημαντική μείωση λανθάνοντος χρόνου στη διεπαφή αέρα, καθώς αποφεύγεται η εξασθένηση του σήματος και οι καθυστερήσεις διάδοσης

- Αυξημένη ευρωστία και ασφάλεια, είτε από κινδύνους που προέρχονται από ακούσιες ανθρωπογενείς παρεμβολές, είτε από σκόπιμη εμπλοκή. Χαρακτηριστικό παράδειγμα της συγκεκριμένης ωφέλειας αποτελούν τα γεγονότα του 2011 στο Γκέτεμπεργκ της Σουηδίας, όπου σε διαδήλωση που έλαβε χώρα κατά τη διάρκεια Συνόδου Κορυφής, οι διαδηλωτές χρησιμοποίησαν έναν παρεμβολέα, εγκατεστημένο σε παρακείμενο διαμέρισμα και πέτυχαν σημαντικότατο επικοινωνιακό πλήγμα, καθώς σε κρίσιμες στιγμές των ταραχών που ακολούθησαν οι 700 και πλέον αστυνομικοί αντιμετώπισαν δυσκολίες επικοινωνίας [131].
- Το σύστημα βασισμένο σε M-MIMO υιοθετείται ευρέως στα τελευταία ασύρματα πρότυπα (WLAN, WiMAX, LTE, LTE-A, κ.λπ.)

Παράλληλα, υπάρχουν και ορισμένα μειονεκτήματα, τα οποία αφορούν:

- Οι απαιτήσεις πόρων και η πολυπλοκότητα του υλικού είναι ιδιαίτερα υψηλές. Κάθε κεραία απαιτεί μεμονωμένες μονάδες RF για επεξεργασία ραδιοφωνικών σημάτων και ενισχυμένο τσιπ DSP για την εκτέλεση προηγμένων αλγορίθμων επεξεργασίας μαθηματικών σημάτων.
- Οι πόροι υλικού αυξάνουν τις απαιτήσεις ισχύος. Η μπαταρία εξαντλείται πιο γρήγορα καθώς η επεξεργασία σύνθετων και υπολογιστικών αλγορίθμων απαιτεί περισσότερη ενέργεια. Αυτό μειώνει τη διάρκεια ζωής της μπαταρίας των συσκευών που βασίζονται σε MIMO
- Τα συστήματα βασισμένα στο MIMO κοστίζουν υψηλότερα σε σύγκριση με το σύστημα με βάση μία κεραία, λόγω της αυξημένης ζήτησης υλικού και προηγμένων λογισμικών.

4.9 Millimetre wave (mmWave)

Οι συχνότητες άνω των 6 GHz, συμπεριλαμβανομένων των ζωνών κυμάτων χιλιοστών (millimeter waves - mmWaves), είναι ενδιαφέρουσες καθώς περιλαμβάνουν σημαντικά περισσότερο φάσμα από την τρέχουσα κατανομή κυψελωτών δικτύων. Η τεχνολογία mmWave αντιπροσωπεύει μια φιλόδοξη λύση για τα δίκτυα επικοινωνιών δημόσιας ασφάλειας, η οποία βασίζεται στο ανεκμετάλλευτο φάσμα που οδηγεί σε μειωμένη συμφόρηση δικτύου και υψηλούς ρυθμούς δεδομένων. Ωστόσο, η επικοινωνία σε τέτοιες συχνότητες αποτελεί ακόμη ένα ανεξερεύνητο πεδίο και εμφανίζει τεράστιες τεχνολογικές προκλήσεις [132].

Όπως εκτενώς αναφέρθηκε στο κεφάλαιο 4.4 το 5G τυποποιήθηκε για πρώτη φορά από το 3GPP στην 15η έκδοσή του (Release 15), στα μέσα του 2018. Μεταγενέστερα και έως τις αρχές του 2020 ολοκληρώθηκε η κυκλοφορία της 16ης έκδοσης (Release 16), χρονιά που το 5G εγκρίθηκε ως ITU IMT-2020 πρότυπο, ενώ τα στάδια ανάπτυξης της 17ης έκδοσης (Release 17) προκύπτουν αναλυτικά από την Εικόνα 33. Εκτός από την αποτελεσματική χρήση του φάσματος κάτω των 6 GHz, οι εκδόσεις 15 και 16 παρέχουν επίσης τις βασικές λειτουργίες για την υποστήριξη της τεχνολογίας mmWave. Προηγουμένως, η χρήση ζωνών συχνοτήτων πολύ πάνω από τα 6 GHz θεωρούνταν ακατάλληλη για κινητές επικοινωνίες λόγω της μεγάλης απώλειας διάδοσης και της ευκολίας με την οποία μπλοκάρονται τα σήματα από το ανθρώπινο σώμα καθώς και από δομικά υλικά και φύλλα. Ενώ αυτές οι προκλήσεις περιορίζουν την ανάπτυξη mmWave, η νέα τεχνολογία κεραίας μας επιτρέπει να εξερευνήσουμε διαφορετικά σενάρια ανάπτυξης και να κατανοήσουμε καλύτερα τα χαρακτηριστικά του καναλιού και τη διάδοση του σήματος [133].

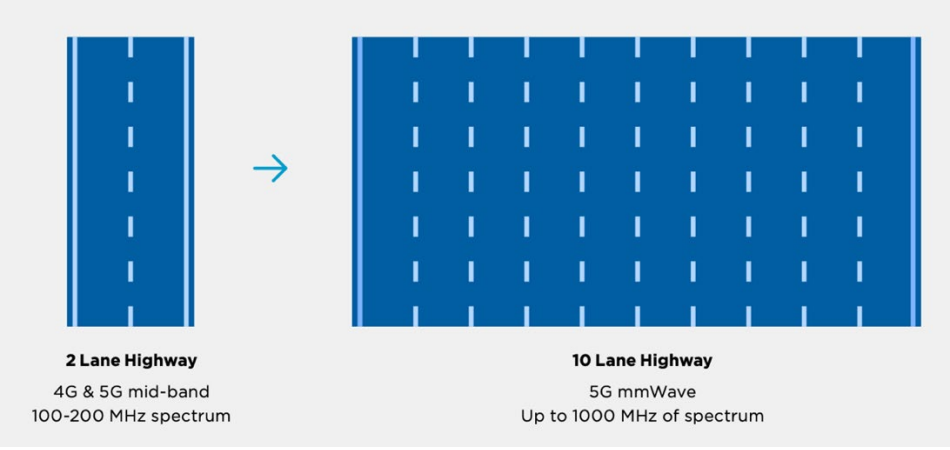
Οι καινοτόμες τεχνολογίες mmWave και τα δίκτυα 5G mmWave προσφέρουν το επίπεδο ανθεκτικότητας, ευελιξίας, εμβέλειας και εύρους ζώνης που απαιτείται για τις σύγχρονες λειτουργίες δημόσιας ασφάλειας, καθώς εμφανίζουν ιδιαιτέρως βελτιωμένα χαρακτηριστικά ασφαλείας και προσφέρουν υψηλή απόδοση για την υποστήριξη εφαρμογών, τόσο σε προαστιακές, όσο και σε αγροτικές περιοχές [134]. Είναι χαρακτηριστικό ότι ενώ η χαμηλή (κάτω από 1 GHz) και η μεσαία ζώνη (1-7 GHz) παρέχουν κάλυψη ευρείας περιοχής, δεν μπορούν να ανταγωνιστούν τη χωρητικότητα του 5G mmWave. Το εύρος συχνοτήτων mmWave μπορεί να υποστηρίξει ταχύτητες gigabit για κάθε χρήστη και επιτρέπει περισσότερους χρήστες (Εικόνα 47). Το 5G mmWave αναφέρεται στο υψηλότερο εύρος ραδιοσυχνοτήτων (πάνω από περίπου 24 GHz) που υποστηρίζεται από το 5G. Την παρούσα χρονική συγκυρία υπάρχουν σε εξέλιξη εμπορικές αναπτύξεις 5G mmWave στα 26 GHz (ΗΠΑ), 26 GHz (Ασία, Ευρώπη), 38 GHz (Κίνα, ΗΠΑ) και 47 GHz (ΗΠΑ) [134].

Τα πλεονεκτήματα του mmWave 5G καθιστούν αυτό ως έναν από τους ισχυρότερους υποψηφίους για μελλοντικούς τομείς κινητής ασύρματης επικοινωνίας [133]:

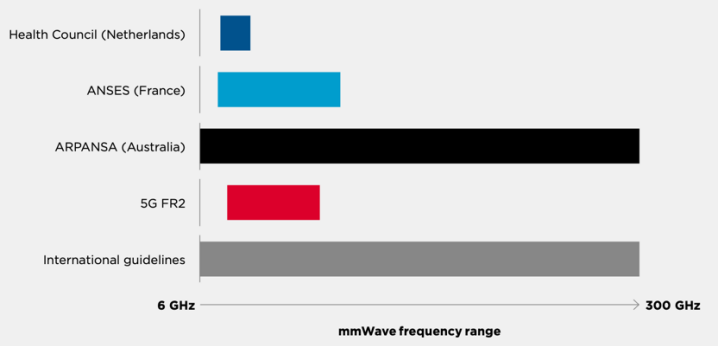
- Παρέχει περισσότερο εύρος ζώνης για να φιλοξενήσει περισσότερους συνδρομητές. Η χωρητικότητα αποδίδει πάνω από 20 φορές τη χωρητικότητα των σημερινών κυψελωτών δικτύων κυψελών [135].
- Το στενό εύρος ζώνης στο εύρος χιλιοστών το καθιστά κατάλληλο για χρήση με μικρά κελιά.
- Η κάλυψη δεν περιορίζεται στη γραμμή όρασης επειδή η κύρια διαδρομή διασποράς είναι εφικτή.

- Η λειτουργία ανίχνευσης καναλιών χρησιμοποιείται για την εξέταση διαφορετικών τύπων απώλειας συχνότητας mmWave προκειμένου τα δίκτυα 5G να λειτουργούν καλά.
- Πολλές κεραίες συσκευάζονται σε μικρότερα μεγέθη λόγω του φυσικώς μικρότερου μεγέθους των κεραιών τους.
- Το δίκτυο 5G mmWave υποστηρίζει backhaul πολλαπλών Gigabit έως 400 μέτρα και κινητή πρόσβαση έως 200-300 μέτρα.

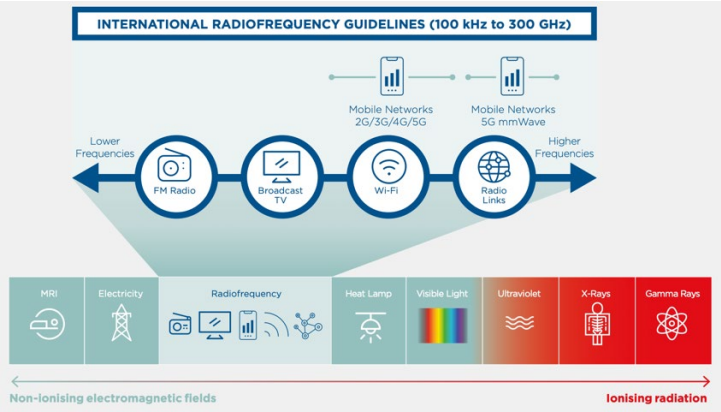
Μια σημαντική συζήτηση έχει ξεκινήσει στην επιστημονική κοινότητα, αναφορικά με τις επιπτώσεις στην υγεία του ανθρώπου από τη χρήση της τεχνολογία mmWave. Στο πλαίσιο αυτό έχουν γίνουν και εξακολουθούν να γίνονται αρκετές έρευνες. Στην επισκόπηση που επιχείρησαν οι [136] συμπεριλήφθηκαν και αξιολογήθηκαν 107 πειραματικές μελέτες του πεδίου, από τις οποίες προέκυψαν χρήσιμα συμπεράσματα, ενώ στο [134] έγινε εκτενής αναφορά στον τρόπο αντιμετώπισης του θέματος από τους Οργανισμούς Υγείας της Ολλανδίας, της Γαλλίας, της Αυστραλίας και των Η.Π.Α.. Χαρακτηριστικό είναι ότι βασισμένες σε διάφορες έρευνες και μελέτες αναθεωρήσανε το εύρος του ηλεκτρομαγνητικού πεδίο ραδιοσυχνοτήτων (Radiofrequency Electromagnetic Field - RF-EMF) σχετικά με το 5G mmWave. Όπως φαίνεται στην Εικόνα 48, οι υπηρεσίες των Χωρών αυτών ακολούθησαν διαφορετικές προσεγγίσεις για τον καθορισμό των περιοχών συχνοτήτων που χρησιμοποιούν. Ωστόσο, καμία από τις υπηρεσίες δεν βρήκε ενδείξεις ότι οι συχνότητες mmWave είναι πιο επικίνδυνες από άλλες ζώνες, αλλά διαφέρουν στην εκτίμησή τους για την ισχύ των διαθέσιμων στοιχείων ως βάση για τη χρήση συχνοτήτων mmWave για 5G. Σε κάθε περίπτωση και με δεδομένο ότι οι έρευνες στο συγκεκριμένο πεδίο βρίσκονται σε πρώιμο στάδιο, δεν υπάρχουν σαφή και ασφαλή συμπεράσματα και εκτιμάται ότι τέτοια θα προκύψουν σε αρκετά χρόνια μετά. Από την ίδια πηγή στην Εικόνα 49 προκύπτει μια αποτύπωση του ηλεκτρομαγνητικού φάσματος γενικότερα και του 5G mmWave.



Εικόνα 47. Το 5G mmWave παρέχει σημαντική αύξηση χωρητικότητας με πρόσθετο φάσμα [134]



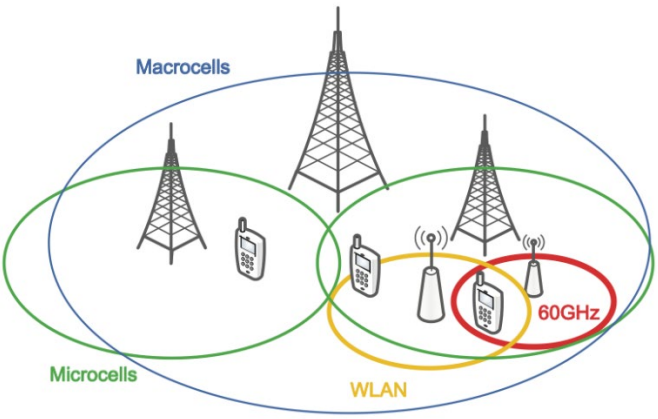
Εικόνα 48. mmWave συχνοτήτων κυμάτων που χρησιμοποιούνται από ορισμένες χώρες [134]



Εικόνα 49.Το ηλεκτρομαγνητικό φάσμα 5G mmWave και άλλων σημάτων ραδιοφώνου

Για την πλήρη εκμετάλλευση των δυνατοτήτων των επικοινωνιών mmWave, συμπεριλαμβανομένων των ολοκληρωμένων κυκλωμάτων και του σχεδιασμού συστημάτων, της διαχείρισης παρεμβολών, της επαναχρησιμοποίησης χώρου, του αντιμπλοκαρίσματος και του δυναμικού ελέγχου, οι [137] πραγματοποίησαν μια έρευνα για τις υπάρχουσες λύσεις και πρότυπα και πρότειναν κατευθυντήριες γραμμές σχεδιασμού σε αρχιτεκτονικές και πρωτόκολλα για επικοινωνίες mmWave. Χαρακτηριστικό παράδειγμα πρότασης αρχιτεκτονικής που χρησιμοποιεί αποδοτικά διαφορετικές τεχνολογίες επικοινωνίες και δημιουργεί ένα ετερογενές δίκτυο επικοινωνίας αποτελεί αυτό της Εικόνα 50.

Ένα από τα βασικά προβλήματα της τεχνολογίας mmWave στην αποδοτική υλοποίηση δικτύων είναι ότι λόγω του μικρού εύρους διάδοσης των κυμάτων χιλιοστού, απαιτείται μεγάλος αριθμός σημείων ραδιοπρόσβασης για την παροχή αξιόπιστης κάλυψης, γεγονός που αυξάνει το κόστος υποδομής. Μια από τις βασικές λύσεις για την αντιμετώπιση της συγκεκριμένης πρόκλησης των ασύρματων επικοινωνιών υψηλού εύρους ζώνης, που προτάθηκε από τους [138] είναι η μετάδοση σημάτων ραδιοσυχνοτήτων μεταξύ των κεντρικών (ή σημείων ελέγχου) και των σημείων ραδιοπρόσβασης (ή των απομακρυσμένων μονάδων κεραίας) με χρήση οπτικών ινών.



Εικόνα 50. Ετερογενές δίκτυο που περιλαμβάνει microcells, microcells WLANs, picocells σε 60GHz

4.10 Internet of Things

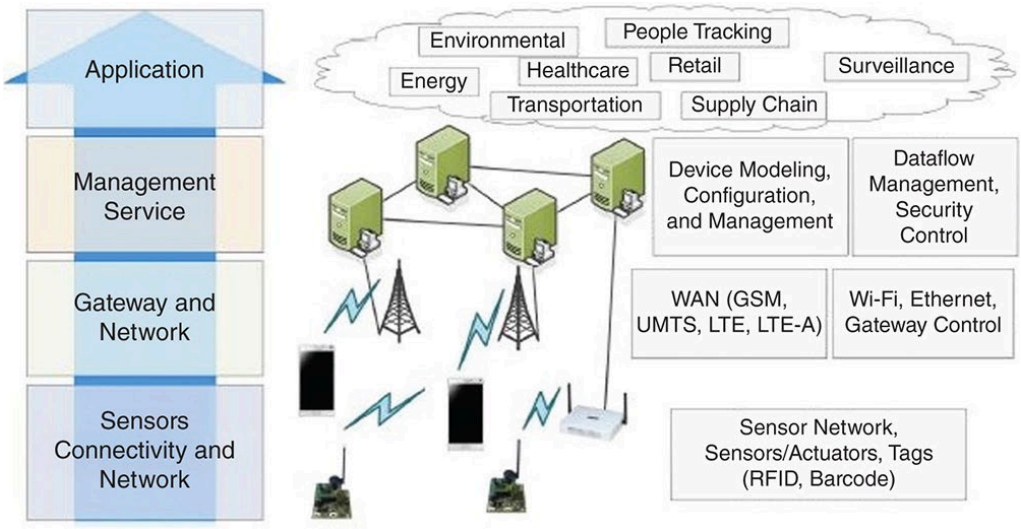
Το IoT αντιπροσωπεύει τη σύγκλιση πολλών διεπιστημονικών τομέων: δικτύωση, ενσωματωμένο υλικό, ραδιοφάσμα, φορητοί υπολογιστές, τεχνολογίες επικοινωνίας, αρχιτεκτονικές λογισμικού, τεχνολογίες ανίχνευσης, ενεργειακή απόδοση, διαχείριση πληροφοριών και ανάλυση δεδομένων. Το IoT επιτρέπει σε ετερογενή φυσικά αντικείμενα να μοιράζονται πληροφορίες και να συντονίζουν αποφάσεις. Το IoT μεταμορφώνει τον τρόπο με τον οποίο αναπτύσσονται και διανέμονται τα προϊόντα και οι υπηρεσίες, καθώς και τον τρόπο διαχείρισης και συντήρησης των υποδομών, επαναπροσδιορίζοντας την αλληλεπίδραση μεταξύ ανθρώπων και μηχανών [139]. Οι οργανισμοί των πρώτων ανταποκριτών μπορούν να επωφελούνται τις βελτιωμένες λειτουργίες του IoT που περιγράφονται παραπάνω [140]. Στο πλαίσιο αυτό έχουν έχουν υλοποιηθεί συστήματα που βασίζονται στο διαδίκτυο των πραγματων και αφορούν στη δημόσια ασφάλεια. Χαρακτηριστικά παραδείγματα τέτοιων υλοποιήσεων θα δούμε στη συνέχεια και συγκεκριμένα καταχωρίστηκαν στον Πίνακας 24 του κεφαλαίου 5.2.1.3.2. [52].

Αν και τα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks - WSNs) είναι ευρέως διαδεδομένα στη διαχείριση καταστροφών, δεν διαθέτουν πολλές κοινωνικο-τεχνο-οικονομικές προοπτικές, καθώς είναι θεμελιωδώς προσανατολισμένα στην επίλυση ενός συγκεκριμένου προβλήματος. Επιπλέον, υπάρχουν ζητήματα που δεν επιλύονται αποδοτικά από τα συγκεκριμένα δίκτυα, με κυριότερα εξ αυτών την αδυναμία διαχείρισης ετερογενών ενσωματωμένων συσκευών (διαφορετικοί επεξεργαστές, χώροι μνήμης, λειτουργικά συστήματα, κ.λπ.), ετερογενών πρωτοκόλλων (ανακάλυψη, δεδομένα, υποδομή, σημασιολογία, επικοινωνία και ασφάλεια), την παροχή υπηρεσιών ανάλυσης, την πρόσβαση πραγματικού χρόνου, τη διαλειτουργικότητα μεταξύ ενεργοποιημένων συσκευών, κ.αλ.. Από την άλλη πλευρά, το IoT έχει αποδειχθεί ότι είναι θεμελιωδώς ικανό να παρέχει πιο σημαντικές, επεκτάσιμες και ενεργειακά αποδοτικές λύσεις σε διάφορα προβλήματα στη

διαχείριση καταστροφών και στην αντιμετώπιση των συνεπειών αυτών, που αφορούν κατά μείζονα λόγο την έγκαιρη προειδοποίηση, την άμεση ενημέρωση, την ανάλυση δεδομένων, τη επίγνωση της κατάστασης, την απομακρυσμένη παρακολούθηση, τις αναλύσεις σε πραγματικό χρόνο και τον εντοπισμό θυμάτων. Στην έννοια του IoT εντάσσονται μια σειρά από πρωτόκολλα επικοινωνίας που εμπλέκονται ενεργά στην υλοποίηση αντίστοιχων εφαμρογών, στα οποία θα αναφερθούμε διεξοδικά στη συνέχεια [141].

Ο ταχύτατα αναπτυσσόμενος κλάδος του διαδικτύου των πραγματων και η όλο και αυξανόμενη εμπλοκή του στην τεχνολογική καθημερινότητα των ανθρώπινων δραστηριοτήτων έχουν επηρεάσει, όπως ήταν αναμενόμενο, και τον κλάδο της δημόσιας ασφάλειας. Σύμφωνα με την Juniper Research[12], οι έξυπνες πόλεις, οι οποίες έχουν ως δομικό στοιχείο το IoT, μπορεί να δουν βελτίωση στους χρόνους απόκρισης έκτακτης ανάγκης έως και 15% και μείωση των βίαιων εγκλημάτων έως και 10% [142]. Το IoT αποτελεί ένα σημαντικό στοιχείο υποστήριξης του 5G, καθώς πολυάριθμες μηχανές, συσκευές και αισθητήρες σε επικοινωνία και αλληλεξάρτηση μεταξύ τους, αυτοματοποιούν διαδικασίες, ανταλλάσσοντας πληροφορίες, σε διαστρωμάτωση επιπέδων, όπως προκύπτει στην Εικόνα 51. Στη βάση της συγκεκριμένης αρχιτεκτονικής είναι το επίπεδο της συλλογής των πληροφοριών, μέσω των αισθητήρων και της συνδεσιμότητας. Το επίπεδο αυτό τροφοδοτεί το επίπεδο του δικτύου, το οποίο με τη σειρά του ενημερώνει το επίπεδο διαχείρισης, για να φτάσουμε έτσι στο επίπεδο εφαρμογών. Αυτή είναι μια γενική εποπτική εικόνα της αρχιτεκτονικής των εφαμρογών IoT [143], [51]. Ωστόσο, η συγκεκριμένη αρχιτεκτονική αποδίδει μόνο μια γενική εικόνα της ιδέας υλοποίησης των εφαρμογών που στηρίζοναται στο διαδίκτυο των πραγματων, καθώς έως σήμερα δεν έχει προτυποποιηθεί μια απολύτως δεσμευτική αρχιτεκτονική. Είναι σύνηθες λοιπόν στη βιβλιογραφία να συναντούμε διαφορετικές οπτικές της αρχιτεκτονικής σχετικά με το IoT. Τούτο γίνεται σαφές από διάφορες εργασίες [140], [144], ενώ με στόχο να συγκεραστούν κατά το δυνατόν οι διαφορετικές οπτικές και να υπάρξει μια τεχνολογική και σχεδιαστική σύγκλιση, από την Κοινοτική Υπηρεσία Πληροφοριών Έρευνας και Ανάπτυξης (Community Research and Development Information Service - CORDIS) στο πλαίσιο του 7ου Προγράμματος Πλαισίου (Seven Framework Programme – 7FP), από 1-9-2010 έως 30-11-2013, υλοποιήθηκε το έργο με τίτλο Αρχιτεκτονική του Διαδικτύου των Πραγμάτων (Internet of Things Architecture), στο οποίο εκτός των άλλων συμμετείχε και η χώρα μας και το οποίο είχε ως στόχο να προτείνει τη δημιουργία ενός αρχιτεκτονικού μοντέλου αναφοράς μαζί με τον ορισμό ενός αρχικού συνόλου βασικών δομικών στοιχείων λειτουργίας του IoT [145].

[12] https://www.juniperresearch.com/home



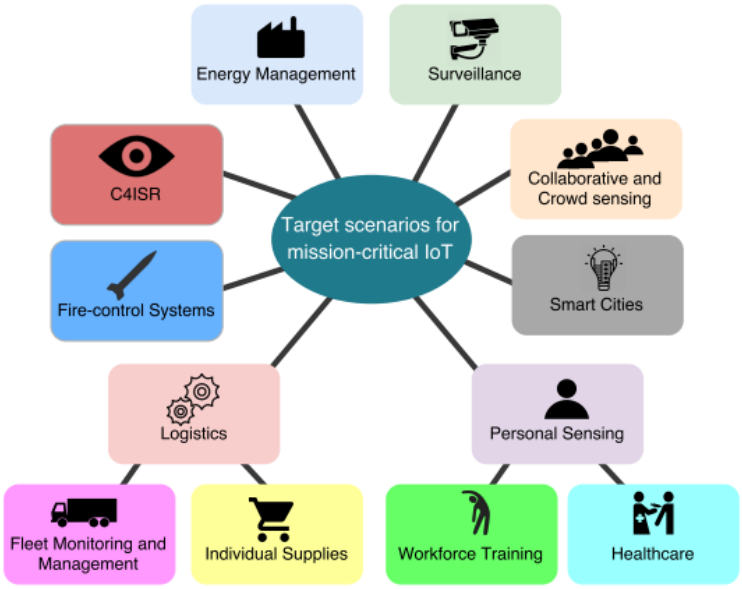
Εικόνα 51. Επίπεδα αρχιτεκτονικής του IoT [51], [143]

Η επισκόπηση που επιχειρήθηκε από τους [140] πλέον του προφανούς στόχου της ανάδειξης της εμπλοκής του IoT στη δημόσια ασφάλεια γενικότερα και στην αντιμετώπιση των συνεπειών των καταστροφών ειδικότερα, μέσα από την προσέγγιση των τεχνολογικών λύσεων που εισάγει στο πεδίο, ήταν να βοηθήσει την αμυντική βιομηχανία να εκμεταλλευτεί τις ευκαιρίες που δημιουργούνται με τη χρήση εμπορικών εφαρμογών IoT σε κρίσιμα για την αποστολή περιβάλλοντα.

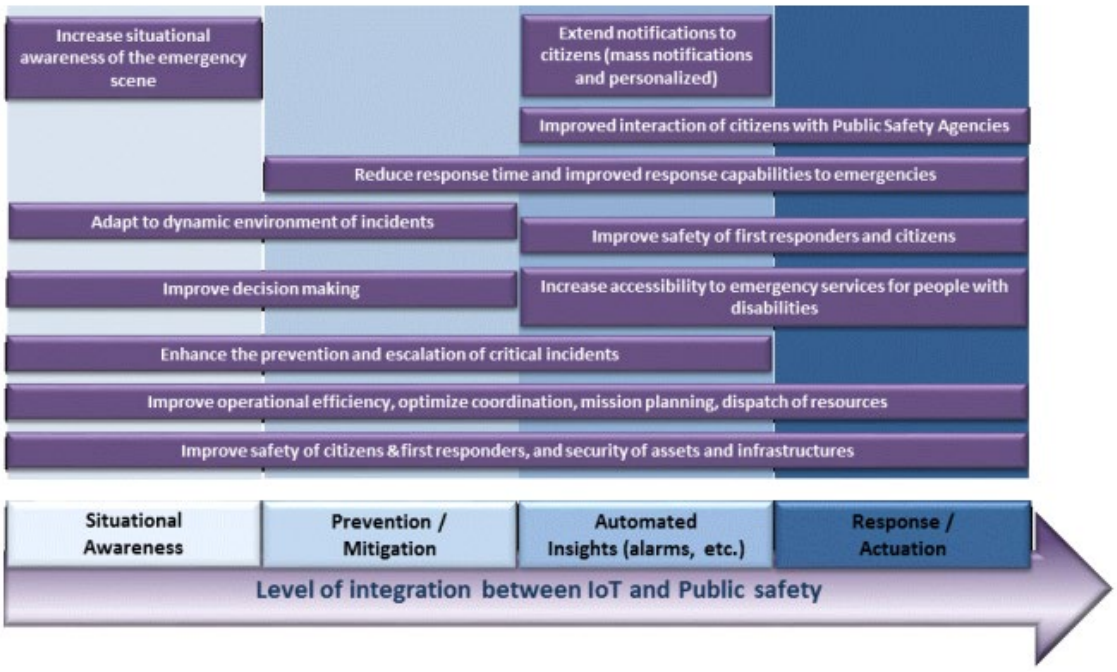
Στο ίδιο άρθρο, με στόχο την πλήρη κατανόηση της περιπλοκότητας υιοθέτησης του IoT σε εφαρμογές δημόσιας ασφάλειας, γίνεται εκτενής αναφορά στις βασικές αρχές του IoT και τα κύρια τυποποιημένα πρωτόκολλα και τεχνολογίες που εμπλέκονται στην υλοποίηση των εφαρμογών αυτών. Η τυποποίηση και στην περίπτωση αυτή έρχεται τόσο από τους γνωστούς Διεθνείς Οργανισμούς ETSI, ITU, ISO, IEEE, Κοινοπραξία του Παγκοσμίου Ιστού (World Wide Web Consortium - W3), όσο και από τα επίσημα στρατιωτικά πρότυπα των Η.Π.Α. (United States Military Standard – MIL-STD). Οι έως σήμερα εφαρμογές που σχετίζονται με το IoT και αφορούν στη δημόσια ασφάλεια έχουν επικεντρωθεί σε ζητήματα που σχετίζονται με τη διοίκηση, τον έλεγχο, την επικοινωνία, την επιτήρηση, την αναγνώριση και την επίγνωση της κατάστασης. Αυτό καθοδηγείται από μια κυρίαρχη άποψη ότι οι αισθητήρες χρησιμεύουν κυρίως ως εργαλεία για τη συλλογή και την κοινή χρήση δεδομένων και τη δημιουργία μιας πιο αποτελεσματικής διοίκησης και ελέγχου των στοιχείων (Εικόνα 52) [140].

Τα συνολικά οφέλη στη δημόσια ασφάλεια από την εμπλοκή του IoT είναι ανδιαμφισβήτητα και συνοψίζονται στην Εικόνα 53 [146]. Μια σειρά από περιπτώσεις χρήσης του IoT στη δημόσια ασφάλεια και τα χαρακτηριστικά αξιολόγησης αυτών έχουν αποτυπωθεί στο [147]. Στην ίδια έκθεση γίνεται αναφορά σε περιστατικά αντιμετώπισης πυρκαγιάς σε οικία, αλλά και σε οίκο ευγηρίας, περιστατικού υγείας που απαιτείται άμεση ιατρική βοήθεια, τροχαίου

ατυχήματος με τραυματίες και διασπορά επικίνδυνων υλικών, διακοπής κυκλοφορίας σε αυτοκινητόδρομο, μαζικών πυροβολισμών σε σχολείο με νεκρούς και τραυματίες, ακραίων καιρικών φαινομένων, και ληστείας σε κατάστημα. Για την αντιμετώπιση αυτών ενεργοποιούνται και αλληλεπιδρούν διαφορετικών ειδών αισθητήρες, βίντεο, θερμικές κάμερες, κόμβοι συνδεσιμότητας συσκευών IoT που υποστηρίζουν τη συνολική εφαρμογή και μια σειρά από πρωτόκολλα επικοινωνίας.



Εικόνα 52. Σενάρια εφαρμογών IoT για τη δημόσια ασφάλεια [140]



Εικόνα 53. Οφέλη του IoT στη δημόσια ασφάλεια, ανάλογα με το επίπεδο ενοποίησης [146]

Αυτή η τεχνολογική συνεργασία στο πλαίσιο υλοποίησης μιας αρχιτεκτονικής εξειδικεύεται στον Πίνακα 10, όπου τα στοιχεία που συμμετέχουν παρουσιάζονται ως πρωταγωνιστές του σκοπού που επιτελούν, όπως αυτός εξειδικεύεται στην περιγραφή για έκαστο εξ αυτών [146]. Τα πρωτόκολλα επικοινωνίας που εμπλέκονται στην τεχνολογία IoT είναι αρκετά και σημαντικά. Μια γρήγορη αναφορά σ` αυτά συναντούμε στο σύνολο σχεδόν της βιβλιογραφίας που σχετίζεται με τις ασύρματες επικοινωνίες. Περιεκτικές παρουσιάσεις των πρωτοκόλλων αυτών με διαφορετική κάθε φορά κατηγοριοποίηση περιλαμβάνονται στις βιβλιογραφικές επισκοπήσεις που επιχειρήθηκαν από τους [52], [140] και [148]. Η παρουσίαση των πρωτοκόλλων αυτών επιλέχθηκε να γίνει με τον ίδιο τρόπο που πραγματοποιήθηκε στα [149], [150] και συγκεκριμένα:

4.10.1 Πρωτόκολλα δικτύωσης

Τα βασικά πρωτόκολλα τις δυνατότητες των οποίων αξιοποιούν οι εφαρμογές IoT συγκετρώνουν κάποια διαφορετικά χαρακτηριστικών, τα σημαντικότερα εκ των οποίων είναι: η εμβέλεια μετάδοσης, το εύρος ζώνης, η περιοχή συχνοτήτων και η ενεργειακή απόδοση. Με οδηγό την εμβέλεια, κατηγοριοποιούνται σε μικρής και μακράς εμβέλειας.

a. Μικρής εμβέλειας: Η απόσταση μεταξύ των συσκευών που συλλέγουν τα δεδομένα και της πύλης που τα επεξεργάζεται είναι μικρότερη των 150 μέτρων. Τα κυριότερα πρωτόκολλα της κατηγορίας είναι:

i. NFC/RFID. Η Επικοινωνία Κοντινού Πεδίου (Near Field Communication – NFC) αποτελεί ένα σύνολο πρωτοκόλλων επικοινωνίας που επιτρέπει την επικοινωνία μεταξύ δύο ηλεκτρονικών συσκευών σε απόσταση 4-10 cm. Η συχνότητα λειτουργίας του είναι 13,56 MHz και οι ρυθμοί δεδομένων του κυμαίνονται από 106 έως 424 kbit/s. Οι συσκευές NFC μπορούν να λειτουργήσουν ως ηλεκτρονικά έγγραφα ταυτότητας αλλά και ως κάρτες-κλειδιά. Με τον όρο Αναγνώριση Ραδιοσυχνοτήτων (Radio Frequency Identification - RFID) περιγράφουμε μια διαδικασία ταυτοποίησης και παρακολούθησης αντικειμένων (γνωστών και ως RF tag) με τη χρήση ραδιοκυμάτων. Ένα σύστημα RFID αποτελείται από έναν αναμεταδότη - ετικέτα (RFID tag) και έναν αναγνώστη (RFID Reader). Το RFID έχει ευρεία χρήση λόγω τη απλότητας του, της εύκολης και αυτοματοποιημένης λειτουργίας του. Η ετικέτα RFID αποτελείται απο ένα μικροτσίπ συνδεδεμένο σε μια κεραία. Αυτή η ετικέτα μπορεί να τοποθετηθεί σε ένα αντικείμενο, με το οποίο και γίνεται η αντιστοίχιση. Οι ετικέτες έχουν πολύ μικρό μέγεθος αρκετά μεγάλη μνήμη είναι επαναχρησιμοποιήσιμες και έχουν πολύ χαμηλό κόστος [151], [152].

ii. Bluetooth/BLE. Το Bluetooth είναι μια ασύρματη τεχνολογία μετάδοσης δεδομένων βασισμένο στο πρότυπο IEEE 802.15.1 που λειτουργεί εντός της μη

αδειδοτημένης ζώνης συχνοτήτων (ISM) των 2,4 GHz. Το 2011 η δημιουργήθηκε το Bluetooth Low Energy (BLE) ή Bluetooth 4.0. Το BLE λειτουργεί στην ίδια ζώνη με το Bluetooth χρησιμοποιεί συχνότητες μεταξύ 2402 και 2480 MHz και διαθέτει 40 κανάλια με εύρος ζώνης 2MHz. Έχει τη δυνατότητα να παραμένει σε κατάσταση αναστολής λειτουργίας έως τη στιγμή που μια σύνδεση ξεκινήσει και έχει σημαντικά βελτιωμένη καθυστέρηση (6ms αντί 100ms) [153].

iii. Zigbee. Το ZigBee είναι μια τεχνολογία χαμηλού κόστους και χαμηλής κατανάλωσης βασισμένο στο πρότυπο IEEE 802.15.4, σχεδιασμένο για εφαρμογές που απαιτούν ασύρματη μεταφορά δεδομένων μικρής εμβέλειας και χαμηλής ταχύτητας. Λειτουργεί σε μη αδειοδοτημένες ISM ζώνες στις συχνότητες: 868 MHz (στην Ευρώπη), 915 MHz (στις Ηνωμένες Πολιτείες) και 2,4 GHz (παγκόσμια). Ο ρυθμός δεδομένων εξαρτάται από τη συχνότητα λειτουργίας του και είναι 250 kbps στα 2,4 GHz, 40 kbps στα 915 MHz και 20 kbps στα 868 MHz ενώ η εμβέλεια του φτάνει τα 100m για το ZigBee και έως 1.6Km για το ZigBee Pro. Η συσκευή που υποστηρίζεται από το πρωτόκολλο μεταδίδει δεδομένα μέσω από ένα δίκτυο πλέγματος ενδιάμεσων συσκευών και διαδρομής πολλαπλών αλμάτων, εξασφαλίζοντας μέσα από τη συγκεκριμένη λειτουργικότητα τη σύνδεση περισσότερων συσκευών σε μεγαλύτερη απόσταση [153], [154], [155].

iv. Z-Wave. Το Z-wave όπως και το Zigbee, είναι ένα πρωτόκολλο δικτύου πλέγματος (mesh). Η ουσιαστική διαφορά τους είναι η απόδοση δεδομένων, καθώς το Z-wave είναι περίπου 6 φορές πιο αργό από το Zigbee. Ωστόσο, απαιτεί λιγότερη ενέργεια για να καλύψει το ίδιο εύρος. Η τεχνολογία Z – Wave ελαχιστοποιεί την κατανάλωση ενέργειας. Η συχνότητα κυμαίνεται στα 800-900 MHz και έχει μέγιστη εμβέλεια μέχρι και 100m με ταχύτητες μετάδοσης έως και 100 Kbps [156].

v. Infrared. Η υπέρυθρη ακτινοβολία χρησιμοποιείται για την εκτέλεση ασύρματης επικοινωνίας μικρής εμβέλειας και μάλιστα όταν υφίσταται οπτική επαφή. Η συχνότητα του υπέρυθρου βρίσκεται στο ηλεκτρομαγνητικό φάσμα, κάτω από το ορατό φως. Το υπέρυθρο επιτρέπει συσκευές για τη μεταφορά δεδομένων σε λειτουργία full-duplex [153]. Φορητοί υπολογιστές, κάμερες, κινητά τηλέφωνα και άλλες συσκευές χρησιμοποιούν υπέρυθρες για επικοινωνία στο «*τελευταίο ένα μέτρο*» με βάση την αρχή point-and-shoot. Τα κύρια χαρακτηριστικά της επικοινωνίας υπερύθρων είναι η φυσικά ασφαλής μεταφορά δεδομένων και ένα εξαιρετικά χαμηλό ποσοστό σφάλματος bit που με τη σειρά του το καθιστά αποτελεσματικό. Ο ρυθμός μεταφοράς υπερύθρων είναι περίπου 4 Mbps [52].

b. Μακράς εμβέλειας. Για επικοινωνία σε αποστάσεις μεγαλύτερες από 150m, υπάρχουν μια σειρά σημαντικών πρωτοκόλλων, τα οποία παρουσιάζονται στη συνέχεια.
   i. Κυψελωτά δίκτυα Κινητής Τηλεφωνίας 4G/5G (Cellular Mobile Networks), στα οποία ήδη αναφερθήκαμε εκτενώς στα κεφάλαια 4.3 και 4.4.
   ii. Narrow band Internet of things – NB-IoT. Πρωτόκολλο του LTE αποκλειστικά προσαρμοσμένο για εφαρμογές του IoT. Ο ρυθμός δεδομένων ανέρχεται στα 200kbps για down-link και 20kbps για up-link, με ωφέλιμο όγκο πληροφορίας τα 1600bytes ανά μήνυμα. Μεταδίδοντας κατά μέσο όρο 200bytes ανά ημέρα, η εκτιμωμένη διάρκεια ζωής της μπαταρίας ανέρχεται σε 10 έτη. Το NB-IoT σχεδιάστηκε ειδικά για εφαρμογές σε δίκτυα ευρείας περιοχής χαμηλής κατανάλωσης (Low Power Wide Area Network – LPWAN) και λειτουργεί στις αδειοδοτημένες ζώνες ραδιοσυχνοτήτων. Η 13η έκδοση του 3GPP (Release 13) προσφέρει βελτιωμένη κάλυψη υποστηρίζοντας μεγάλο αριθμό συσκευών χαμηλής κατανάλωσης με χαμηλό κόστος, μικρό χρόνο απόκρισης, μικρή καθυστέρηση και βελτιωμένη αρχιτεκτονική δικτύου. Επίσης παρέχει συμβατότητα με την υπάρχουσα υποδομή του δικτύου κινητής τηλεφωνίας και εφάμιλλο επίπεδο ασφαλείας, ενώ η διάρκεια ζωής της μπαταρίας επεκτάθηκε σε περισσότερα από 15 έτη. Η δυνατότητα υποστήριξης εφαρμογών σε διαφορετικές ζώνες συχνοτήτων με εύρος ζώνης τα 200khz ως αυτόνομο δίκτυο αποτελεί επίσης ένα πολύ σημαντικό στοιχείο. Επιπλέον διαθέτει δυο λειτουργίες για εξοικονόμηση ενέργειας με στόχο την μεγιστοποίηση της απόδοσης, μια εκ των οποίων επιτρέπει στις συσκευές να μεταβαίνουν σε κατάσταση βαθύ ύπνου για έως και 310 ώρες. Στα σημαντικά θετικά στοιχεία του εντάσσεται το γεγονός ότι δεν επηρεάζεται σημαντικά από παρεμβολές και υποστηρίζει μετάδοση 20db, η οποία εξασφαλίζει την ικανότητα διείσδυσης σε δύσκολοπρόσιτες περιοχές με υπεράριθμες μεταδόσεις, γεγονός που το καθιστά κατάλληλο για εφαρμογές κτιρίων, υπογείων και συσκευών που λειτουργούν σε ορυχεία. Επίσης προσφέρει υψηλή χωρητικότητα που μπορεί να φτάσει σε δισεκατομμύρια συνδέσεις εξοπλισμού και η οποία επαρκεί για να καλύψει τις απαιτήσεις σύνδεσης διαφορετικών εφαρμογών [157].
   iii. Wi-Fi (IEEE 802.11). Το IEEE 802.11 αποτελεί ένα πρότυπο για τα Δίκτυα Ευρείας Περιοχής, γνωστό και ως Wi-Fi (Wireless Fidelity). Σήμερα αποτελεί ένα από τα πιο διαδεδομένα πρότυπα διαθέσιμο σχεδόν παντού (σπίτια, δημόσια κτίρια, επιχειρήσεις) και υποστηρίζεται από τεράστια ποικιλία συσκευών. Λειτουργεί στις συχνότητες 2,4 – 2,5 GHz, ενώ μια σειρά από τις εκδόσεις του χρησιμοποιούν και επιπλέον συχνότητες λειτουργίας διατηρώντας πάντα

συμβατότητα με τις παλαιότερες εκδόσεις. Σήμερα ο όγκος των δεδομένων που μεταφέρονται μέσω WiFi κυμαίνεται ανάμεσα στο 50% - 80% ανάλογα με τη χώρα σύμφωνα με την IEEE η οποία είναι υπεύθυνη για την εξέλιξη των προτυποποιήσεων του. Για τις επικοινωνίες των πρώτων ανταποκριτών θα μπορούσαμε να ξεχωρίσουμε συγκεκριμένες εκδόσεις για τις δυνατότητες αξιοποίησης τους σε κρίσιμες εφαρμογές στο κοντινό μέλλον [152], [153], [158], [159]:

- 802.11ah (Wi-Fi Halow). Για εφαρμογές IoT που επιτρέπει επικοινωνίες χαμηλής κατανάλωσης και υψηλής ταχύτητας δεδομένων. Λειτουργεί στη μη αδειοδοτημένη ζώνη συχνοτήτων κάτω του 1 GHz. Υποστηρίζει έως 8000 συσκευές με κάλυψη 1 km και συνεπώς είναι κατάλληλη για εφαρμογές που απαιτούν χαμηλό κόστος, χαμηλή κατανάλωση ενέργειας και μεγάλη εμβέλεια. Το φυσικό επίπεδο μπορεί να χωριστεί σε δύο κατηγορίες: Στην 2MHz, 4MHz, 8MHz, 16MHz λειτουργία μετάδοσης και στην 1MHz λειτουργία μετάδοσης. Η μεγάλη κάλυψη, η χαμηλή κατανάλωση ενέργειας, η εγγενής υποστήριξη του IP πρωτοκόλλου και ο μεγάλος αριθμός υποστήριξης συσκευών αποτελούν τα κύρια πλεονεκτήματά του.
- 802.11bf WLAN sensing: Δυνατότητα ανίχνευσης χαρακτηριστικών ενός επιδιωκόμενου στόχου σε δεδομένο περιβάλλον λαμβάνοντας ταυτόχρονα μετρήσεις της εμβέλειας, ταχύτητας, γωνιακής κίνησης, καθώς και την αναγνώριση παρουσίας ή εγγύτητας αντικειμένων όπως ανθρώπων ή ζώων.
- 802.11az Next Generation Positioning: Χρήση σε εφαρμογές πλοήγησης σε εσωτερικούς χώρους με εξαιρετικά μεγάλη ακρίβεια, (κάτω από 1 m). Καθώς και αξιοπιστία πλοήγησης σε εξαιρετικά πυκνά περιβάλλοντα (στάδιο/αεροδρόμιο)
- 802.11ay αποτελεί την επόμενη γενιά των 60 GHz: Που δίνει έμφαση στην αυξημένη απόδοση και εμβέλεια, ιδανικό για εφαρμογές επαυξημένης και εικονικής πραγματικότητας καθώς και για την μετάδοση βίντεο ανάλυσης 8K.

iv. LoRaWAN. Το Δίκτυο Ευρείας Περιοχής Χαμηλού Εύρους (Low Range Wide Area Networking – LoRaWAN) είναι ένα MAC πρωτόκολλο δικτύου που σχεδιάστηκε για εφαρμογές του IoT. Είναι κατάλληλο για Ασύρματα Μητροπολιτικά Δίκτυα (Wireless Metropolitan Area Networks - WMANs και για Ασύρματα Τοπικά Δίκτυα (Wireless Local Area Networkw – WLANs), καθώς χρησιμοποιεί αμφίδρομη επικοινωνία με χαμηλό ρυθμό μετάδοσης δεδομένων.

Μπορεί να λειτουργήσει σε ολόκληρη τη ζώνη EU ISM (μη αδειοδοτημένη κατηγορία) των 868 MHz, αλλά έχει τρία υποχρεωτικά κανάλια: 868.10, 868.30 και 868.50 MHz. Επιτυγχάνει ρυθμούς μετάδοσης που ποικίλουν από 290bps έως 50kbps με εμβέλεια που κυμαίνεται σε 2-5 km για αστικό περιβάλλον, 15 km για περιαστικό και 45 km στην ύπαιθρο. Το LoRaWAN περιγράφει κατηγορίες συσκευών μικρής και μέτριας κατανάλωσης ενέργειας, καθώς και μόνιμης κατάστασης λειτουργίας. Τέλος η διάρκεια ζωής των μπαταριών στις συσκευές κυμαίνεται από 8 έως 10 έτη. Το LoRaWAN είναι αρκετά ανθεκτικό στις παρεμβολές, και εξαιρετικά παραμετροποιήσιμο. Επιτυγχάνει μεγάλη εμβέλεια, ιδιαίτερα όταν οι συσκευές βρίσκονται σε οπτική επαφή, ενώ υπάρχει σημαντική μείωσή της σε αστικό περιβάλλον. Επιτυγχάνει αξιοπιστία εκ του γεγονότος ότι κάθε μήνυμα που μεταδίδεται από μια συσκευή λαμβάνεται από όλους τους σταθμούς βάσης της περιοχής [160], [161].

v. Sigfox. Αποτελεί μια χαμηλής ισχύος ασύρματη τεχνολογία που σχεδιάστηκε για την αμφίδρομη μεταφορά δεδομένων χαμηλού ρυθμού, κατάλληλη για εφαρμογές του IoT και χρήση σε δίκτυα WMANs/WLANs. Λειτουργεί στις μη αδειοδοτημένες ραδιοσυχνότητες (ISM) των 868MHz στην Ευρώπη, 915MHz στη Βόρεια Αμερική, και 433MHz στην Ασία. Οι up-link μεταδόσεις του ανέρχονται σε 140 μεταδόσεις με μέγιστο φορτίο τα 12bytes ενώ οι down-link μεταδόσεις ανέρχονται σε 4 με μέγιστο φορτίο τα 8bytes ανά ημέρα/συσκευή. Ο ρυθμός μετάδοσης είναι περίπου 100 bps (π.χ. εύρος ζώνης 100 Hz) και 600 bps (π.χ. εύρος ζώνης 600 Hz). Το Sigfox παρουσιάζει πολύ χαμηλή κατανάλωση ενέργειας, υψηλή ευαισθησία δέκτη και χαμηλό κόστος σχεδίασης κεραίας. Είναι ανθεκτικό σε παρεμβολές και συγκρούσεις. Κάθε αισθητήρας στέλνει κάθε πακέτο δεδομένων σε τρία κανάλια επικοινωνίας σε ψευδοτυχαία επιλεγμένες χρονικές στιγμές, έτσι τουλάχιστον 3 σταθμοί Βάσης (BS) μπορούν να λάβουν τα μηνύματα ταυτόχρονα από όλα τα κανάλια, γεγονός που οδηγεί σε περαιτέρω μείωση του κόστους χρησιμοποιώντας συσκευές μικρότερων απαιτήσεων. Ωστόσο, η ίδια αυτή μετάδοση επιφέρει την αύξηση του βαθμού κατάληψης του καναλιού και αυτό οδηγεί και στην αύξηση του αριθμού των ενδεχόμενων συγκρούσεων [162].

vi. WiMAX. Η Παγκόσμια Διαλειτουργικότητα για Πρόσβαση σε Μικροκύματα (Worldwide Interoperability for Microwave Access - WiMAX) ορίζεται από το πρότυπο IEEE 802.16 που προορίζεται για παροχή ασύρματων υπηρεσιών φωνής και δεδομένων υψηλού εύρους ζώνης για μεγάλο χρονικό διάστημα με εμβέλεια για εξωτερικό περιβάλλον. Οι παραλλαγές του IEEE 802.16a και 802.16d (γνωστό ως IEEE 802.16-2004) προσφέρουν μια βιώσιμη λύση μεγάλης απόστασης για την

παροχή πρόσβαση στο διαδίκτυο, ενώ η έκδοση 802.16e είναι κατάλληλη για τελικές συσκευές. Στο πλαίσιο αντιμετώπισης έκτακτης ανάγκης, το WiMAX φαίνεται κατάλληλο για την υποστήριξη του κέντρου ελέγχου και διοίκησης, με δυνατότητες μεγάλης εμβέλειας επικοινωνία. [52], [153], [163]. Μια σημαντική συγκριτική μελέτη της απόδοσης των προτύπων 802.11, 802.11a/b/g, 802.16, 802.16a/e παρουσιάζεται στην εργασία των [163], στο πλαίσιο της έρευνάς τους για την παροχή απομακρυσμένης πρόσβασης σε υπηρεσίες υγείας (e-HealthCare).

4.10.2 Πρωτόκολλα επιπέδου εφαρμογής

Τα πρωτόκολλα που παρουσιάζονται στην ενότητα αυτή αποτελούν τα πλέον αντιπροσωπευτικά πρωτόκολλα του επιπέδου εφαρμογών του IoT:

a. MQTT: Το πρωτόκολλο Μεταφοράς Τηλεμετρίας σε Ουρά Μηνυμάτων (Message Queue Telemetry Transport – MQTT) είναι ένα από τα πιο πολυχρησιμοποιημένα πρωτόκολλα του επιπέδου μεταφοράς σε εφαρμογές IoT. Διαχειρίζεται δυναμικά πολλά δεδομένα και από πολλές συσκευές. Το πρωτόκολλο αυτό ανήκει στην οικογένεια των πρωτοκόλλων δημοσίευσης / εγγραφής και εξυπηρετεί τις περιπτώσεις που απαιτείται αποτύπωμα μικρού κώδικα. Λειτουργεί ασύγχρονα και αποδοτικά σε συνθήκες ασταθούς σύνδεσης της γραμμής μετάδοσης των δεδομένων και ως εκ τούτου καθίσταται ιδανικό για περιορισμένα περιβάλλοντα (χαμηλόρυθμη σύνδεση, υψηλή καθυστέρηση, μικρή επεξεργαστική ισχύος συσκευές ή μικρής μνήμης συσκευές). Παρέχει εύκολη ενσωμάτωση νέων συσκευών και έχει χαμηλή κατανάλωση ενέργειας, ενώ χιλιάδες συσκευές είναι εφικτό να συνδεθούν χωρίς να απαιτείται άδεια χρήσης και χωρίς οι συσκευές που αποστέλλουν δεδομένα να απαιτείται να γνωρίζουν οτιδήποτε για τους δέκτες. Έτσι, το MQTT είναι κατάλληλο για μεγάλα δίκτυα μικρών συσκευών για τις οποίες υπάρχει ανάγκη να παρακολουθούνται ή να ελέγχονται μέσω διαδικτύου [164], [165], [166].

b. CoAP: Το Πρωτόκολλο Περιορισμένης Εφαρμογής (Constrained Application Protocol - CoAP) είναι ένα πρωτόκολλο επίπεδου εφαρμογής για το IoT μέσω του διαδικτύου για συσκευές με μικρή υπολογιστική δυνατότητα. Η λειτουργικότητα του CoAP είναι παρόμοια με την αντίστοιχη του HTTP και έχει σχεδιαστεί ειδικά για συσκευές που βασίζονται σε περιορισμούς. Για να καλύψει τις απαιτήσει του IoT, τροποποιεί ορισμένες λειτουργίες του HTTP, επιτυγχάνοντας τελικώς χαμηλότερη κατανάλωση ενέργειας και μικρότερες απώλειες στη λειτουργία των συνδέσμων. Συγκριτικά με τα υπόλοιπα πρωτόκολλα του ιδίου επιπέδου θεωρείται ότι είναι «ελαφρύτερο». Το CoAP ουσιαστικά παρέχει λύση στην ενοποίηση του δικτύου των πραγμάτων με τις υπόλοιπες υπηρεσίες του διαδικτύου. Με δεδομένο ότι χρησιμοποιεί απλή διεπαφή με το HTTP παρέχει σημαντικές βελτιώσεις στην

παράδοση των πακέτων, μείωση των επιβαρύνσεων και απλότητα εργασιών, ενώ παράλληλα αποτελεί ένα καλό πρωτόκολλο για εφαρμογές IoT, καθώς παρέχει μηχανισμούς αξιοπιστίας του δικτύου και λειτουργεί από προεπιλογή με UDP. Υποστηρίζει πολυεκπομπή, που επιτρέπει σε ένα αίτημα να δημοσιεύσει ένα μήνυμα σε πολλές συσκευές ταυτόχρονα, είναι απλό και με πολύ χαμηλό κόστος. Οι συσκευές που εμπλέκονται στην υλοποίηση λειτουργούν σε ένα περιορισμένο περιβάλλον και το CoAP κλήθηκε να αποτελέσει τη λύση στις ειδικές αυτές απαιτήσεις, λαμβάνοντας υπόψη την ενέργεια, τον αυτοματισμό και άλλες εφαρμογές M2M. Συγκεκριμένα, με το CoAP μπορούμε να διαχειριστούμε εφαρμογές και υπηρεσίες που προσφέρουν οι δήμοι στους πολίτες [139], [166].

c. XMPP: Το Επεκτάσιμο Πρωτόκολλο Μηνυμάτων και Παρουσίας (eXtensible Messaging and Presence Protocol – XMPP) σχεδιάστηκε από την κοινότητα ανοιχτού κώδικα της Jabber το 1998, με σκοπό την άμεση επικοινωνία μεταξύ των χρηστών. Βασίζεται στο μοντέλο αιτήματος / απάντησης και λειτουργεί πάνω από το πρωτόκολλο TCP/IP. Το XMPP είναι ένα από τα δημοφιλή πρωτόκολλα για εφαμρογές IoT καθώς υποστηρίζει μικρά μηνύματα και χαμηλή καθυστέρηση, αλλά και συνομιλία και φωνητικές κλήσεις πολλών χρηστών. Βασίζεται σε XML και αποτελεί μια καλή λύση για εφαρμογές ανταλλαγής άμεσων μηνυμάτων και αναζήτηση ενεργής διαδικτυακής παρουσίας. Ωστόσο επιφέρει σημαντική επιβάρυνση στο δίκτυο [27]. Παρά την απλότητά του, τη δυνατότητα χρήσης του σε ετερογενείς εφαρμογές, το ότι παρέχει τη δυνατότητα πολλαπλής ταυτόχρονης σύνδεσης έχει ως αποτέλεσμα την υψηλή κατανάλωση εύρους ζώνης και υψηλή χρήση CPU [139], [166].

d. AMQP: Το Σύνθετο Πρωτόκολλο Ουράς Μηνυμάτων (Advanced Message Queueing Protocol – AMQP) είναι ένα πρωτόκολλο που υποστηρίζει εφαρμογές του IoT με ανάγκες για ανταλλαγή μεγάλου όγκου μηνυμάτων. Βασίζεται στο μοντέλο εξυπηρετητή / πελάτη, πάνω από το πρωτόκολλο επιπέδου δικτύου TCP/IP και κάνει χρήση του μοντέλου μηνυμάτων δημοσίευσης / εγγραφής. Σχεδιάστηκε το 2003 για χρήση κυρίως από τραπεζικά ιδρύματα, όπως και το MQTT και τα κύρια χαρακτηριστικά του αφορούν σε εξαιρετική απόδοση, αξιοπιστία, ασφάλεια και διαλειτουργικότητα. Υποστηρίζει αποδοτικά την αποστολή μεγάλου όγκου δεδομένων χωρίς να επηρεάζονται οι επιδόσεις του συστήματος που υποστηρίζει. Είναι σημαντικά επεκτάσιμο και παρέχει ικανοποιητικό επίπεδο ασφάλεια στη μετάδοση μηνυμάτων. Είναι ακατάλληλο για περιβάλλοντα περιορισμένων πόρων και εφαρμογές πραγματικού χρόνου και δεν παρέχει ή υποστηρίζει μηχανισμό αυτοματοποιημένου εντοπισμού [139], [166].

e. DDS: Η Υπηρεσία Διανομής Δεδομένων (Data Distribution Service - DDS) είναι ένα πρωτόκολλο δημοσίευσης / εγγραφής για επικοινωνίες M2M σε πραγματικό χρόνο, το οποίο αναπτύχθηκε το 2004 [28]. Το DDS παρέχει συνδεσιμότητα δεδομένων χαμηλής καθυστέρησης, εξαιρετική αξιοπιστία και μια κλιμακωτή αρχιτεκτονική που χρειάζονται οι εφαρμογές του IoT καίριας σημασίας. Το DDS προσφέρει μια ποικιλία κριτηρίων επικοινωνίας όπως (α) ασφάλεια, (β) κατεπείγουσα λειτουργία, (γ) προτεραιότητα, (δ) ανθεκτικότητα και (ε) αξιοπιστία. Η μετάδοση δεδομένων στο DDS είναι ελεγχόμενη και ως εκ τούτου αξιόπιστη και συνεπής. Οι νέες συσκευές ανιχνεύονται αυτόματα, όπως γίνεται και η προσθήκη τους στο δίκτυο. Όπως αντιλαμβανόμαστε βέβαια, το πρωτόκολλο DDS αδυνατεί να λειτουργήσει αξιόπιστα όταν διατίθενται ελάχιστοι πόροι. [139], [166].

ΠΡΩΤΑΓΩΝΙΣΤΕΣ	ΠΕΡΙΓΡΑΦΗ
IoT αισθητήρες και συσκευές	Αισθητήρες IoT και συσκευές που είναι εγκατεστημένες σε κτίρια, ανοιχτούς χώρους και περιβάλλοντες χώρους, όπως αισθητήρες έξυπνων κτιρίων, αισθητήρες περιβάλλοντος, σύστημα εντοπισμού εσωτερικών χώρων κ.λπ..
Κληροδοτημένα συστήματα	Συμπεριλαμβάνονται παλαιού τύπου συστήματα CCTV, προηγμένες αναλογικές ή IP κάμερες με δυνατότητες ανίχνευσης, συστήματα διαχείρισης κτιρίων, σύστημα ανίχνευσης εισβολής κ.λπ, τα οποία μπορούν να χρησιμοποιηθούν για επίγνωση της κατάστασης, με την προϋπόθεση ότι θα αναπτυχθούν πύλες για την αναφορά των δεδομένων σε πλατφόρμες IoT.
Συστήματα δημόσιας προειδοποίησης	Σύστημα δημόσιας προειδοποίησης για μαζικές ειδοποιήσεις με βάση SMS, εκπομπή κινητής τηλεφωνίας, τηλεόραση, σειρήνες κ.λπ.
Πλατφόρμα IoT και δεδομένων	Πλατφόρμα IoT που αναπτύσσεται στο πλαίσιο έξυπνων πόλεων ή έξυπνων κτιρίων, που εκτελεί λειτουργίες όπως διαχείριση συσκευών, ανταλλαγή και κοινή χρήση δεδομένων, συνάθροιση, επεξεργασία, ανάλυση, τεχνητή νοημοσύνη, αποθήκευση, ασφάλεια και απόρρητο (έλεγχος ταυτότητας, εξουσιοδότηση, ταυτότητα, πιστοποίηση κ.λπ.).
IoT συσκευές και ενεργοποιητές	Συσκευές βασισμένες στο IoT που μπορούν είτε να ενεργοποιήσουν συναγερμό είτε να ενεργοποιήσουν έναν ενεργοποιητή που εμπλέκεται σε άλλη λειτουργία στο σύστημα δημόσιας ασφάλειας
Κέντρα ελέγχου των υπηρεσιών δημόσιας ασφάλειας	Το κέντρο ελέγχου μπορεί να λαμβάνει μια κοινή εικόνα λειτουργίας από διαφορετικά συστήματα IoT. Το 112 και το αντίστοιχο δίκτυο επικοινωνίας έκτακτης ανάγκης αποτελούν μέρος της συνολικής υποδομής του δικτύου των φορέων δημόσιας ασφάλειας.
Εφαρμογές και συσκευές για πρώτους ανταποκριτές	Οι εφαρμογές επαυξημένης και εικονικής πραγματικότητας, εφαρμογές για κινητές συσκευές πρώτης απάντησης, υπηρεσίες βάσει τοποθεσίας και εφαρμογές διαλογής. Οι εφαρμογές πρώτης απάντησης χρησιμοποιούν συνήθως κρίσιμα δίκτυα επικοινωνίας με ευρυζωνικές δυνατότητες. Περιλαμβάνει επίσης ειδικές συσκευές δημόσιας ασφάλειας, όπως φορητές συσκευές πρώτης απάντησης, ανιχνευτές επικίνδυνων υλικών (HazMat) ή πυροβολισμών.
Εφαρμογές για πολίτες	Μπορεί να κυμαίνεται από εφαρμογές για κινητές συσκευές για κλήσεις έκτακτης ανάγκης (φωνή, βίντεο, κείμενο), εξατομικευμένες οδηγίες ασφάλειας ή/και έκτακτης ανάγκης, πλοήγηση/εκκένωση βάσει τοποθεσίας σε περίπτωση έκτακτης ανάγκης, εφαρμογές ηλεκτρονικής υγείας και φορητές συσκευές κ.λπ.
Δημόσιες προειδοποιήσεις	Οι δημόσιες προειδοποιήσεις που βασίζονται στο IoT μπορούν να ενσωματωθούν σε εφαρμογές για κινητές συσκευές πολιτών, ψηφιακές πινακίδες (π.χ. φωτεινά βέλη/πινακίδες σε διαδρόμους, δυναμικές πινακίδες εξόδου κ.λπ.), συστήματα ψηφιακών μέσων (π.χ. σε δημόσιες οθόνες και/ή συστήματα δημόσιας διεύθυνσης), σήματα μεταβλητών μηνυμάτων (π.χ. σε αυτοκινητόδρομους), μέσα κοινωνικής δικτύωσης κ.λπ.
Δημόσια δίκτυα	Δημόσια δίκτυα (π.χ. 4G, 5G) ή/και δίκτυα ασύρματης πρόσβασης χαμηλής ισχύος (LPWAN) θα μπορούσαν να χρησιμοποιηθούν για τη σύνδεση συσκευών, εφαρμογών και πλατφορμών
Δίκτυο κρίσιμων επικοινωνιών	Δίκτυα υψηλής ανθεκτικότητας που παρέχουν υπηρεσίες επικοινωνίας όπου τα συμβατικά δίκτυα δεν μπορούν να καλύψουν τις απαιτούμενες απαιτήσεις. Η εμβέλεια του κρίσιμου δικτύου επικοινωνίας μπορεί να επεκταθεί μέσω δικτύων που μπορούν να αναπτυχθούν μέσω π.χ. drones.

Πίνακας 10. Φορείς που εμπλέκονται στην αρχιτεκτονική IoT και σκοπός που επιτελείται [146]

4.11 Cloud, Fog, Edge Computing

Η φυσική συνέχεια των τεχνολογιών και πρωτοκόλλων επικοινωνίας που εμπλέκονται στο IoT είναι οι έννοιες της συλλογής και ανάλυσης δεδομένων. Στις συγκεκριμένες επιμέρους εργασίες των δικτύων επικοινωνίας της δημόσιας ασφάλειας εμφανίζονται ιδιαίτερες προκλήσεις που αφορούν κατά κύριο λόγο στην περιπλοκότητα και ετερογένεια των δεδομένων. Διαφορετικοί τύποι δεδομένων, τα οποία μεταδίδονται με διαφορετικές μορφές θα πρέπει να συλλεγούν και να επεξεργαστούν αποδοτικά και αποτελεσματικά [139].

Η ραγδαία ανάπτυξη του IoT οδηγεί στις έξυπνες πόλεις και κατ` επέκταση σε περιβάλλοντα σαφώς πιο απαιτητικά στην παροχή αξιόπιστων υπηρεσιών δημόσιας ασφάλειας. Οι πόλεις μεγαλώνουν με ταχύτατους ρυθμούς (Εικόνα 54) και μαζί τους μεγαλώνει η δυσκολία των συνθηκών στις οποίες οι οργανισμοί και φορείς θα πρέπει να παρέχουν το αγαθό της δημόσιας ασφάλειας. Όμως αυτό δεν αποτελεί μόνο πρόβλημα, καθώς η ανάπτυξη των πόλεων συνοδεύεται από την απόκτηση «ευφυίας» από τις υποδομές τους και τις υπηρεσίες που αυτές παρέχουν. Η ευφυία είναι αδιαμφισβήτητα ένα έδαφος γόνιμο για την παροχή βελτιωμένων και σύγχρονων υπηρεσιών δημόσιας ασφάλειας. Ενεργή και σημαντική συμμετοχή σ` αυτό έχουν η νεφοϋπολογιστική (cloud computing), η υπολογιστική ακμής (edge computing) και ομίχλης (fog computing), για τους λόγους που θα εξειδικεύσουμε στη συνέχεια.

Εικόνα 54. Οι πόλεις μεγαλώνουν - Smart Cities [167]

4.11.1 Cloud Computing.

Ξεκινώντας από μια γρήγορη εποπτική ματιά της τεχνολογίας νεφουπολογιστικής (cloud computing), ορίζουμε αυτή ως οτιδήποτε περιλαμβάνει την παροχή φιλοξενούμενων υπηρεσιών μέσω του διαδικτύου. Οι υπηρεσίες αυτές χωρίζονται σε τρεις κύριες κατηγορίες ή τύπους υπολογιστικού νέφους: υποδομή ως υπηρεσία (Infrastructure as a Service - IaaS), πλατφόρμα ως υπηρεσία (Platform as a Servise - PaaS) και λογισμικό ως υπηρεσία (Software as a Servise - SaaS) (Εικόνα 55). Ένα σύννεφο μπορεί να είναι ιδιωτικό ή δημόσιο και έχει κυρίαρχο στόχο να παρέχει εύκολη, κλιμακούμενη πρόσβαση σε υπολογιστικούς πόρους και υπηρεσίες πληροφορικής. Η υποδομή cloud περιλαμβάνει τα στοιχεία υλικού και λογισμικού που απαιτούνται για τη σωστή εφαρμογή ενός μοντέλου υπολογιστικού νέφους [168].

Τα μοντέλα ανάπτυξης του υπολογιστικού νέφους που συναντούμε είναι τριών ειδών:

1. Ιδιωτικές υπηρεσίες υπολογιστικού νέφους. Παρέχονται από το κέντρο δεδομένων μιας επιχείρησης σε εσωτερικούς χρήστες. Το μοντέλο προσφέρει την ευελιξία και την ευκολία του cloud, διατηρώντας παράλληλα τη διαχείριση, τον έλεγχο και την ασφάλεια που επιθυμεί μια επιχείριση. Οι εσωτερικοί χρήστες έχουν πρόσβαση με χρέωση ή μη. Οι κοινές ιδιωτικές τεχνολογίες cloud και προμηθευτές περιλαμβάνουν το VMware και το OpenStack.

2. Δημόσιο υπολογιστικό νέφος. Ένας πάροχος υπηρεσιών νέφους (Cloud Service Provider – CSP) παρέχει την υπηρεσία cloud μέσω του διαδικτύου. Τα κορυφαία δημόσια CSP περιλαμβάνουν τα AWS, Microsoft Azure, IBM και Google Cloud Platform (GCP), καθώς και τα IBM, Oracle και Tencent.

3. Υβριδικός συνδυασμός των δύο προηγούμενων κατηγοριών. Οι εταιρείες μπορούν να εκτελούν κρίσιμους φόρτους εργασίας ή ευαίσθητες εφαρμογές στο ιδιωτικό cloud και να χρησιμοποιούν το δημόσιο cloud για να χειρίζονται τεράτιους όγκους εργασίας ή αύξηση ζήτησης των πελατών τους. Ο στόχος είναι να δημιουργηθεί ένα ενοποιημένο, αυτοματοποιημένο, επεκτάσιμο περιβάλλον που εκμεταλλεύεται όλα όσα μπορεί να προσφέρει μια δημόσια υποδομή, διατηρώντας παράλληλα τον έλεγχο των κρίσιμων για την αποστολή δεδομένων.

Από τα παραπάνω γίνεται αντιληπτό γιατί η νεφοϋπολογιστική θεωρείται μια από τις καλύτερες και περισσότερο χρησιμοποιημένες τεχνολογίες για αποθήκευση δεδομένων και διαμοιρασμό αυτών μεταξύ διαφορετικών συσκευών που εμπλέκονται στις υλοποιημένες εφαρμογές του διαδικτύου των πραγμάτων. Τα στοιχεία που αφορούν στην εκθετική αύξηση των μεγεθών των δεδομένων είναι συναρπαστικά, καθώς σύμφωνα με το [169]:

- 2,5 εκατομμύρια byte δεδομένων ημερησίως κατά το 2021
- 91% των χρηστών του Instagram αλληλεπίδρασαν με βίντεο κατά το 2022
- 70% του ΑΕΠ παγκοσμίως θα έχει ψηφιοποιηθεί μέχρι το τέλος του 2022
- 10^{21} bytes δεδομένων θα αποθηκευτούν στο cloud παγκοσμίως, μέχρι το 2025

- 650 εκατομμύρια tweets ημερησίως απέστειλαν οι χρήστες κατά το 2022
- 44 zettabyte θα αποτελούν ολόκληρο το ψηφιακό σύμπαν μέχρι το τέλος του 2020,
- 333,2 δισεκατομμύρια email καθημερινά αποστέλλονταν κατά το 2022

Εικόνα 55. Διαφορετικοί τύποι νεφοϋπολογιστικής [168]

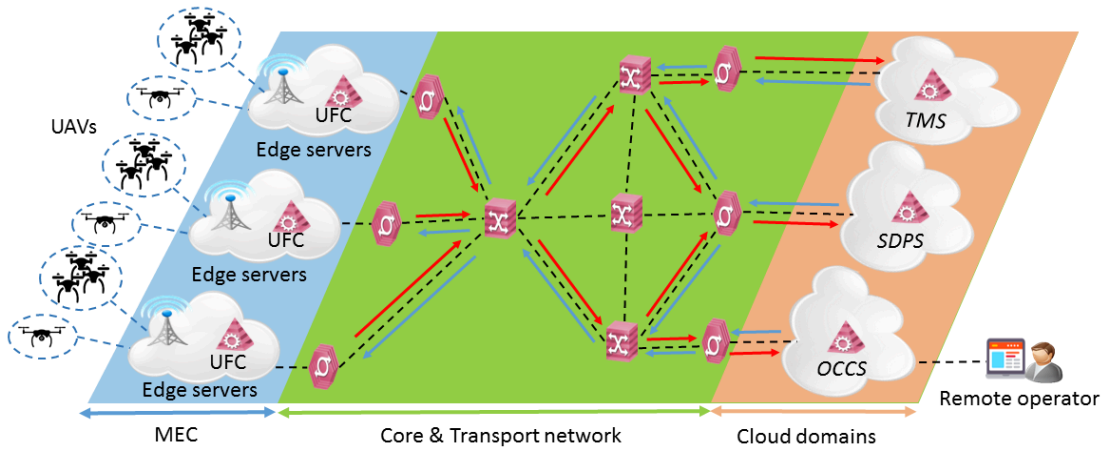
Σύμφωνα με το [170] για τις υπηρεσίες επιβολής του νόμου, η ανάπτυξη δεδομένων καθοδηγείται από τεχνολογίες όπως οι κάμερες που φορούν οι επαγγελματίες της δημόσιας ασφάλειας, οι οποίες δημιουργούν περίπου επτά terabyte δεδομένων το μήνα για ένα τυπικό αστυνομικό τμήμα (περίπου ίσο με 1.500 CD-ROM), βίντεο παρακολούθησης, αισθητήρες και άλλα. Καθώς τεράστιες ποσότητες δεδομένων παράγονται καθημερινά και «ρέουν» στις υπηρεσίες επιβολής του νόμου, η δυνατότητα διαχείρισης αυτών και απόκτησης γνώσεων από αυτά θα αλλάξει τον τρόπο με τον οποίο οι υπηρεσίες δημόσιας ασφάλειας αντιδρούν σε περιστατικά, επιλύουν υποθέσεις και εργάζονται. Χαρακτηριστικό παράδειγμα του μεγέθους των δεδομένων που οι συγκεκριμένες υπηρεσίες καλούνται να διαχειριστούν αποτελεί το περιστατικό βομβιστικής επίθεσης στο μαραθώνιο της Βοστώνης (15-05-2013), όπου εντός των 24 πρώτων ωρών από την επίθεση υπήρχαν 480.000 διακριτές εικόνες - φωτογραφίες και βίντεο, από το σημείο λίγο πριν, κατά τη διάρκεια και λίγο μετά την έκρηξη [170]. Η πρόκληση βέβαια συνίσταται στην εξαγωγή γνώσης. Στην προκειμένη περίπτωση δε, οι συγκεκριμένες εικόνες και βίντεο θα πρέπει να αξιολογηθούν στον ταχύτερο δυνατό χρόνο, ώστε να αξιοποιηθεί κατάλληλα οποιαδήποτε τυχόν πληροφορία που είναι ικανή να οδηγήσει σε σύλληψη των υπαιτίων. Αντιλαμβανόμαστε βέβαια ότι εάν δεν εμπλακεί η τεχνολογία και ο αυτοματισμός που εισάγει στην έρευνα, αυτό δεν είναι εφικτό να πραγματοποιηθεί συμβατικά, ή τουλάχιστον εάν υλοποιηθεί έτσι αυτό δεν θα είναι αποδοτικό.

Αναμφίβολο είναι ότι τα μεγάλα δεδομένα και η διαχείριση αυτών παρουσιάζουν ιδιαίτερες προκλήσεις και ευκαιρίες και για τον λόγο αυτό αποτελούν έναν αυτοτελές, ιδιαιτέρως ενδιαφέροντα και με απίστευτες προεκτάσεις κλάδο της πληροφορικής. Τα οφέλη είναι πολλαπλά, καθώς η πληροφορία είναι διαθέσιμη οποιαδήποτε στιγμή, από οιονδήποτε χρήστη έχει πρόσβαση και από οποιοδήποτε σημείο, υφίσταται δυνατότητα κλιμάκωσης της υποδομής, το κόστος είναι άμεσα συσχετισμένο με τις ανάγκες, παρέχεται ανθεκτικότητα και

ευελιξία στη διαχείριση των δεδομένων μέσω της ευρείας πρόσβασης στο δίκτυο, διασφαλίζεται η επιχειρησιακή συνέχεια, καθώς είναι εφικτή η αποκατάσταση και ανάκτηση των δεδομένων έπειτα από οποιαδήποτε καταστροφή.

Από την άλλη, στα αρνητικά της νεφοϋπολογιστικής συγκαταλέγονται στοιχεία που σχετίζονται με την ασφάλεια των δεδομένων, το υψηλό κόστος, τη δυσκολία στην παρακολούθηση των τεχνολογιών χειρισμού του cloud, την απόδοση και καθυστερήσεις κατά τη μεταφορά δεδομένων και την επίλυση προβλημάτων που ανακύπτουν, ιδιαίτερα στις περιπτώσεις αλλαγής παρόχων. Ειδικότερα για την ασφάλεια, υπάρχει μεγάλη επιφάνεια έκθεση των οργανισμών και υπηρεσιών που καταφεύγουν στις λύσεις νεφοϋπολογιστικής (διεπαφές, API, προσβασιμότητα, ανάθεση ρόλων πρόσβασης κ.λπ.).

Μια Κινητή Υπολογιστική Πλατφόρμα Εφαρμογών (Mobile Computing Applications Platform - MCAP) που βασίζεται σε νεφοϋπολογιστική υλοποιήθηκε από τους [42] με σκοπό να παρέχει βελτιωμένη επίγνωση της κατάστασης στους πρώτους ανταποκριτές.



Εικόνα 56. Αρχιτεκτονική που εμπλέκει τη νεφελοϋπολογιστική [171]

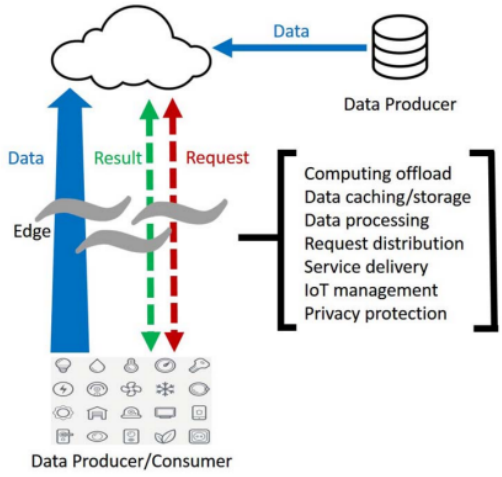
Η αρχιτεκτονική αυτής περιλαμβάνει μια πλατφόρμα με δυνατότητα σύνδεσης στο cloud για ορισμό, ανάπτυξη και λειτουργία εφαρμογών διασύνδεσης smartphones, tablets και οχημάτων. Στο [171] η αρχιτεκτονική που υλοποιήθηκε εκμεταλλεύεται τις δυνατότητες του 5G και συγκεκριμένα του Υπολογιστική Αιχμής Πολλαπλής Πρόσβασης (Multi-access Edge Computing - MEC) για να φιλοξενήσει στο cloud όλες τις υπηρεσίες διαχείρισης της εφαρμογής, στην οποία μάλιστα συμμετέχουν και UAVs. Στην Εικόνα 56 φαίνεται ξεκάθαρα ότι η Υπηρεσία Διοίκησης και Ελέγχου (Operator Command and Control Service - OCCS), η Συμπληρωματική Υπηρεσία Παρόχου Δεδομένων (Supplementary Data Provider Service – SDPS) και η Υπηρεσία Διαχείρισης Κυκλοφορίας UAV (UAVs Traffic Management Service - UTMS) ελέγχονται από τον τομέα του cloud.

Σύμφωνα με τους [172] το cloud computing θεωρείται μια ισχυρή τεχνολογία που αποσκοπεί στη βελτίωση της Ποιότητας Εμπειρίας (Quality of experience - QoE), καθώς παρέχει, με οικονομικά αποδοτικό και ελαστικό τρόπο, δυνατότητες αποθήκευσης και επεξεργασίας.

Ωστόσο, υπάρχουν εγγενείς περιορισμοί του cloud computing, στους οποίους αναφερθήκαμε ήδη και συνοψίζονται στην υψηλή καθυστέρηση, στην έλλειψη επίγνωσης του περιβάλλοντος και υποστήριξης κινητικότητας και αναποτελεσματικότητας λόγω μεγάλων χρόνων επεξεργασίας, που θέτουν σοβαρούς περιορισμούς στη χρήση σε έξυπνα περιβάλλοντα σε πραγματικό χρόνο.

4.11.2 Edge Computing

Για να αντιμετωπιστούν οι περιορισμοί του υπολογιστικού νέφους στο πλαίσιο της υποστήριξης των τεχνολογικών δομών των έξυπνων πόλεων σε πραγματικό χρόνο, που συνιστά ένα φιλόξενο περιβάλλον για την υλοποίηση των PSNs και τις εφαρμογών αυτών, η υπολογιστική ακμή (edge computing) κρίνεται ως μια βιώσιμη λύση [173]. Ο υπολογισμός αιχμής, μαζί με τις άλλες παρεμφερείς τεχνολογικές λύσεις, όπως είναι το cloudlet και το fog computing, στα οποία θα αναφερθούμε στη συνέχεια, φιλοδοξεί να καλύψει το κενό της επεξεργασίας στο άκρο του δικτύου και να φέρει έτσι στο σημείο αυτό τα εντυπωσιακά χαρακτηριστικά του cloud computing [172]. Η υπολογιστική ισχύς έρχεται πιο κοντά στα σημεία παραγωγής των δεδομένων, με σκοπό την άμεση και γρήγορη ανάλυση και επεξεργασία τους. Η ιδιότυπη αυτή αποκέντρωση των υποδομών στα συστήματα που υλοποιούνται και η τοποθέτησή τους στο «άκρο» των δικτύων μειώνει το κόστος και την πολυπλοκότητα της αρχιτεκτονικής των συστημάτων, στοιχεία απολύτως επιθυμητά στην υλοποίηση των PSNs. Επιπλέον, η μεταφορά δεδομένων στο cloud έχει ως αποτέλεσμα την κατανάλωση εύρους ζώνης, η οποία μπορεί να προκαλέσει συμφόρηση δικτύου, ή ν` αυξήσει τον κίνδυνο διαρροής δεδομένων λόγω αύξησης της επιφάνειας επίθεσης. Η λύση της υπολογιστικής ακμής εντάσσει προηγμένο υπολογιστικό υλικό στην άκρη και βελτιώνει την ικανότητα άμεσης και επιτόπιας επεξεργασίας δεδομένων [174]. Ποιος είναι ο ορισμός του «άκρου» του δικτύου, στο οποίο αναφερόμαστε; Είναι οιοσδήποτε υπολογιστικός πόρος που παρεμβάλλεται μεταξύ πηγών και του cloud. Στην Εικόνα 57 φαίνονται οι αμφίδρομες ροές υπολογισμών στα άκρα. Η λογική του υπολογιστικού άκρου είναι ότι ο υπολογισμός θα πρέπει να γίνεται κοντά σε πηγές δεδομένων. Η διαφορά με την υπολογιστική ομίχλης είναι ότι αυτή εστιάζει περισσότερο στην υποδομή, ενώ η υπολογιστική άκρων εστιάζει στα πράγματα [173]. Στον Πίνακα παρατίθεται μια συγκριτική καταγραφή των βασικών χαρακτηριστικών που παρουσιάζουν οι τεχνολογίες αυτές, όπως αυτές αναλύθηκαν και αποτυπώθηκαν στην έρευνα των [175], η οποία θα γίνει απολύτως ξεκάθαρη και με την ανάλυση για την υπολογιστή στο σύννεφο. Η εμπλοκή του edge computing και του IoT στην παροχή ασφαλέστερων πόλεων είναι αδιαμφισβήτητη (Εικόνα 58) και οφείλεται τόσο στην ευρεία ανάπτυξη των πρωτοκόλλων επικοινωνίας, όσο και σε τεχνολογίες επαυξημένης πραγματικότητας, εικονικής πραγματικότητας, ψηφιακών διδύμων και μηχανικής μάθησης [172], [176].

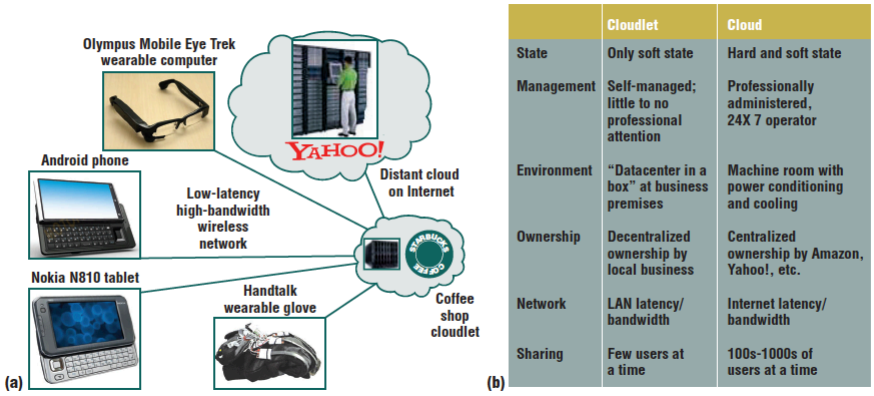


Εικόνα 57. Παράδειγμα υπολογιστικής ακμής [175]

Εικόνα 58. Edge Computing [167]

	Cloud Computing	Cloudlets	Fog Computing	Edge Computing
Επίγνωση περιεχομένου	Όχι	Χαμηλή	Μέτρια	Υψηλή
Γεωδιανομή	Κεντρικοποιημένη	Κατανεμημένη	Κατανεμημένη	Κατανεμημένη
Καθυστέρηση	Υψηλή	Χαμηλή	Χαμηλή	Χαμηλή
Κινητικότητα	Όχι / Περιορισμένη	Ναι	Ναι	Ναι
Απόσταση	Πολλαπλών μεταπηδήσεων	Μονού	Μονού / Πολλαπλών	Μονού
Επεκτασιμότητα	Ναι	Ναι	Ναι	Ναι
Ευελιξία	Ναι	Ναι	Ναι	Ναι
Κόστος ανάπτυξης	Υψηλό	Χαμηλό	Χαμηλό	Υψηλό

Πίνακας 11. Συγκριτικά στοιχεία υπολογιστικής σύννεφου και άκρων [175]



	Cloudlet	Cloud
State	Only soft state	Hard and soft state
Management	Self-managed; little to no professional attention	Professionally administered, 24X 7 operator
Environment	"Datacenter in a box" at business premises	Machine room with power conditioning and cooling
Ownership	Decentralized ownership by local business	Centralized ownership by Amazon, Yahoo!, etc.
Network	LAN latency/ bandwidth	Internet latency/ bandwidth
Sharing	Few users at a time	100s-1000s of users at a time

Εικόνα 59. (α) Το cloudlet περιλαμβάνει υπολογιστική υποδομή εγγύτητας που μπορεί να αξιοποιηθεί από κινητές συσκευές (β) Βασικές διαφορές cloudlet και cloud computing [177].

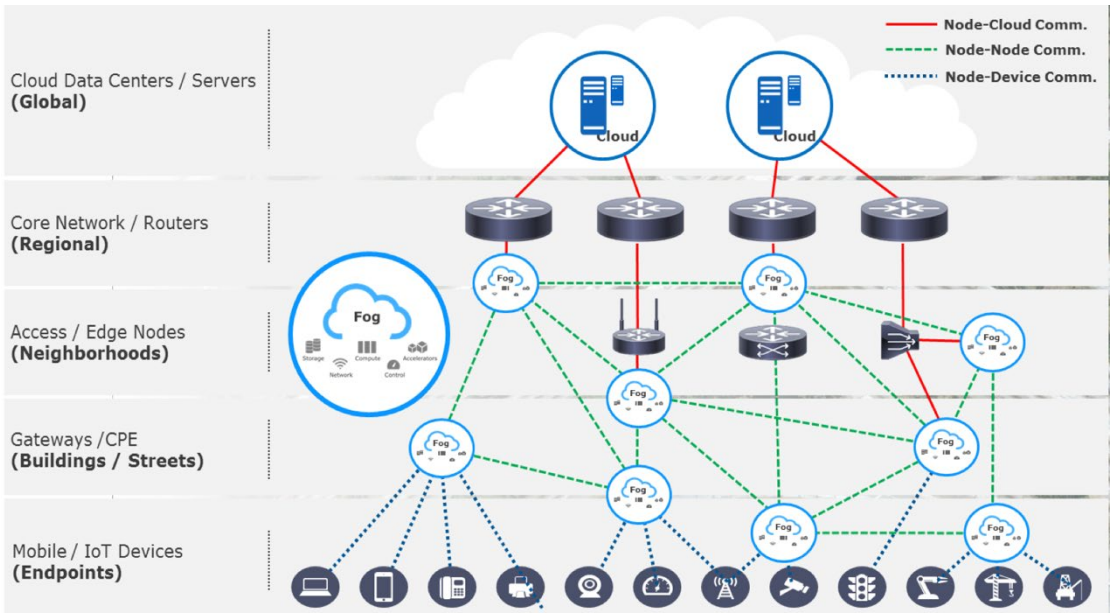
Μια άλλη κατηγορία υπολογιστικού νέφους που βρίσκεται στο άκρο και εισήχθη στην τεχνολογική πραγματικότητα με στόχο να επιλύσει τα προβλήματα μειωμένης κινητικότητας που παρουσίαζε το cloud, είναι το cloudlet. Οι κινητές συσκευές περιλαμβάνουν έναν μόνιμο συμβιβασμό, την «φτώχεια» των πόρων, η οποία εκ των πραγμάτων αποτελεί εμπόδιο στην ανάπτυξη πολλών εφαρμογών. Τη λύση φάνηκε αρχικά να δίνει το cloud, όμως οι υψηλές καθυστερήσεις τα επακόλουθα αυτών (υψηλός λανθάνων χρόνος, τρέμουλο (jitter), κ.λπ.) συνιστούν κάποια από τα θεμελιώδη εμπόδια [177]. Η έννοια του cloudlet και οι διαφορές του με το cloud αποτυπώνονται στην Εικόνα 59. Σε σχέση με τις διαφορές, αυτές εστιάζονται στην κατάσταση, τη διαχείριση, το περιβάλλον ανάπτυξης, το ιδιοκτησιακό καθεστώς της υποδομής, το δίκτυο διασύνδεσης και τον αριθμό των χρηστών που διαμοιράζονται τους πόρους. Ταυτόσημος τεχνολογικά όρος με αυτόν του cloudlet είναι και το Ακολούθησέ με Σύννεφο (Follow-Me Cloud – FMC), έτσι όπως αναλυτικά αποδίδεται στο [178], καθώς το πλαίσιο FMC στοχεύει να παρέχει κινητικότητα στις υπηρεσίες cloud, ακολουθώντας τους χρήστες με μετεγκατάσταση των απαιτούμενων τμημάτων και υπηρεσιών που προτείνεται, ώστε να εξασφαλιστεί το απαιτούμενο QoE. Μια εκτενής περιγραφή του τρόπου λειτουργία των cloudlet και η αρχιτεκτονική αυτών παρουσιάζεται στο [179]. Στο ίδιο άρθρο ορίζεται ότι το cloudlet αφορά σε ένα σύνολο αξιόπιστων υπολογιστών με πλούσιους πόρους που είναι καλά συνδεδεμένοι στο διαδίκτυο και είναι διαθέσιμοι για χρήστες κινητών συσκευών που βρίσκονται κοντά. Δεν απαιτείται να βρίσκονται σε μια σταθερή υποδομή κοντά στο σημείο ασύρματης πρόσβασης, αλλά διαμορφώνονται με δυναμικό τρόπο με οποιαδήποτε συσκευή σε ένα δίκτυο LAN.

4.11.3 Fog Computing.

Ο υπολογισμός ομίχλης (Fog Computing) αναφέρθηκε από τη Cisco το 2012 [180]. Το όνομα περιγράφει την εγγύτητα των υπολογισμών στο σημείο που δημιουργούνται τα δεδομένα, παραλληλίζοντας την εγγύτητα της ομίχλης στο έδαφος. Μάλιστα, πολλοί άνθρωποι

χρησιμοποιούν τους όρους fog computing και edge computing εναλλακτικά, επειδή και οι δύο περιλαμβάνουν την προσέγγιση της νοημοσύνης και της επεξεργασίας στο σημείο όπου δημιουργούνται τα δεδομένα, για τη βελτίωση της αποτελεσματικότητας. Σύμφωνα με την Κοινοπραξία OpenFog (OpenFog Consortium) που ξεκίνησε η Cisco το 2015 σε συνεργασία με άλλους τηλεπικοινωνιακούς και τεχνολογικού κολοσσούς (Microsoft, Dell, Intel, ARM) και το Πανεπιστήμιο του Πρίνστον, η βασική διαφορά μεταξύ του edge και του fog computing είναι το σημείο που τοποθετείται η νοημοσύνη και η υπολογιστική ισχύς [181].

Οι κόμβοι fog computing που αποτελούν μέρος εφαρμογών μιας έξυπνης πόλης σχηματίζουν ένα πλέγμα για να παρέχουν εξισορρόπηση φορτίου, ανθεκτικότητα, ανοχή σφαλμάτων και ελαχιστοποίηση της επικοινωνίας cloud (Εικόνα 60). Επιπλέον, έχουν τη δυνατότητα να επικοινωνούν σε κάθε κατεύθυνση (peer-to-peer), να ανακαλύπτουν, εμπιστεύονται και χρησιμοποιούν τις υπηρεσίες άλλου κόμβου, προκειμένου να δημιουργήσουν αξιοπιστία, διαθεσιμότητα, εμπιστευτικότητα [182].



Εικόνα 60. Σύνδεση κόμβων fog computing σε μια έξυπνη πόλη [182]

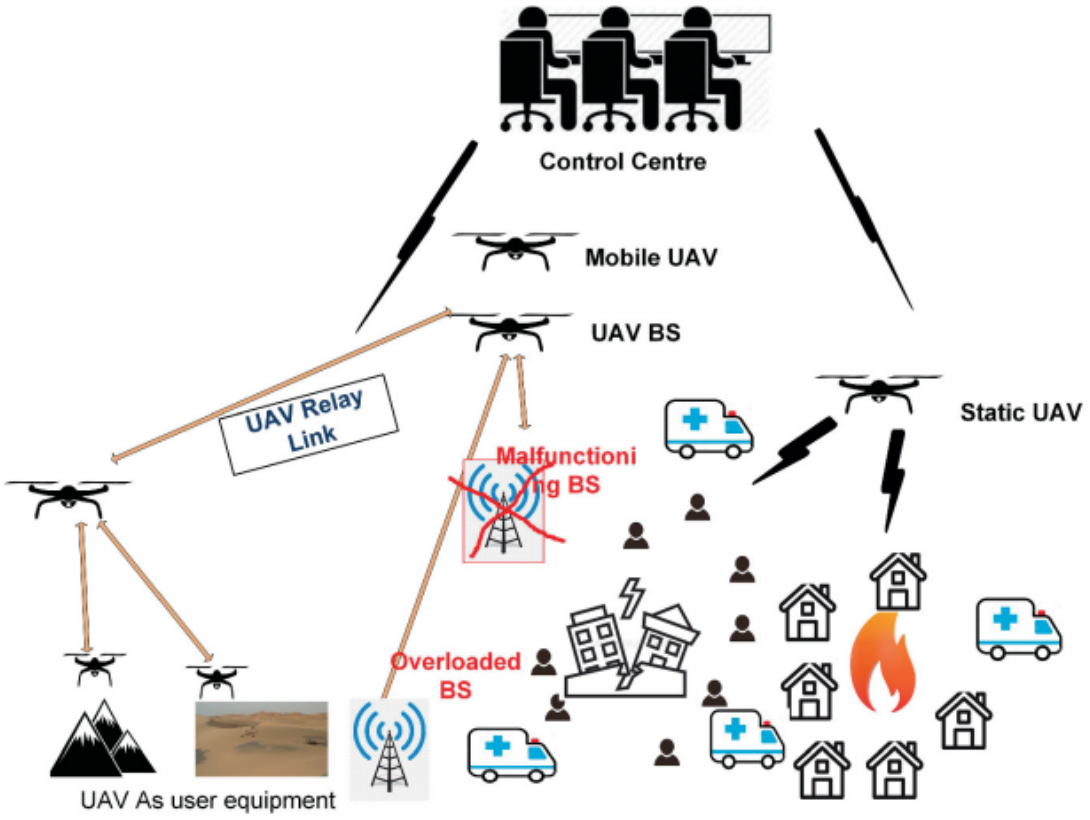
Μια επισκόπηση του fog computing επιχειρήθηκε από τους [183], οι οποίοι αναφέρθηκαν στην ενσωμάτωση των τεχνολογιών αυτών για την εξυπηρέτηση ενός συστήματος με τον όρο ολοκληρωμένο σύστημα IoT-fog-cloud (iIFC), το οποίο συνιστά μια ολοκληρωμένη, προηγμένη πλατφόρμα για την ανάπτυξη και λειτουργία διαφόρων τύπων εφαρμογών στις έξυπνες πόλεις. Στόχος αποτελούν οι καλύτερες δυνατότητες και απόδοση του συστήματος που υποστηρίζουν. Τα οφέλη μπορούν να καρπωθούν εφαρμογές δημόσιας ασφάλειας, που υποστηρίζουν ένα PSN. Αυτά συνοψίζονται στη διατήρηση του εύρους ζώνης, λόγω του μικρότερου όγκου δεδομένων που αποστέλλονται συγκριτικά με το cloud και ο βελτιωμένος χρόνος απόκρισης, ενώ στα αρνητικά εντάσσονται τα ζητήματα ασφάλειας και το κόστος, λόγω της χρήσης αυξημένων πόρων.

4.12 Unmanned Aerial Vehicle

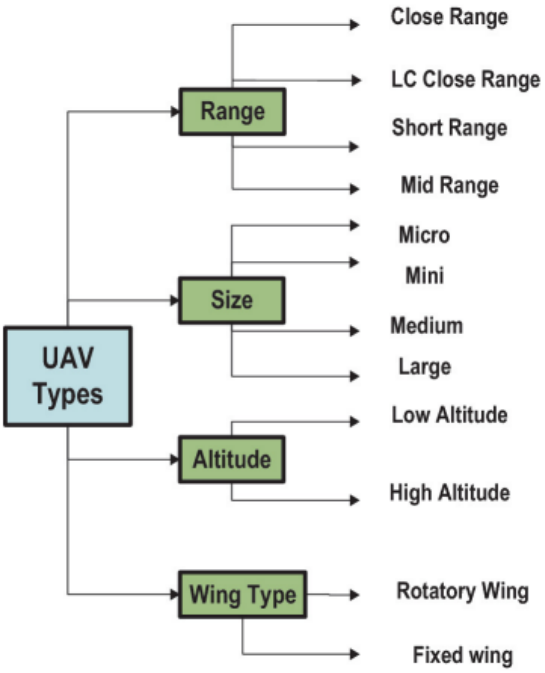
Τα μη επανδρωμένα εναέρια οχήματα (Unmanned Aerial Vehicles - UAVs) γνωστά και ως drones δεν αποτελούν μια τεχνολογία ή κάποιο ξεχωριστό πρότυπο επικοινωνίας, αλλά μια λύση υλικού που εμπλέκεται κυρίως στην υβριδική υλοποίηση δικτύων δημόσιας ασφάλειας, ή στην υποστήριξη αυτών σε περίπτωση που λαμβάνουν χώρα ζημιές στην υποδομή. [44]. Τα UAVs έχουν σημαντική δυναμική στην υποστήριξη των σύγχρονων PSNs, όπως θα γίνει ξεκάθαρο στη συνέχεια και η συμμετοχή τους στη δημόσια ασφάλεια εμφανίζεται ως τάση που ολοένα κερδίζει έδαφος [184]. Μάλιστα, τα συστήματα πολλαπλών UAVs, λειτουργώντας συνεργατικά, μπορούν να ολοκληρώσουν πιο αποτελεσματικά και σαφώς πιο οικονομικά διάφορες αποστολές συγκριτικά με ένα μόνο UAV [185].

Βέβαια, υπάρχουν ακόμη αρκετά ζητήματα που πρέπει να επιλυθούν και τα οποία αποτελούν τεχνολογικές προκλήσεις, για την αξιόπιστη ένταξή τους στα δίκτυα δημόσιας ασφάλειας. Τα UAVs μπορούν να υποστηρίξουν δυναμικά όλων των ειδών τα δίκτυα (MANETs, VANETs, ad-hoc, κ.λπ.) που δύναται να αποτελέσουν δομικά στοιχεία ενός δικτύου κρίσιμων επικοινωνιών. Ο ξαφνικός τρόπος με τον οποίο εμφανίζονται και πολλαπλασιάζονται οι απαιτήσεις και ανάγκες για τα δίκτυα δημόσιας ασφάλειας απαιτεί άμεσα αναπτυσσόμενα μέσα επικοινωνίας, που θα υποστηρίξουν την υφιστάμενη υποδομή. Όπως είναι αντιληπτό, θα ήταν οικονομικά ασύμφορο να υποστηρίξουμε αυτά με μόνιμες εγκαταστάσεις που θα παρείχαν υψηλής χωρητικότητας PSNs, καθώς με τον τρόπο αυτό θα εγκλωβίζαμε για αρκετό χρονικό διάστημα πόρους που θα ήταν αδρανείς [186]. Μια αρχιτεκτονική ενός PSN με την εμπλοκή UAVs, στη γενική της λογική λειτουργίας, θα είχε την μορφή που φαίνεται στην Εικόνα 61 [44].

Τα UAV μπορούν να χρησιμοποιηθούν και να υποστηρίξουν ένα PSN με διαφορετικό τρόπο και συγκεκριμένα είτε ως εναέριοι σταθμοί βάσης, που έχει ως αποτέλεσμα τη βελτίωση της κάλυψης, της χωρητικότητας, της αξιοπιστίας και της ενεργειακής απόδοσης των ασύρματων δικτύων, είτε ως ιπτάμενα κινητά τερματικά μέσα σε ένα δίκτυο κινητής τηλεφωνίας, ενεργοποιώντας μια ευρεία γκάμα εφαρμογών, από ροή βίντεο σε πραγματικό χρόνο έως παράδοση αντικειμένων [184].



Εικόνα 61. PSN με τη βοήθεια UAVs [44]

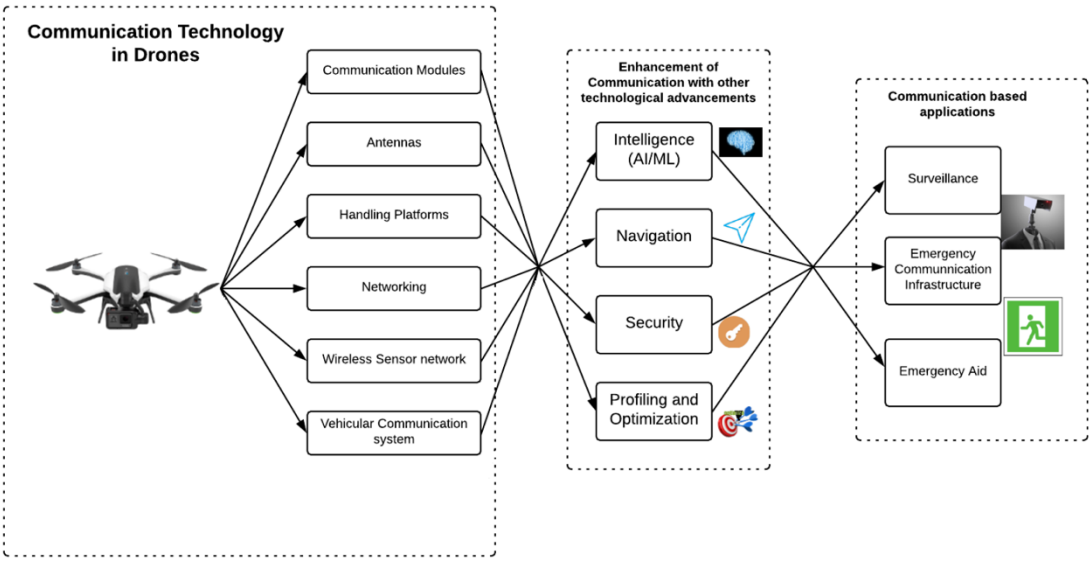


Εικόνα 62. Είδη των UAVs [44]

Η κατηγοριοποίηση των πολλών και διαφορετικών ειδών UAVs μπορεί να γίνει με βάση διαφορετικά, κάθε φορά, χαρακτηριστικά και συγκεκριμένα την εμβέλεια (range), το μέγεθος (size), το ύψος υπέρπτησης (altitude), ή το είδος των φτερών (wing type) (Εικόνα 62). Σε

κάθε περίπτωση και ανάλογα με τις απαιτήσεις που επιχειρούμε να καλύψουμε χρησιμοποιούμε διαφορετικών ειδών UAVs ή συνδυασμό αυτών [44]. Ταξινόμηση βέβαια μπορεί να υπάρξει και με βάση άλλα χαρακτηριστικά ή κατηγορίες. Οι [186] ομαδοποιούν τα UAVs σε τρεις μεγάλες κατηγορίες: (α)με βάση το υψόμετρο, (β)με βάση το δίκτυο και (γ)με βάση τις εφαρμογές που υλοποιούν και στη συνέχεια εστιάζουν στην προοπτική της ενεργειακής απόδοσης των UAVs (Εικόνα 66).

Ανεξάρτητα από τον τρόπο που κατηγοριοποιούμε τα UAVs, το πεδίο εφαρμογών τους παρουσιάζει έναν αξιοσημείωτο πλουραλισμό. Στην Εικόνα 63 προκύπτουν διαγραμματικά οι αλληλοσυνδέσεις και αλληλεξαρτήσεις μεταξύ των τριών διακριτών τμημάτων που ορίζονται ως (α)τεχνολογίες επικοινωνίας προσαρμοσμένες σε UAVs (συστήματα επικοινωνίας, κεραίες, συστήματα δικτύωσης, κ.λπ.), (β)ενίσχυση της επικοινωνίας με άλλες τεχνολογικές εξελίξεις (τεχνητή νοημοσύνη, ασφάλεια, κ.λπ.) και (γ)εφαρμογές που βασίζονται στην επικοινωνία (επιτήρηση, υποδομή επείγουσας επικοινωνίας και βοήθειας) [187]. Εάν, για παράδειγμα, υπάρχει επικοινωνία μεταξύ ενός UAV και ενός ασθενοφόρου, μέσω ενός εξελιγμένου συστήματος επικοινωνίας σε όχημα, ένας αλγόριθμος τεχνητής νοημοσύνης μπορεί να ενεργοποιείται είτε εκτός σύνδεσης σε UAV, είτε online στο cloud, με σκοπό να παρακολουθεί τις διαδρομές ενός ασθενοφόρου και να καθορίσει την καλύτερη διαδρομή για την παροχή βοήθειας έκτακτης ανάγκης.



Εικόνα 63. Πεδίο εφαρμογής της τεχνολογίας επικοινωνίας με drones [187]

Για τις ανάγκες των επικοινωνιών δημόσιας ασφάλειας, τα UAVs μπορούν να χρησιμοποιούν επικοινωνίες με επίκεντρο τη συσκευή, καθιστώντας έτσι εφικτή την απ` ευθείας σύνδεση συσκευών – χρηστών με τα UAVs, ιδιαίτερα σε καταστάσεις καταστροφής των επίγειων σταθμών βάσης (Terrestrial Base Stations - TBSs), χωρίς να υφίσταται εναλλακτικό κανάλι επικοινωνίας. Έτσι, οι υπηρεσίες δημόσιας ασφάλειας, όπως MCPTT, ελέγχου και

δεδομένων, μεταφοράς φωνής, βίντεο και ομαδικών κλήσεων, μπορούν να βασιστούν σε UAVs. Οι αρχιτεκτονικές που έχουν κατά καιρούς προταθεί στο πλαίσιο επιστημονικών εργασιών φιλοδοξούν να δώσουν ικανοποιητικές λύσεις στα προβλήματα που παρουσιάζει η ενεργός εμπλοκή των UAVs στην υλοποίηση των PSNs. Τα κυριότερα εξ αυτών που συνιστούν ταυτόχρονα προκλήσεις υλοποίησης είναι (Εικόνα 64):

1. Τοποθέτηση. Την ονομάζουμε τοποθέτηση 3D, καθώς θα πρέπει να προσδιοριστεί η βέλτιστη θέση στο χώρο γεγονός που αυξάνει τη δυσκολία, καθώς συνιστά ένα πολυπαραγοντικό πρόβλημα, με δεδομένο ότι θα πρέπει να συνυπολογιστούν παράγοντες που σχετίζονται με τη θέση των χρηστών, τις συνθήκες του καναλιού, τους ενεργειακούς περιορισμούς και τις παρεμβολές με άλλα UAVs. Στο [188] προτείνεται μια μέθοδος για την εύρεση των θέσεων των σταθμών βάσης επί των UAVs χρησιμοποιώντας έναν ευριστικό αλγόριθμο (Εικόνα 65).

2. Διαχείριση πόρων. Η αποτελεσματική διαχείριση πόρων του PSN που υποστηρίζεται από UAVs συνιστά σχεδιαστική πρόκληση επειδή οι πόροι είναι κοινοί και με τα υπόλοιπα στοιχεία της υποδομής του δικτύου.

3. Σχεδιασμός τροχιάς. Είναι ένα πρόβλημα βελτιστοποίησης, καθώς αναζητούμε το καλύτερο «μονοπάτι», δηλαδή τη διαδρομή που θα μεγιστοποιεί ή ελαχιστοποιεί, κατά περίπτωση βασικούς δείκτες, όπως ενέργεια, ισχύς, μήκος διαδρομής, χρόνος απόκρισης, καθυστερήσεις, κ.λπ.. Πολλές παράμετροι εμπλέκονται, ενώ σε περιπτώσεις πολλαπλών UAVs θα πρέπει να συνυπολογιστεί και η αποφυγή σύγκρουσης μεταξύ τους. Μια προσπάθεια σχεδιασμού της τροχιάς πολλαπλών UAVs που συμμετέχουν σε επιτήρηση για εφαρμογή δημόσιας ασφάλειας έγινε από τους [189], οι οποίοι θίγουν και το σοβαρό ζήτημα της έλλειψης νομοθετικού πλαισίου και της ύπαρξης πολλών παράνομων UAVs που συνιστούν κίνδυνο (Εικόνα 65).

4. Χειρισμός παρεμβολών. Όπως έχουμε ήδη αναφέρει για μεγιστοποίηση της απόδοσης του δικτύου κάλυψης πολλές φορές τα PSNs περιλαμβάνουν πολλά UAVs. Τότε όμως γεννάται ζήτημα παρεμβολών μεταξύ τους καθώς αναζητούμε τον τρόπο να λαμβάνουμε τη μέγιστη δυνατή κάλυψη από κάθε ένα UAV, χωρίς το κόστος παρεμβολών γειτονικών UAVs.

5. Μοντελοποίηση καναλιών. Η ποιότητα της επικοινωνίας καθορίζεται σε πολύ μεγάλο βαθμό από τα χαρακτηριστικά του καναλιού πομπού / δέκτη. Στην περίπτωση των UAVs που συμμετέχουν σε PSN η μοντελοποίηση είναι ακόμη δυσκολότερη συγκριτικά με επίγεια υποβοηθούμενα PSNs, καθώς το κανάλι που πρέπει να μοντελοποιηθεί είναι αέρος – εδάφους. Τα χαρακτηριστικά προβλήματα τέτοιου

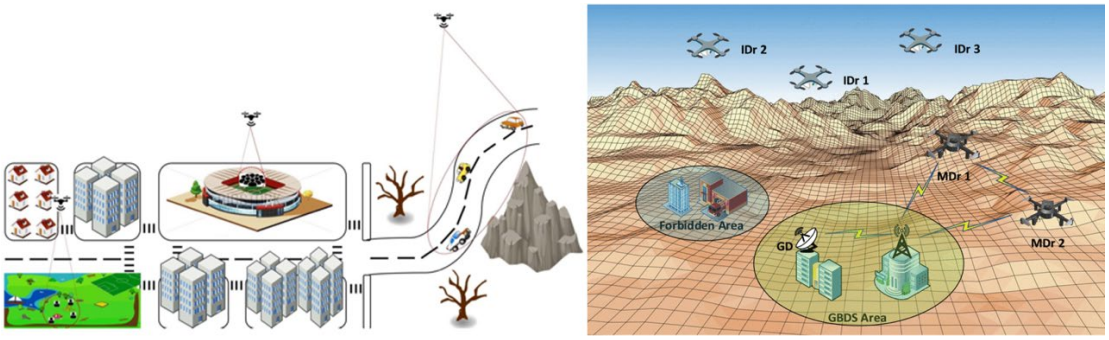
είδους επικοινωνίας επιχείρησαν να αναδείξουν οι [190], οι οποίοι μελέτησαν την επίδραση της βροχής, των σύννεφων, της απορρόφησης αερίων και εξασθένισης πολλαπλών διαδρομών στη σύνδεση αέρα – εδάφους των HAPs, στα οποία θα αναφερθούμε εκτενώς στο 5.2.2.2.

6. Συνδεσιμότητα οπισθοζεύξης. Η συνδεσιμότητα οπισθοζεύξης που απαιτούν τα UAVs που συμμετέχουν στο PSN είναι ασύρματη και υλοποιείται, όπως αναφέραμε ήδη στο 4.9 με mmWave, ή με WiFi (4.10.1), ή με δορυφορικές συνδέσεις (5.2.2.1). Ο δορυφόρος προσφέρει μεγάλη χωρητικότητα, αλλά μεγαλύτερες καθυστερήσεις και υψηλό κόστος. Χαμηλό κόστος και μικρές καθυστερήσεις προσφέρει το Wi-Fi backhauling, τον οποίο το καθιστά τον πιθανότερο υποψήφιο για οπισθοζεύξη (backhauling). Μια αξιόλογη μελέτη παρουσιάζεται στην εργασία των [191], οι οποίοι ασχολήθηκαν με τη δορυφορική κατερχόμενη οπισθοζεύξη που επιτυγχάνεται με μια πλατφόρμα μεγάλου υψομέτρου (HAP), συγκριτικά και με οπτικές συνδέσεις.

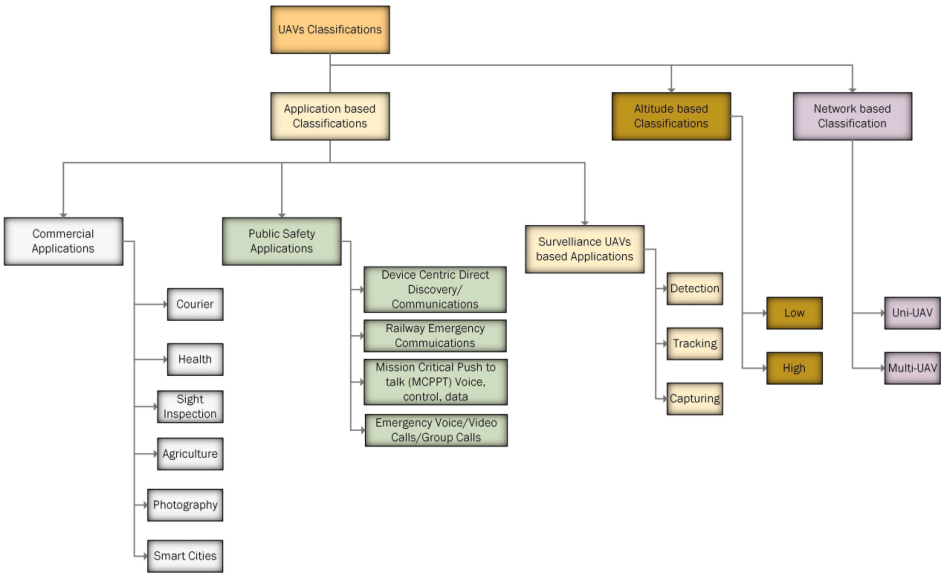
7. Περιορισμός ενέργειας. Η περιορισμένη μπαταρία είναι μια σημαντική πρόκληση της λειτουργίας των UAVs. Οι μπαταρίες φέρονται από τα UAVs και ως εκ τούτου οι ενεργειακές απαιτήσεις που θα δημιουργηθούν από τα συστήματα που φέρουν και αναλαμβάνουν την επεξεργασία πληροφοριών, τη διαχείριση κινητικότητας, τον έλεγχο επικοινωνίας, κ.αλ. έχουν πεπερασμένα όρια. Οι έρευνες στο συγκεκριμένο πεδίο επικεντρώνονται στην εύρεση αποτελεσματικής χρήσης της ενέργειας που συνεπάγεται την παράταση ζωής της μπαταρίας των UAVs. Μια χαρακτηριστική προσπάθεια μελέτης για ενεργειακά αποδοτική επικοινωνία UAV μέσω βελτιστοποίησης τροχιάς είναι η [192].

8. Ασφάλεια. Οι συνδέσεις επικοινωνίας των UAVs είναι ασύρματες, επομένως ευάλωτες από τυχόν επιτήδειους. Η ασφάλεια γίνεται δυσκολότερη και από την τοπολογία του δικτύου. Διάφορες λύσεις έχουν προταθεί στη βιβλιογραφία, οι οποίες βασίζονται τόσο σε συμβατικές μεθόδους (πολλαπλές κεραίες, κατάλληλη επιλογή ρελέ, επεξεργασία σήματος), όσο και σε προηγμένες (τεχνητή νοημοσύνη). Οι τρωτότητες και πιθανές απειλές αναλύονται εμπεριστατωμένα στο [193]

Εικόνα 64. Προκλήσεις υλοποίησης PSNs με εμπλοκή UAVs [50]



Εικόνα 65. Ενδεικτικά ζητήματα προκλήσεων υλοποίησης PSN με εμπλοκή UAVs: (a)Τοποθέτηση 3D [188] και (b)Σχεδιασμός τροχιάς [189].



Εικόνα 66. Κατηγοριοποίηση UAVs με βάση τις εφαρμογές, το υψόμετρο και την υποδομή δικτύου [186].

Είναι γεγονός ότι για την εμπλοκή των UAVs στην αποδοτική υποστήριξη ενός PSN υπάρχουν στη βιβλιογραφία πληθώρα ερευνών. Κάποιες εξ αυτών φιλοδοξούν να καλύψουν ένα πολύ συγκεκριμένο ερευνητικό πεδίο, ή να προτείνουν μια πιθανά εφικτή λύση για μια τεχνολογική πρόκληση και άλλες που υλοποιήθηκαν στο πλαίσιο συγκεκριμένου ερευνητικού έργου. Χαρακτηριστική περίπτωση από τις τελευταίες αποτελεί το έργο FASTER, στο οποίο θα αναφερθούμε εκτενώς στη συνέχεια, στην αρχιτεκτονική του οποίου εντάχθηκαν τα UAVs. Μάλιστα, αναφέρονται στη δημιουργία μια ειδικής περίπτωσης ad-hoc δικτύου, ενός Flying ad-hoc δίκτυο (FANET) το οποίο υλοποιείται με τη συμμετοχή σμήνους UAVs (Swarm Unmanned Aerial Vehicles - SUAVs) και το οποίο υποστηρίζει ένα PSN. Στο [194] μελετήθηκε η συμπεριφορά κάθε UAV, ως ξεχωριστή οντότητα, μέσα σε ένα δίκτυο σμήνους και αναδείχθηκαν τα προβλήματα του SUAVs που σχετίζονται με την αυτόνομη πλοήγησή του μέσα από διαφορετικά, η δημιουργία βέλτιστων διαδρομών για να διασφαλιστεί ότι τα UAVs επιτυγχάνουν τους στόχους τους με ασφαλή και συντονισμένο τρόπο. Στην ίδια κατεύθυνση μάλιστα, στο [195] ερευνήθηκε η δυνατότητα αυτόνομης λειτουργίας των SUAVs, η κατανομή εργασιών και ο αλληλοσυντονισμός τους, τα οποία προϋποθέτουν την επικοινωνία UAV προς UAV.

Σε κάθε περίπτωση, οι προκλήσεις εξακολουθούν να είναι πολλές και σημαντικές. Με δεδομένο όμως ότι τα UAVs αποτελούν ένα εργαλείο που έχει ήδη αποδείξει ότι μπορεί να υποστηρίξει την αποδοτική λειτουργία των PSNs, ακόμη και με κάποια προβλήματα, εκτιμάται ως σχεδόν βέβαιο ότι τα μελλοντικά PSNs θα έχουν στην υβριδική αρχιτεκτονική και UAVs και ότι τα βήματα που αναμένουμε να δούμε στο συγκεκριμένο πεδίο θα συμβαδίζουν με τον γοργό ρυθμό που κινούνται οι τεχνολογικές εξελίξεις γύρω από αυτά.

4.13 Optical Communications

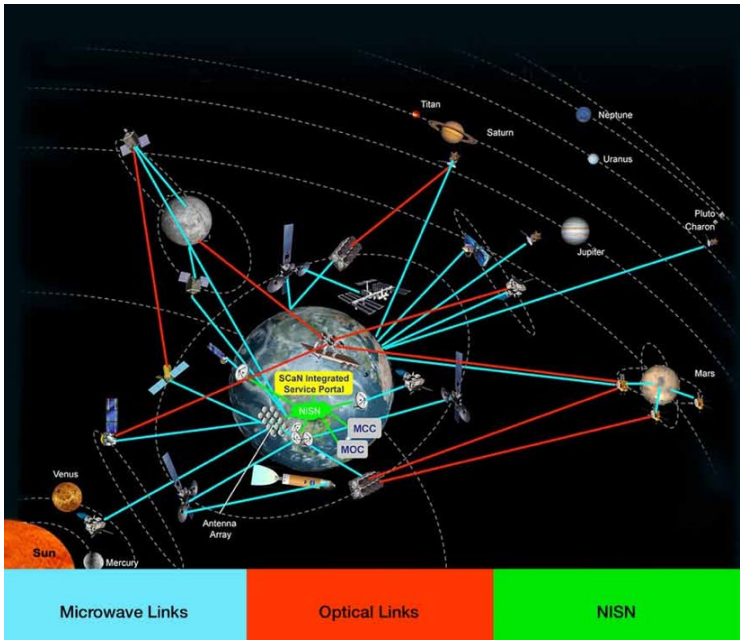
4.13.1 Γενικά

Η τεχνολογία ασύρματων οπτικών επικοινωνιών (Wireless Optical Communications - WOC) σε καταστάσεις που απαιτείται η δημόσια ασφάλεια και η αποκατάσταση καταστροφών δεν είναι ιδιαίτερα διαδεδομένη, βρίσκεται όμως σε ένα ώριμο στάδιο [196] και κινείται με ταχείς ρυθμούς. Η διαστημική υπηρεσία των ΗΠΑ (NASA) πρωτοπορεί με μια σειρά από έργα της [197] που αφορούν τις ασύρματες οπτικές επικοινωνίες στο διάστημα (Free Space Optical – FSO) (Πίνακας 12), ενώ σήμερα υπάρχουν πολλές στρατιωτικές εφαρμογές καθώς και αρκετές εμπορικές υλοποιήσεις [198]. Παρά το γεγονός πως η χρήση των WOC έχει μελετηθεί για αρκετές δεκαετίες, η διάδοση τους ξεκίνησε ουσιαστικά στα τέλη τις δεκαετίας του 1990 αρχές του 2000 [199].

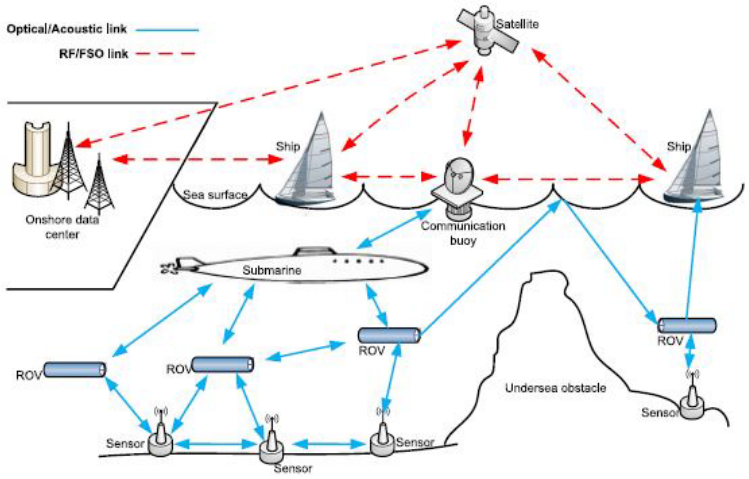
Η σημασία της τεχνολογία των WOC σε εφαρμογές δημόσιας ασφάλειας και αποκατάστασης καταστροφών (Public Safety Disaster Recovery - PSDR) είναι σημαντική και ιδιαίτερα ενδιαφέρουσα διότι παρέχει μεγάλο εύρος ζώνης, μεγάλη ταχύτητα δεδομένων, πολύ μικρή καθυστέρηση, μεγαλύτερη ασφάλεια, μικρότερο χρόνο εγκατάστασης, δεν απαιτεί αδειοδοτημένο φάσμα, έχει μικρότερα κόστη, διαθέτει απλότητα στο σχεδιασμό [200], γεγονός που καλύπτει τις σύγχρονες απαιτήσεις των πρώτων ανταποκριτών για μετάδοση σε πραγματικό χρόνο βίντεο και δεδομένων. Είναι επίσης σημαντικό να τονίσουμε πως οι WOC βρίσκουν εφαρμογή στο διάστημα στον αέρα, στη γη αλλά και υποθαλάσσια [201] (Εικόνα 68) με αρκετά σημαντικά πλεονεκτήματα έναντι των ραδιοεπικοινωνιών. Παρόλα αυτά οι WOC έχουν και ορισμένους περιορισμούς που οφείλονται κυρίως στην απαίτηση άμεσης οπτικής επαφής ανάμεσα στα σημεία εκπομπής και λήψης, και αυτό είναι κάτι που η ερευνητική κοινότητα προσπαθεί να βρει λύσεις κυρίως με τη χρήση υβριδικών συστημάτων επικοινωνίας FSO/RF.

α/α	Πρόγραμμα	Ρυθμοί Μετάδοσης	Κατερχόμενη ζεύξη	Ανερχόμενη ζεύξη	Χρήση
1	Laser Communications Relay Demonstration (LCRD) [202]	1.2 Gbps	-	-	Επικοινωνίες υψηλής ταχύτητας δεδομένων μεταξύ διαστημικών σκαφών και επίγειων σταθμών
2	Lunar Laser Communications Demonstration (LLCD) [203]		622 Mbps	20 Mbps	Επικοινωνίες υψηλής ταχύτητας δεδομένων μεταξύ της Σελήνης - Γης
3	Space Telecommunications Radio System (STRS) [204]	Έως 1 Gbps			Επικοινωνίες στο περιβάλλον του βαθέως διαστήματος
4	Laser Communications and Sensor Demonstration (LCSD) [205]	200 Mbps			Επικοινωνίες μεταξύ CubeSats και επίγειων σταθμών

Πίνακας 12. Προγράμματα της NASA με χρήση FSO επικοινωνιών



Εικόνα 67. Με κόκκινο οι συνδέσεις FSO Communication ανάμεσα στους σταθμούς, πηγή:NASA



Εικόνα 68. Υποθαλάσσιο δίκτυο αισθητήρων με χρήση οπτικών επικοινωνιών σε συνεργασία με επίγειο και δορυφορικό δίκτυο ραδιοεπικοινωνιών [201]

4.13.2 Ο ρόλος των οπτικών επικοινωνιών στη δημόσια ασφάλεια

Ο ρόλος των WOC σε καταστάσεις διαχείρισης καταστροφών και δημόσιας ασφάλειας είναι να παρέχει αξιόπιστες και ασφαλείς επικοινωνίες σε καταστάσεις έκτακτης ανάγκης. Τα συστήματα οπτικών επικοινωνιών μπορούν να χρησιμοποιηθούν για τη μετάδοση κρίσιμων πληροφοριών, παρέχοντας δυνατότητες για διοίκηση και έλεγχο, υποστήριξη αποστολών έρευνας και διάσωσης καθώς και δυνατότητες μετάδοσης σε πραγματικό χρόνο της πραγματικής εικόνας από την πληγείσα περιοχή. Σε σενάρια καταστροφών, παραδοσιακές επικοινωνίες όπως η κινητή τηλεφωνία και οι δορυφορικές επικοινωνίες θα μπορούσαν να υπερφορτωθούν, καθιστώντας δύσκολη την παροχή αξιόπιστων επικοινωνιών. Έτσι οι οπτικές επικοινωνίες θα μπορούσαν να αποτελέσουν ένα εναλλακτικό κανάλι επικοινωνίας το οποίο είναι ανθεκτικό σε παρεμβολές και μπορεί να λειτουργήσει σε δύσκολες περιβαλλοντικές συνθήκες. Η χρήση των συστημάτων οπτικών επικοινωνιών θα μπορούσε να χρησιμοποιηθεί για την ανάπτυξη δικτύων κρίσιμων επικοινωνιών σε περιοχές που έχουν υποστεί μεγάλες καταστροφές, εξασφαλίζοντας υπηρεσίες δεδομένων και φωνής τόσο για τους πρώτους ανταποκριτές όσο και για το υπόλοιπο προσωπικό που λειτουργεί υποστηρικτικά. Η πληροφορίες αφορούν την αναμετάδοση κρίσιμων πληροφοριών όπως το γεωγραφικό στίγμα των αγνοουμένων, την έκταση των ζημιών αλλά και πληροφορίες για την κατάσταση των υποδομών.

Οι οπτικές επικοινωνίες επίσης μπορούν να αξιοποιηθούν σε αποστολές έρευνας και διάσωσης παρέχοντας τη δυνατότητα για μεταφορά σε πραγματικό χρόνο βίντεο και δεδομένων ανάμεσα στους πρώτους ανταποκριτές και τα κέντρα ελέγχου και διοίκησης. Αυτό επιτρέπει τη δημιουργία κοινής επιχειρησιακής εικόνας ενισχύοντας τον αποδοτικότερο συντονισμό των επιχειρήσεων έρευνας και διάσωσης αποσκοπώντας στη μείωση του χρόνου

αναζήτησης και διάσωσης των αγνοουμένων. Επιπρόσθετα, οι WOC μπορούν να χρησιμοποιηθούν για την επιτήρηση την πληγείσας περιοχής, παρέχοντας δεδομένα σε πραγματικό χρόνο για τις επικρατούσες περιβαλλοντικές συνθήκες όπως επίσης και την κατάσταση των κρίσιμων υποδομών. Αυτές οι πληροφορίες θα μπορούσαν να αξιοποιηθούν για την πρόβλεψη και πρόληψη από δευτερεύοντες κινδύνους, όπως πυρκαγιές και διαρροές νερού. Μια επίσης σημαντική παράμετρο είναι η ασφάλεια των επικοινωνιών που διαθέτουν οι οπτικές επικοινωνίες διασφαλίζοντας την μετάδοση ευαίσθητων πληροφοριών, όπως οι εντολές και οδηγίες από τα κέντρα διοίκησης και ελέγχου, χωρίς τον κίνδυνο παρεμβολών ή υποκλοπών.

Οι WOC ως τεχνολογία χρησιμοποιούν ακτίνες laser για την μετάδοση των δεδομένων μέσω του αέρα, διαθέτουν αρκετά πλεονεκτήματα αλλά και μειονεκτήματα συγκριτικά με τις άλλες παραδοσιακές τεχνολογίες ασύρματων επικοινωνιών. Τα πλεονεκτήματα που αυτά εμφανίζουν είναι:

- Υψηλός ρυθμός μετάδοσης δεδομένων [200], της τάξης αρκετών Gbit/s, ο οποίος είναι πολύ υψηλότερος από τις αντίστοιχες παραδοσιακές ασύρματες τεχνολογίες όπως το Wi-Fi.
- Υψηλή ασφάλεια, καθώς οι WOC χρησιμοποιούν κατευθυνόμενες ακτίνες laser ανάμεσα στους κόμβους γεγονός που καθιστά δύσκολη την υποκλοπή από τρίτους μη εξουσιοδοτημένους χρήστες [200].
- Δεν επηρεάζονται από ηλεκτρομαγνητικές παρεμβολές (EMI) και έτσι αποτελούν μια πιο αξιόπιστη επιλογή για χρήση σε περιοχές με υψηλά επίπεδα EMI [200].
- Χαμηλή κατανάλωση ενέργειας: Οι οπτικές επικοινωνίες μπορούν να μεταδώσουν δεδομένα με μικρότερη ισχύ από τα παραδοσιακά συστήματα ασύρματης επικοινωνίας, κάτι που μπορεί να είναι σημαντικό για την επικοινωνία σε απομακρυσμένες περιοχές, ή περιοχές που έχουν πληγεί από καταστροφές, όπου η ισχύς ενδέχεται να είναι περιορισμένη.

Στα μειονεκτήματα από την εμπλοκή τους σε συστήματα επικοινωνίας δημόσιας ασφάλειας θα λέγαμε ότι εντάσσονται:

- Απαίτηση οπτικής επαφής (LoS): Οι WOC απαιτούν οπτική επαφή ανάμεσα στους σταθμούς εκπομπής και λήψης , με αποτέλεσμα τον περιορισμό της εμβέλειας και της ευελιξίας του συστήματος. Επίσης εμπόδια όπως κτίρια, δέντρα και ομίχλη μπορεί να μπλοκάρουν την ακτίνα λέιζερ και να προκαλέσουν απώλεια σήματος.
- Καιρικές Συνθήκες: Οι WOC μπορούν να επηρεαστούν από καιρικές συνθήκες όπως ομίχλη, βροχή και χιόνι, οι οποίες μπορεί να προκαλέσουν απώλεια ή εξασθένηση του σήματος

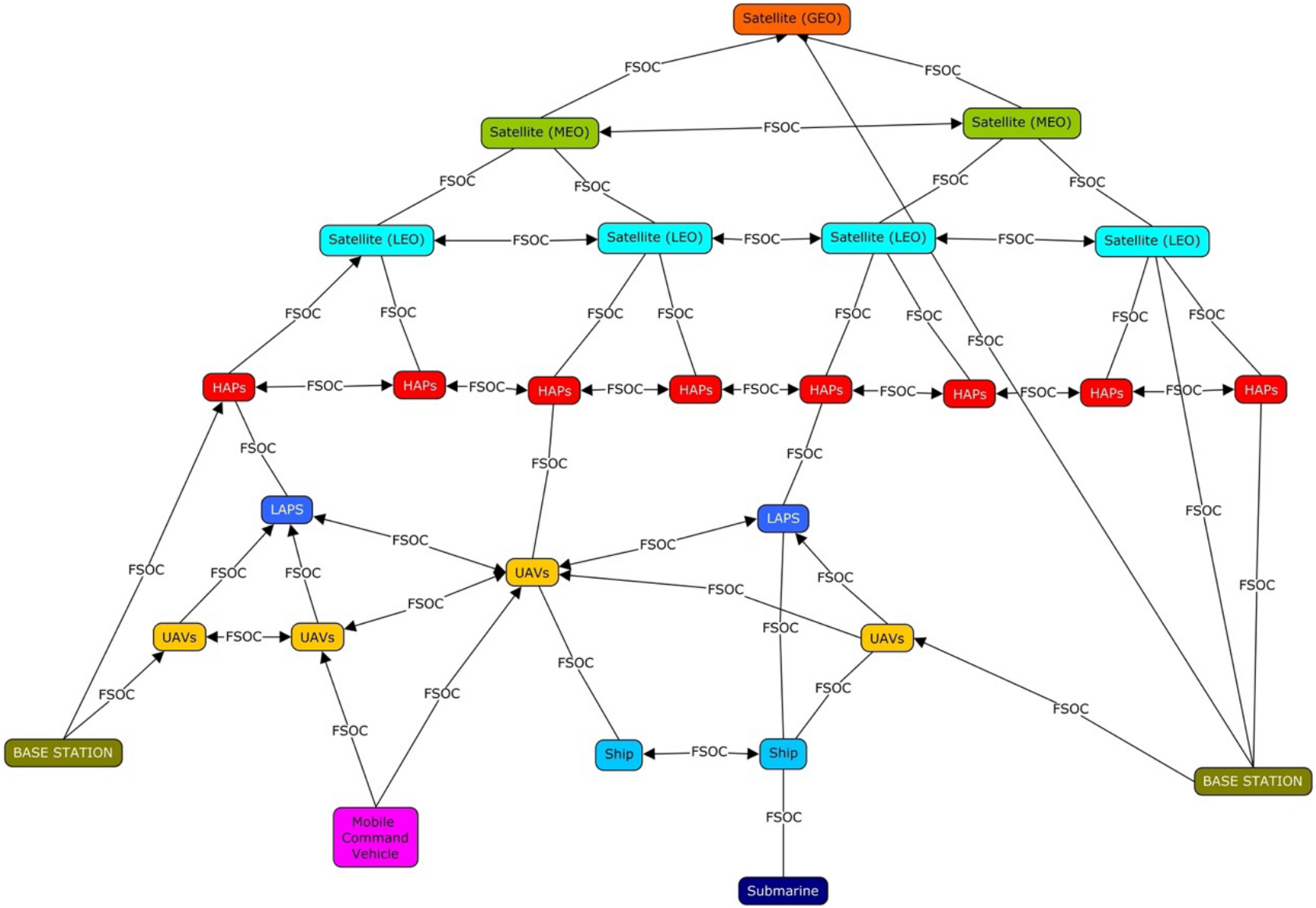
- Μεγαλύτερο Κόστος: Ο εξοπλισμός των συστημάτων WOC μπορεί να είναι πιο ακριβός από τον παραδοσιακό εξοπλισμό ασύρματης επικοινωνίας.
- Ασφάλεια για τους χρήστες: Τα συστήματα WOC χρησιμοποιούν ακτίνες λέιζερ, οι οποίες μπορεί να είναι επικίνδυνες εάν δεν τηρούνται οι οδηγίες προστασίας
- Μειωμένη διείσδυση: Δεν είναι κατάλληλες για χρήσεις σε πυκνό αστικό περιβάλλον ή σε περιοχές με πυκνή βλάστηση για D2D επικοινωνίες με δεδομένο ότι δεν υπάρχει δυνατότητα διείσδυσης μέσα από τοίχους ή δένδρα.

Συμπερασματικά, θα μπορούσαμε να αναφέρουμε πως οι ασύρματες οπτικές επικοινωνίες διαθέτουν αρκετά πλεονεκτήματα έναντι των παραδοσιακών ασύρματων επικοινωνιών, όπως ο υψηλός ρυθμός δεδομένων, η μεγαλύτερη ασφάλεια, η ανοσία σε ηλεκτρομαγνητικές παρεμβολές καθώς και η μικρότερη κατανάλωση ενέργειας που απαιτούν. Ωστόσο, υπάρχουν και αρκετοί σημαντικοί περιορισμοί όπως η απαίτηση για οπτική επαφή ανάμεσα στους σταθμούς, η ευαισθησία σε καιρικά φαινόμενα, το κόστος αλλά και η ασφάλεια για τους χρήστες.

Με αυτά τα δεδομένα οι WOC θα μπορούσαν χρησιμοποιηθούν σε σενάρια και στις πέντε περιοχές ενδιαφέροντος (διάστημα, εναέρια, επίγεια, θαλάσσια και υποθαλάσσια). Τα σενάρια αυτά είναι (Εικόνα 69):

Ως σταθμός βάσης οπισθοζεύξης με στόχο την επικοινωνία ανάμεσα στους κόμβους [200]. Για παράδειγμα:

- Δορυφόρου (GEO, MEO, LEO) με δορυφόρο
- Δορυφόρου με Πλατφόρμες μεγάλου υψομέτρου (High Altitude Platforms -HAPs)
- Δορυφόρου με Πλατφόρμες μικρού υψομέτρου (Low Altitude Platforms -LAPs)
- Δορυφόρου με Επίγειο Σταθμό Βάσης (ΕΣΒ)
- HAP με HAP
- HAP με LAPs η με ΕΣΒ
- LAP με ΕΣΒ
- LAP με μεταφερόμενο ΕΣΒ
- Σημείου προς σημείο [206]



Εικόνα 69. Σενάρια χρήσης FSOC με στοιχεία από [200]

4.13.3 Το μέλλον των οπτικών επικοινωνιών

Σήμερα οι οπτικές επικοινωνίες χρησιμοποιούνται κυρίως σε στρατιωτικές εφαρμογές [200], παρόλα αυτά υπάρχουν εταιρείες όπως η X. Company, Huawei [206] οι οποίες έχουν υλοποιήσει έργα σε επίγειους σταθμούς κυρίως για επικοινωνίες σημείου προς σημείο [198]. Το 2022 Google (Alphabet) ίδρυσε την Aalyria [207] η οποία εξελίσσει σήμερα την τεχνογνωσία που είχε αναπτύξει από το πρόγραμμα Loon το οποίο τερματίστηκε το 2021 και αφορούσε τα συστήματα ασύρματης οπτικής επικοινωνίας ανάμεσα στα αερόστατα που παρείχαν υπηρεσίες κινητής επικοινωνίας σε διάφορες χώρες του κόσμου. Σίγουρα οι ασύρματες οπτικές επικοινωνίες έχουν αρκετό δρόμο ακόμη για να αξιοποιηθούν στον τομέα της δημόσιας ασφάλειας και της αποκατάστασης καταστροφών. Όμως υβριδικά συστήματα WOC σε συνδυασμό με της πέμπτης γενιάς κινητές επικοινωνίες (5G) που σήμερα δοκιμάζονται δίνουν πολλές υποσχέσεις για τη δημιουργία μελλοντικών ασύρματων δικτύων που άμεσα θα μπορούν να προσφέρουν κάλυψη με αξιόπιστες, ασφαλείς, ευρυζωνικές επικοινωνίες σε κάθε πληγείσα περιοχή.

4.14 Φάσμα ραδιοσυχνοτήτων (spectrum)

Το ραδιοφάσμα είναι το μέρος του ηλεκτρομαγνητικού φάσματος με συχνότητες από 3 Hz έως 300 GHz[13]. Τα ηλεκτρομαγνητικά κύματα σε αυτό το φάσμα συχνοτήτων, που ονομάζονται ραδιοκύματα, χρησιμοποιούνται ευρέως στη σύγχρονη τεχνολογία, ιδιαίτερα στις τηλεπικοινωνίες. [208] Η χρήση του ραδιοφάσματος εμπλέκεται σε ένα ευρύ πλέγμα εφαρμογών, ανάμεσα στις οποίες εξέχουσα θέση καταλαμβάνει η δημόσια ασφάλεια (δίκτυα επικοινωνίας για υπηρεσίες έκτακτης ανάγκης).

Το φάσμα ραδιοσυχνοτήτων (spectrum) δεν συγκαταλέγεται στις τεχνολογίες που υλοποιούν δίκτυα δημόσιας ασφάλειας, αλλά αποτελεί ένα από τα κύρια ζητήματα για την υλοποίηση αυτών [51]. Είναι ένας σπάνιος και πολύτιμος φυσικός πόρος, το «χρυσάφι» της επικοινωνίας και απασχολεί θεμελιωδώς κάθε υλοποίηση δικτύου δημόσιας ασφάλειας. Απόδειξη της σπουδαιότητάς του συνιστά το γεγονός ότι το σύνολο σχεδόν των χωρών παγκοσμίως έχουν αναθέσει τη διαχείρισή του σε Κρατικούς Φορείς και Οργανισμούς. Για τη χώρα μας, η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ[14]), ως Εθνική Ρυθμιστική Αρχή (ΕΡΑ) διαχειρίζεται το εμπορικό φάσμα ραδιοσυχνοτήτων με εξαίρεση αυτό της

[13] https://el.wikipedia.org/wiki/%CE%A1%CE%B1%CE%B4%CE%B9%CE%BF%CE%BA%CF%8D%CE%BC%CE%B1%CF%84%CE%B1

[14] https://www.eett.gr/eett/schetika-me-tin-eett/armodiotites/

ραδιοφωνίας και τηλεόρασης, σύμφωνα με όσα ορίζονται στις διατάξεις του Ν. 4070/2012[15] «*Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις*», όπως αυτές τροποποιήθηκαν και συμπληρώθηκαν με το Ν.4727/2020 και Ν.4951/2022. Τόσο η δική μας ΕΡΑ, όσο και των υπολοίπων ευρωπαϊκών χωρών ανήκουν στο Σώμα Ευρωπαίων Ρυθμιστών για τις Ηλεκτρονικές Επικοινωνίες (Body of European Regulators for Electronic Communications - BEREC), που έχει ως βασικό σκοπό τη διασφάλιση της συνεπούς εφαρμογής του ενωσιακού κανονιστικού πλαισίου για τις ηλεκτρονικές επικοινωνίες [209]. Στις βασικές προτεραιότητες του BEREC για το 2023 ανήκουν η προώθηση της πλήρους συνδεσιμότητας για τους καταναλωτές και τις επιχειρήσεις, η ενίσχυση των αειφόρων και ανοικτών ψηφιακών αγορών και η ενδυνάμωση των τελικών χρηστών. Στις επί μέρους δράσεις που στοχεύουν να συμβάλλουν στην εκπλήρωση των στόχων του προγράμματος πολιτικής της ΕΕ «Πορεία προς την Ψηφιακή Δεκαετία» με χρονικό ορίζοντα το 2030, εξετάζονται οι επιπτώσεις της τεχνητής νοημοσύνης στην αγορά τηλεπικοινωνιών και αναλύονται οι τεχνολογικές εξελίξεις (tower/fiber companies, δορυφόροι LEO, IoT, cloud/edge/fog computing κ.λπ.) [209].

Στο άρθρο 8 της υπ` αρίθμ: 243/2012/ΕΕ Απόφασης του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Μαρτίου 2012, σχετικά με την καθιέρωση πολυετούς προγράμματος πολίτικης για το ραδιοφάσμα ορίζεται ότι: «*Η Επιτροπή, σε συνεργασία με τα κράτη μελή, προσπαθεί να διασφαλίσει τη διάθεση επαρκούς φάσματος υπό εναρμονισμένους όρους, ώστε να στηριχτεί η ανάπτυξη υπηρεσιών ασφαλείας και η ελεύθερη κυκλοφορία σχετικών συσκευών, καθώς και η ανάπτυξη καινοτόμων δυσλειτουργικών λύσεων για τη δημόσια ασφάλεια και προστασία, την πολίτικη προστασία και την αρωγή σε περιπτώσεις καταστροφών*» [210].

Ο συντονισμός του φάσματος σε παγκόσμιο επίπεδο αποτελεί αρμοδιότητα της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU). Μάλιστα μια συνοπτική αποτύπωση των περιοχών συχνοτήτων και τις ονομασίες τους σύμφωνα με την ITU προκύπτει στον Πίνακας 16. Σύμφωνα με τα συμπεράσματα της παγκόσμιας διάσκεψης ραδιοεπικοινωνιών της ITU [211], το 2007, η συνολική αξία των εξαρτώμενων από το φάσμα υπηρεσιών στην ΕΕ υπερέβαινε τα 200 δις €, δηλαδή αντιπροσώπευε το 2% - 2,5% του ετήσιου ευρωπαϊκού ακαθάριστου προϊόντος. Η πράξη έχει αποδείξει ότι οι προκλήσεις της αποτελεσματικής διαχείρισης του φάσματος ραδιοσυχνοτήτων αντιμετωπίζονται καλύτερα με τη συνεργασία μεταξύ χωρών. Αξιοσημείωτο είναι ότι στο πλαίσιο της περιόδου που διανύουμε, όπου τα δίκτυα πέμπτης γενιάς (5G) αναπτύσσονται με ταχύτατους ρυθμούς, καταγράφεται μια τάση του τηλεπικοινωνιακού κόσμου να προάγουν την ανάπτυξη τοπικών και ιδιωτικών δικτύων από παρόχους και μη, ανάλογα με τη διαθεσιμότητα του αναγκαίου φάσματος [212]. Στο κλίμα

[15] https://www.kodiko.gr/nomothesia/document/117878/nomos-4070-2012

αυτό, κάθε χώρα ακολουθεί διαφορετικές πρακτικές αναφορικά με την εκχώρηση του φάσματος, επιτρέποντας ή όχι την ανάπτυξη τοπικών δικτύων, παρέχοντας τη δυνατότητα μίσθωσης ζωνών φάσματος από παρόχους, εκχωρώντας φάσμα σε παρόχους μέσω δημοπρασιών, ή ενεργώντας απ` ευθείας αναθέσεις.

Κάθε υλοποίηση που παρουσιάζεται στην παρούσα εργασία πραγματεύεται και το ζήτημα του φάσματος ραδιοσυχνοτήτων στο οποίο λειτουργεί το αντίστοιχο πρότυπο ή τεχνολογία. Χαρακτηριστικό παράδειγμα αναφοράς αποτελούν το 5G και το FirstNet, για τα οποία έγινε εκτενής και αναλυτική αποτύπωση στα κεφάλαια 4.4.2.3 και 5.2.1.3.1, αντίστοιχα. Στο [148] γίνεται μια περιεκτική επισκόπηση της κατανομής των Η.Π.Α. για τις ζώνες των VHF, UHF, 700 MHz, 800 MHz, 900 MHz και 4,9 GHz, το οποίο είναι μια χαρακτηριστική περίπτωση για να γίνει απολύτως αντιληπτός ο τρόπος με τον οποίο γίνεται η διαχείριση του ραδιοφάσματος από τις χώρες. Εν προκειμένω, η FCC έχει λάβει μέτρα για να διασφαλίσει ότι ο αριθμός κλήσης επείγουσας κατάστασης (911) και άλλες κρίσιμες επικοινωνίες παραμένουν λειτουργικές όταν συμβαίνει η καταστροφή. Τα κανάλια δημόσιας ασφάλειας είναι διαθέσιμα στη ζώνη VHF, ζώνη 220 MHz, UHF, T-Band, στενή ζώνη 700 MHz, ευρεία ζώνη 700 MHz, ζώνη 800 MHz, 4,9 GHz και 5,9 GHz, σύμφωνα με τον Πίνακας 13.

Όπως καταγράφεται λεπτομερώς στη συνέχεια στη FirstNet Authority έχει εκχωρηθεί η ευρυζωνική κατανομή φάσματος 758-769/788-799 MHz για τις ανάγκες λειτουργίας του FirstNet. Τα κανάλια στενής ζώνης των 700 MHz και στη ζώνη NPSPAC των 800 MHz εκχωρούνται σύμφωνα με τα σχέδια καναλιών που έχουν αναπτυχθεί από τις 55 Περιφερειακές Επιτροπές Σχεδιασμού (RPC) και έχουν εγκριθεί από την Επιτροπή. Όλα τα κανάλια, εκτός από εκείνα στις μπάντες των 4,9 GHz και 5,9 GHz, υπόκεινται σε συντονισμό συχνοτήτων για να διασφαλιστεί ότι δεν υπάρχουν αμοιβαίες παρεμβολές [213]. Περαιτέρω, η αδειοδοτημένη και μη κατανομή φάσματος στις Η.Π.Α. δείχνεται αναλυτικά στον Πίνακας 15 και Πίνακας 14, αντίστοιχα.

Συχνότητα	**MHz διαθέσιμα για PS**	**Συχνότητα**	**MHz διαθέσιμα για PS**
25-50 MHz (**VHF Low Band**)	6.3 MHz	768-775/798-805 (**700 Narrowband**)	14 MHz (7 MHz x 7 MHz) (συνεχές)
150-174 MHz (**VHF High Band**)	3.6 MHz (όχι συνεχές)	806-809/851-854 MHz (**NPSPAC Band**)	6 MHz (3 MHz x 3 MHz) (συνεχές)
220-222 (**220 MHz band**)	0.1 MHz	809-815/854-860 MHz (**800 MHz Band**)	3.5 MHz (1.75 MHz x 1.75 MHz) (όχι συνεχές)
450-470 (**UHF Band**)	3.7 MHz (όχι συνεχές)	4940-4990 MHz (**4.9 GHz Band**)	50 MHz (συνεχές)
758-769/788-799 MHz (**700 Broadband**)	22 MHz (11 MHz x 11 MHz) (συνεχές)	5850-5925 MHz band (**5.9 GHz Band**)	75 MHz (συνεχές)

Πίνακας 13. Ραδιοφάσμα δημόσιας ασφάλειας στις Η.Π.Α.

Band	Usage	Frequency
ISM band I	Cordless phones, 1G WLANs	902–928 MHz
ISM band II	Bluetooth®, 802.11b, 802.11g WLANs	2.4–2.4835 GHz
ISM band III	Wireless PBX	5.725–5.85 GHz
U-NII1 band I	Indoor systems, 802.11a WLANs	5.15–5.25 GHz
U-NII band II	Short-range outdoor systems, 802.11a WLANs	5.25–5.35 GHz
U-NII band III	Long-range outdoor systems, 802.11a WLANs	5.725–5.825 GHz

Πίνακας 14. Μη αδειοδοτημένη κατανομή φάσματος στις Η.Π.Α.

Service/system	Frequency
AM radio	535–1605 KHz
FM radio	88–108 MHz
Broadcast TV (channels 2–6)	54–88 MHz
Broadcast TV (channels 7–13)	174–216 MHz
Broadcast TV (UHF)	470–806 MHz
Broadband wireless	746–764 MHz, 776–794 MHz
3G wireless	1.7–1.85 GHz, 2.5–2.69 GHz
1G and 2G cellular	806–902 MHz
Personal communications systems	1.85–1.99 GHz
Wireless communications service	2.305–2.32 GHz, 2.345–2.36 GHz
Satellite digital radio	2.32–2.325 GHz
MMDS	2.15–2.68 GHz
Satellite TV	12.2–12.7 GHz
LMDS	27.5–29.5 GHz, 31–31.3 GHz
Fixed wireless services	38.6–40 GHz

Πίνακας 15. Αδειοδοτημένη κατανομή φάσματος στις Η.Π.Α. [214]

Ονομασία		Αρχικά	Συχνότητα		Μήκος κύματος		Εφαρμογές
Εξαιρετικά χαμηλή συχνότητα		ELF Extremely Low	3-30	Hz	10.000-100.000	Km	Αντιληπτό ως ήχος αν μετατραπεί σε μηχανική ταλάντωση
Υπερ-χαμηλή συχνότητα		SLF Super Low	30-300		1.000-10.000		Αντιληπτό ως ήχος αν μετατραπεί σε μηχανική ταλάντωση, ηλεκτρικά δίκτυα διανομής, υποβρύχια
Κατεξοχήν χαμηλή συχνότητα		ULF Ultra Low	300-3000		100-1.000		Αντιληπτό ως ήχος αν μετατραπεί σε μηχανική ταλάντωση, τηλεπικοινωνίες σε ορυχεία
Πολύ χαμηλή συχνότητα (υπερμακρά κύματα)		VLF Very Low	3-30	KHz	10-100		Αντιληπτό ως ήχος αν μετατραπεί σε μηχανική ταλάντωση, υποβρύχια
Χαμηλή συχνότητα (μακρά κύματα)		LF Low	30-300		1-10		Ραδιοφωνικές μεταδόσεις AM, ραδιοφάροι, ερασιτεχνικοί πομποδέκτες
Μέση συχνότητα (μεσαία κύματα)		MF Medium	300-3000		100-1.000	m	Ραδιοσυστήματα πλοήγησης, ραδιοφωνικές μεταδόσεις AM, ναυτιλία, αεροναυτιλία
Υψηλή συχνότητα (βραχέα κύματα)		HF Hight	3-30	MHz	10-100		Βραχέα ραδιοφώνου, ερασιτεχνικές ραδιοεκπομπές, ερασιτεχνικοί πομποδέκτες
Πολύ υψηλή συχνότητα (υπερβραχέα κύματα)		VHF Very Hight	30-300		1-10		Ραδιοφωνικές μεταδόσεις FM, τηλεοπτικές εμπομπές, αεροναυτιλία
Μικροκύματα	Κατεξοχήν υψηλή συχνότητα	UHF Ultra High	300-3000		10-100	cm	Τηλεοπτικές εκπομπές, κινητή τηλεφωνία, ασύρματα τηλέφωνα. Φούρνοι μικροκυμάτων
	Υπερ-υψηλή συχνότητα	SHF Super Hight	3-30	GHz	1-10		Ασύρματα δίκτυα, δορυφορικές συνδέσεις, δορυφορική τηλεόραση
	Εξαιρετικά υψηλή συχνότητα	EHF Extremely Hight	30-300		1-10	mm	Ραδιοτηλεσκόπια, συστήματα ασφαλείας, ανιχνευτές

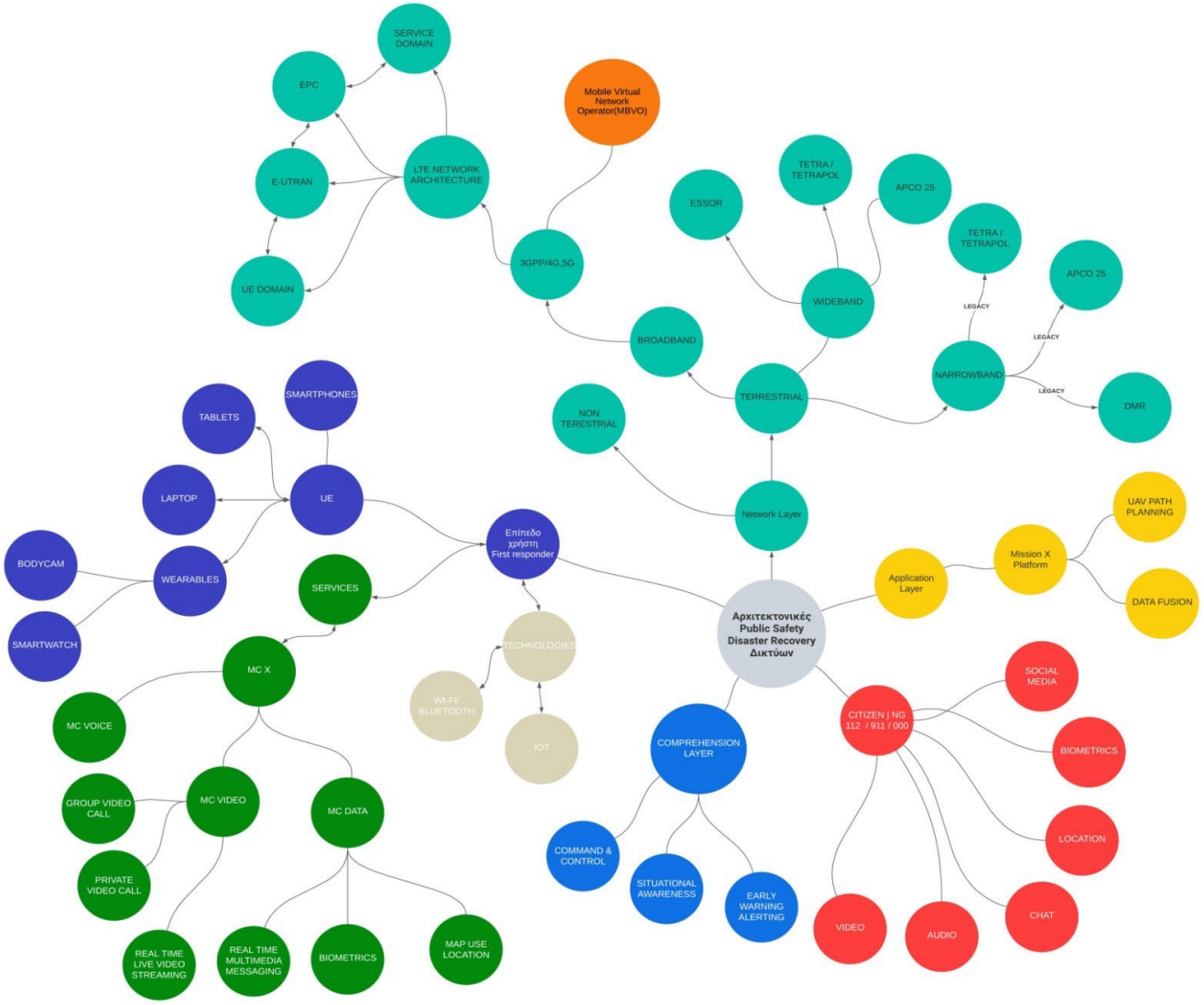
Πίνακας 16. Συχνότητες κατά ITU

5 *Θέματα υλοποίησης*

Αφού έγινε εκτενής αναφορά στις τεχνολογίες που εμπλέκονται στην υλοποίηση έργων για τη δημόσια ασφάλεια, παρατίθενται οι κύριες τεχνολογικές προσεγγίσεις, ως αυτές προέκυψαν από τη βιβλιογραφία, οι οποίες αφορούν σε βασικές τεχνολογικές λύσεις, δομημένες αρχιτεκτονικές δικτύων επικοινωνίας δημόσιας ασφάλειας και ολοκληρωμένες πλατφόρμες κρίσιμων επικοινωνιών που έχουν δοκιμαστεί, ή τελούν υπό δοκιμή.

Βρισκόμαστε σε μία χρονική συγκυρία, όπου παγκοσμίως καταβάλλεται μια οργανωμένη προσπάθεια πλήρους μετάβασης από τα δίκτυα στενής ζώνης στα ευρυζωνικά δίκτυα δημόσιας ασφάλεια, είτε με στενό χρονολογικό ορίζοντα που δεν υπερβαίνει το 2025, είτε με ευρύτερο χρονικό προσανατολισμό που φτάνει στο 2030. Πληθώρα δικτύων δημόσιας ασφάλειας εξελίσσεται παγκοσμίως, ή έχουν ήδη καταστεί λειτουργικά και εξυπηρετούν τις ανάγκες των κρίσιμων επικοινωνιών. Λύσεις αποκλειστικών δικτύων, ή συνεργατικές προσεγγίσεις κυβερνήσεων με εταιρίες, φιλοδοξούν να βελτιώσουν τις παρεχόμενες υπηρεσίες στον τομέα των επικοινωνιών της δημόσιας ασφάλειας και να αποτελέσουν ένα πολύτιμο εργαλείο στα «χέρια» των πρώτων ανταποκριτών.

Από τη μελέτη των αρχιτεκτονικών αυτών προέκυψαν κάποια ξεκάθαρα ιδιαίτερα χαρακτηριστικά τους, σε όλες τις φάσεις υλοποίησης. Για την καλύτερη περιγραφή των δομικών τους στοιχείων, επιχειρήθηκε η κατηγοριοποίηση των φάσεων που συγκεντρώνουν κοινά χαρακτηριστικά στο σύνολο σχεδόν των αρχιτεκτονικών των έργων που μελετήθηκαν. Έτσι, οδηγηθήκαμε σε πέντε διακριτά επίπεδα, τα οποία αλληλεπιδρούν μεταξύ τους και συνθέτουν τη λειτουργική και αποδοτική εικόνα των αρχιτεκτονικών δικτύων δημόσιας ασφάλειας: (α)Επίπεδο Αντίληψης, (β)Επίπεδο Δικτύου, (γ)Επίπεδο Επεξεργασίας Δεδομένων, (δ)Επίπεδο Χρήστη και (ε)Επίπεδο Εφαρμογών. Η κατηγοριοποίηση αυτή χαρτογραφήθηκε εννοιολογικά και παρουσιάζεται στην Εικόνα 70. Εκτός βέβαια από τα επίπεδα αρχιτεκτονικής, είναι σημαντικό να αναφερθούμε ξεχωριστά στο κρίσιμο ζήτημα της ασφάλειας των δικτύων επικοινωνιών δημόσιας ασφάλειας.



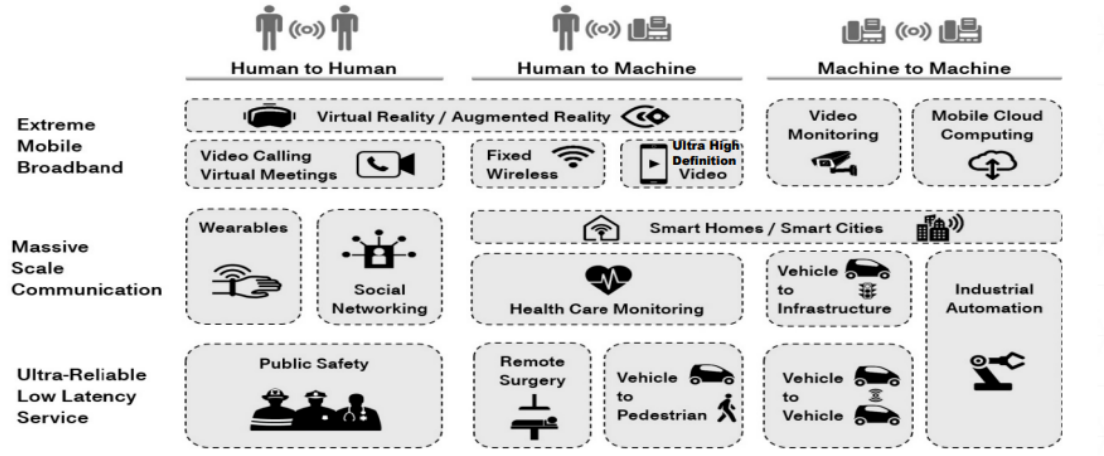
Εικόνα 70. Εννοιολογικός χάρτης των πέντε (5) επιπέδων των αρχιτεκτονικών των Δικτύων Δημόσιας Ασφάλειας και των στοιχείων που τα συνθέτουν

5.1 Επίπεδο Αντίληψης

Αποτελεί το πρώτο επίπεδο και περιγράφει – προσδιορίζει τις πηγές δεδομένων παρακολούθησης, συλλέγοντας τις πληροφορίες που φτάνουν σε πραγματικό χρόνο από κάθε είδους αισθητήρες (π.χ. ασφαλείας, βιομετρικούς, περιβαλλοντικούς εντοπισμού θέσης, κ.λπ.) ή με κάθε δυνατό τρόπο (π.χ., βίντεο, κείμενο, chat, ήχο, κ.λπ.). Ξεχωριστή θέση στο επίπεδο αντίληψης κατέχουν η ενιαία γραμμή κλήσης κινδύνου (διαφέρει από χώρα σε χώρα: 911, 112, 000, κ.λπ.) και τα μέσα κοινωνικής δικτύωσης, καθώς έχουν ως βασικό συστατικό τη συμμετοχή των πολιτών στη δημόσια ασφάλεια. Αυτή είναι και η διάκριση σε υποενότητες στο συγκεκριμένο επίπεδο, δηλαδή τα δεδομένα από αισθητήρες και τα δεδομένα από τη συμμετοχή των πολιτών.

5.1.1 Δεδομένα από αισθητήρες

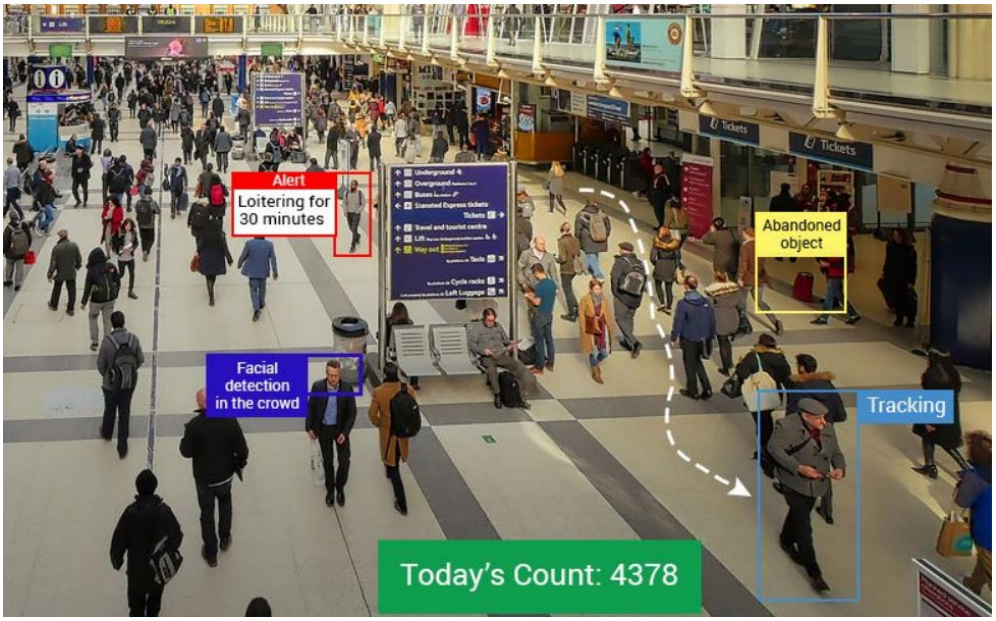
Με την άμεση και ουσιαστική εμπλοκή του IoT στην υλοποίηση των PSNs, η οποία περιγράφηκε διεξοδικά στο κεφάλαιο 4.10, την ταχεία ανάπτυξη της υπολογιστικής στα άκρα και την μετάβαση στην ευρυζωνική επικοινωνία, αλλά και την επικείμενη ολοκληρωτική συμμετοχή των δικτύων 5G στις υλοποιήσεις και εφαρμογές, γίνεται αντιληπτό ότι και στο επίπεδο αντίληψης έχουν γίνει θεαματικά βήματα. Στην Εικόνα 71 προκύπτει μια διδιάστατη κατηγοριοποίηση των τεχνολογιών και αισθητήρων που έχουν επωμιστεί να «αντιληφθούν» την πληροφορία και να τη μεταφέρουν στο επίπεδο δικτύου. Συσκευές εξαιρετικά χαμηλής καθυστέρησης, επικοινωνίας σε μαζική κλίμακα ή ακραίας κινητικότητας ευρυζωνικής τεχνολογία βοηθούν στην επικοινωνία μεταξύ χρηστών (human to human), χρηστών με την υποδομή (human to machine) και παρέχουν αυτοματισμούς μεταξύ των στοιχείων της υποδομής (machine to machine).



Εικόνα 71. Εφαρμογές επιπέδου αντίληψης [215]

Μια πλειάδα από διαφορετικού τύπου συσκευές έχουν αναπτυχθεί με σκοπό να συλλέξουν την πληροφορία από το πεδίο γρήγορα, αποδοτικά και με ασφάλεια και οι οποίες συνιστούν τα εργαλεία των πρώτων ανταποκριτών, αλλά και του συνόλου των επαγγελματιών της δημόσιας ασφάλειας. Στο επίπεδο αυτό, το οποίο ταυτίζεται με το αντίστοιχο της αρχιτεκτονικής του IoT [216] εντάσσονται τα αντικείμενα, δηλαδή παντός είδους αισθητήρες, φορετές συσκευές ή ανιχνευτές που είναι εγκατεστημένες είτε σε σταθερές υποδομές, είτε σε κινητά μέσα (χρήστες, οχήματα, UAVs, κ.λπ.). Η αναγνώριση προσώπου, η ανίχνευση και καταμέτρηση αντικειμένων, η αναγνώριση εικόνας, η ανίχνευση κίνησης, εισβολής, πολύωρης περιπλάνησης που μπορεί να καθίσταται ύποπτη, η αναγνώριση συναισθημάτων, ηλικίας, φύλου είναι στοιχεία που θα πρέπει να γίνονται αυτοματοποιημένα, στο πλαίσιο της τεχνολογικής υποστήριξης που παρέχεται στο προσωπικό της δημόσιας ασφάλειας. Περαιτέρω δε, η εικονική και επαυξημένη πραγματικότητα εμπλέκονται ενεργά στη βελτίωση των ενεργειών που εντάσσονται στο επίπεδο αντίληψης.

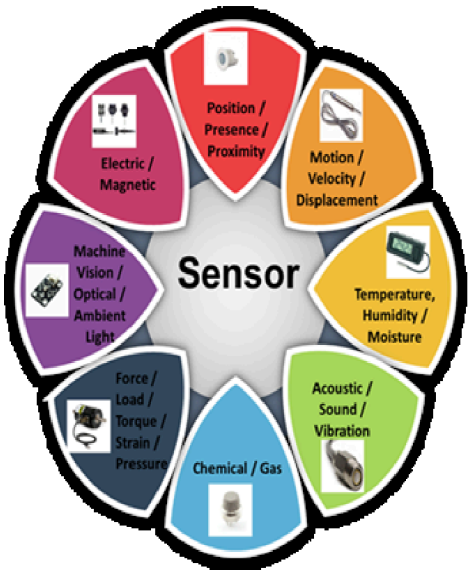
Χαρακτηριστικό στιγμιότυπο ανάλυσης βίντεο επιτήρησης περιοχής φαίνεται στην Εικόνα 72, όπου σε πραγματικό χρόνο γίνεται επεξεργασία των δεδομένων αποστολής της κάμερα ασφαλείας και ταυτόχρονα επιτυγχάνεται αναγνώριση προσώπου, εγκαταλελειμμένου αντικειμένου, διαδρομής που ακολούθησε συγκεκριμένο άτομο και περιπλανώμενο άτομο για 30 λεπτά. Τα οφέλη για τη δημόσια ασφάλεια είναι πολλαπλά, αν αναλογιστούμε τους ανθρώπινους πόρους που θα απαιτούσε η συγκεκριμένη εργασία και την επισφάλεια του αποτελέσματος που συναρτάται με το επίπεδο προσφερόμενων υπηρεσιών του εκάστοτε επαγγελματία. Ο εισηγμένος αυτοματισμός και η τεχνολογική βοήθεια είναι προς τη σωστή κατεύθυνση, όμως θα πρέπει να γίνεται με διαδικασίες απολύτως πιστοποιημένες και ασφαλείς.



Εικόνα 72. Ανάλυση βίντεο κάμερας ασφαλείας σε πραγματικό χρόνο [217]

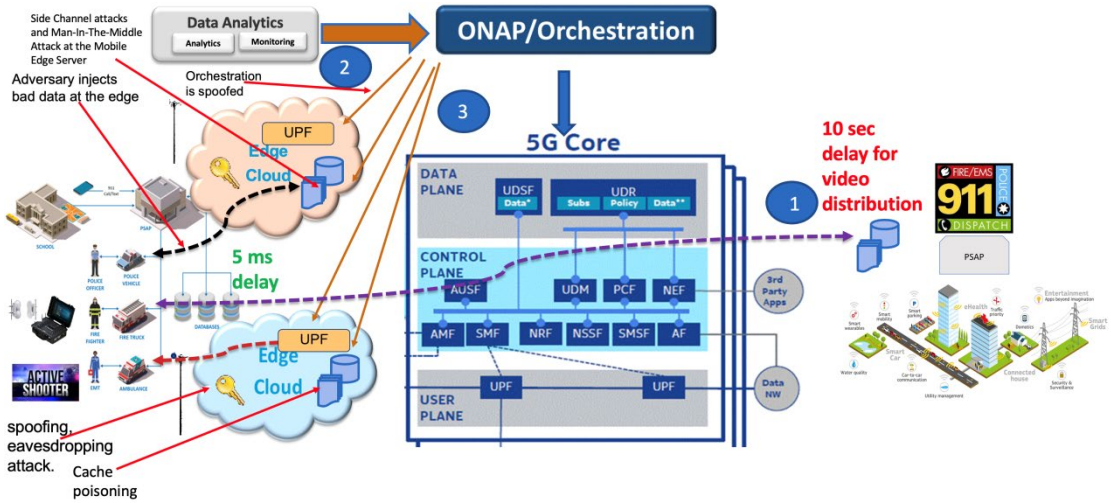
Η έννοια του αισθητήρα είναι ευρέως γνωστή. Ωστόσο, είναι σημαντικό ν` αναφερθούμε επιγραμματικά στα διάφορα είδη αυτών, καθώς είναι γεγονός ότι ο πλουραλισμός των αντικειμένων που καλύπτουν τις περισσότερες φορές μας εκπλήσσει. Ασχέτως της ταξινόμησης με την οποία τους προσεγγίζουμε οι αισθητήρες θερμοκρασίας, εγγύτητας, επιταχυνσιόμετρα, γυροσκόπια, υπερύθρων, υπερήχων, πίεσης, φωτός, καπνού, αερίων, αλκοόλ, αφής, χρώματος, υγρασίας, θέσης, μαγνητικοί, ήχου, κλίσης, ροής και στάθμης, καταπόνησης και βάρους είναι μόνο κάποιοι από τους υπάρχοντες, που «ντύνουν» διάφορες συσκευές της δημόσιας ασφάλειας [218]. Μια βασική κατηγοριοποίηση των αισθητήρων είναι ο διαχωρισμός τους σε ψηφιακούς και αναλογικούς. Είναι προφανές ότι στην περίπτωση των PSNs που μελετάμε αναφερόμαστε κύρια σε ψηφιακούς αισθητήρες. Στο [219], από όπου και η Εικόνα 74 γίνεται μια αξιόλογη αναφορά στα διάφορα είδη αισθητήρων.

Εικόνα 73. Διαφορετικοί τύποι αισθητήρων [218]



Εικόνα 74. Διαφορετικές κατηγορίες αισθητήρων [219]

Όμως, το επίπεδο αντίληψης δεν εξαντλείται με τη συλλογή των δεδομένων, αλλά αφορά και στην πρωτογενή επεξεργασία αυτών για την εξαγωγή αποτελεσμάτων, με σκοπό να τροφοδοτήσει ανάλογα τα υπόλοιπα επίπεδα της εφαρμογής. Αυτό έγινε ήδη πλήρως κατανοητό από την τεχνολογία της υπολογιστικής αιχμής (edge/fog computing) στην οποία αναφερθήκαμε διεξοδικά στο κεφάλαιο 4.11. Προκύπτει βέβαια εμφατικά από διάφορες περιπτώσεις χρήσης. Ένα τέτοιο χαρακτηριστικό παράδειγμα είναι η περίπτωση μαζικών πυροβολισμών σε σχολείο που παρουσιάζεται αναλύεται στο [220] και παρουσιάζεται στην Εικόνα 75, όπου η συλλογή της πληροφορίας σε όλα τα στάδια γίνεται στα δύο άκρα του σχήματος και συγκεκριμένα αριστερά: με τη συμμετοχή των πρώτων ανταποκριτών και δεξιά, από τις κλήσεις των πολιτών στο 911. Η επεξεργασία αυτών, εν προκειμένω σε ένα δίκτυο 5G, γίνεται στο άκρο, με την υποστήριξη του υπολογισμού άκρων πολλαπλής πρόσβασης (MEC) που παρέχει τα οφέλη χαμηλής καθυστέρησης.



Εικόνα 75. Περίπτωση μαζικών πυροβολισμών σε σχολείο - 5G MEC Network [220]

5.1.2 Δεδομένα από συμμετοχή πολιτών

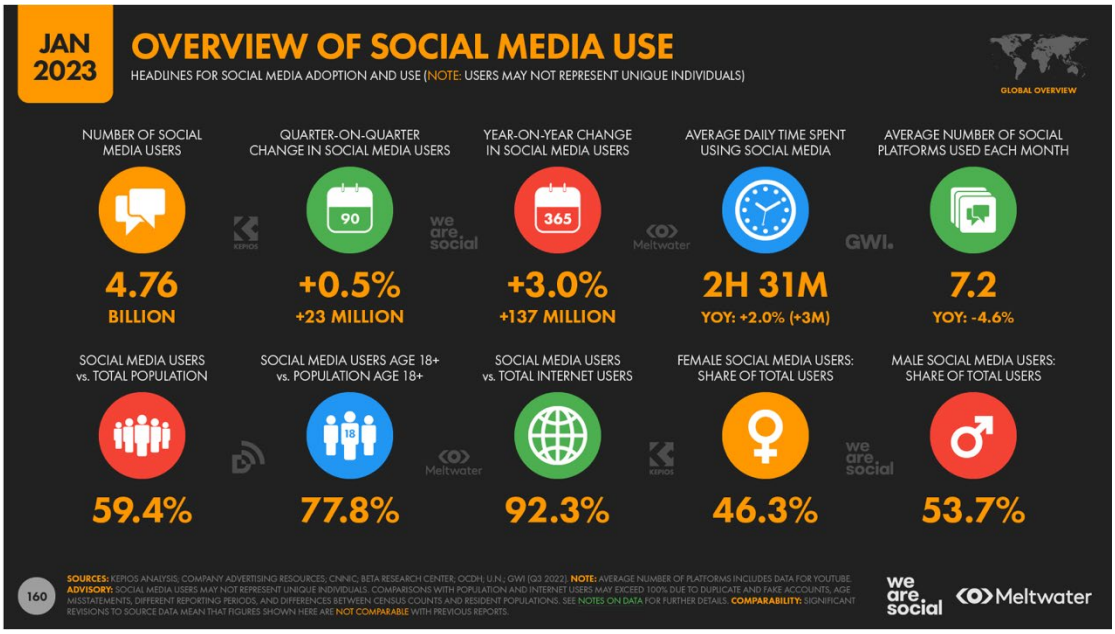
Η ενεργή συμμετοχή των πολιτών στη δημόσια ασφάλεια είναι επιθυμητή, αλλά για να είναι ωφέλιμη θα πρέπει να συντονιστεί, μεθοδευτεί και αξιολογηθεί από τους επαγγελματίες του τομέα. Από τη πολύτιμη έγκυρη πληροφορία που θα δώσει ένας αυτόπτης μάρτυρας ενός βίαιου περιστατικού, που θα οδηγήσει στη σύλληψη των δραστών, ή ενδεχομένως την έγκαιρη επέμβαση των δυνάμεων ασφαλείας και αποτροπή του επικείμενου παράνομου συμβάντος, έως τη σωρεία ψευδών πληροφοριών που συλλέγονται σε περιπτώσεις που οι αρχές παρακινούν τους πολίτες να συνεισφέρουν, όλα χρήζουν προσεκτικής αξιολόγησης.

5.1.2.1 Μέσα κοινωνικής δικτύωσης

Η επικοινωνία είναι το κλειδί για την επιβίωση σε κάθε σενάριο καταστροφής και τα μέσα κοινωνικής δικτύωσης γίνονται ολοένα και περισσότερο ένας βασικός τρόπος επικοινωνίας

[221]. Τα μεγέθη που αφορούν στα μέσα κοινωνικής δικτύωσης είναι συγκλονιστικά (Εικόνα 76) [222] [223], καθώς:

- έχουν περισσότερους από 4,76 δισεκατομμύρια χρήστες παγκοσμίως,
- το 59,3% του παγκόσμιου πληθυσμού χρησιμοποιεί τουλάχιστον μια πλατφόρμα,
- 190 εκατομμύρια νέοι χρήστες τον τελευταίο χρόνο (2022),
- ο μέσος άνθρωπος ξοδεύει 2 ώρες και 31 λεπτά στην καθημερινότητά του στα μέσα κοινωνικής δικτύωσης,
- 92,3% των ανθρώπων που χρησιμοποιούν το διαδίκτυο χρησιμοποιούν και τα μέσα κοινωνικής δικτύωσης,
- ο ετήσιος ρυθμός νέων χρηστών κατ` έτος είναι 3%, που μεταφράζεται σε 137 εκατομμύρια νέους χρήστες

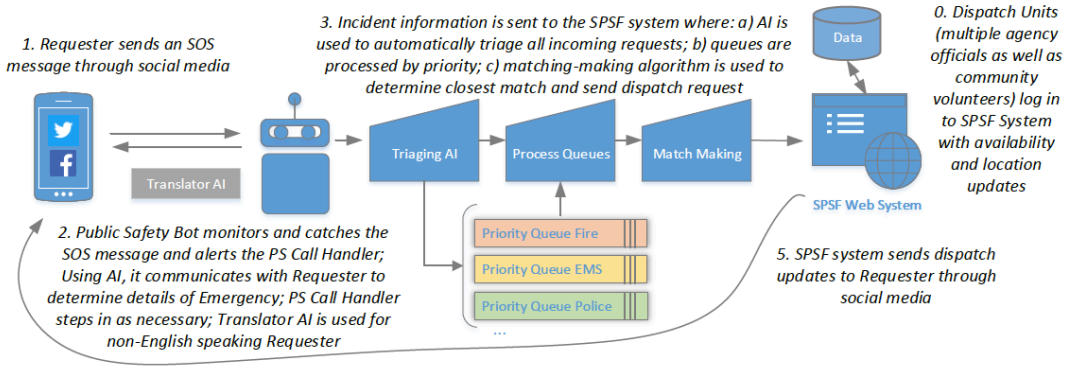


Εικόνα 76. Στατιστικά στοιχεία χρηστών των μέσων κοινωνικής δικτύωσης έως Ιανουάριο 2023 [222]

Η σημασία και η αποτελεσματικότητα των προσπαθειών διάσωσης που βασίζονται στην κοινότητα έχουν προκύψει από συγκεκριμένα περιστατικά. Παράλληλα, η αδυναμία επικοινωνίας μέσω των δικτύων κινητής τηλεφωνίας σε συγκεκριμένες περιπτώσεις καταστροφών έχουν αναδείξει την ανάγκη να υπάρχουν εναλλακτικές οδοί, που θα λειτουργούν συμπληρωματικά στον ενιαίο αριθμό κλήσης έκτακτης ανάγκης. Χαρακτηριστικό παράδειγμα αποτελούν οι περιπτώσεις που κατά τη διάρκεια των τυφώνων Χάρβεϊ και Ίρμα στις Η.Π.Α., οι εγκλωβισμένοι μοιράστηκαν τις τοποθεσίες τους με επαγγελματίες έκτακτης ανάγκης μέσω δημοφιλών πλατφορμών κοινωνικής δικτύωσης όπως το Twitter, το Facebook και το Instagram και απέστειλαν φωτογραφίες για να βοηθήσουν τους πρώτους ανταποκριτές να εκτιμήσουν τη σοβαρότητα της κατάστασης [224]. Οι συγγραφείς στο [221] προτείνουν μια έξυπνη αρχιτεκτονική πλαισίου δημόσιας ασφάλειας

(Smart Public Safety Framework - SPSF) που υλοποιεί αποτελεσματική επικοινωνία θυμάτων και επαγγελματιών χρησιμοποιώντας τα μέσα κοινωνικής δικτύωσης (Εικόνα 77). Μάλιστα, για την παρακολούθηση, ανάλυση και διαλογή αιτημάτων χρησιμοποιείται η τεχνητή νοημοσύνη, ενώ η πλατφόρμα παρέχει στους χρήστες τη δυνατότητα εκπομπής σήματος κινδύνου (SOS) και τα μηνύματα επεξεργάζονται από έναν πράκτορα (agent - bot) της πλατφόρμας, χωρίς ωστόσο από τις δοκιμές να μπορεί ν` αποδειχθεί με ασφάλεια εάν αυτή η πρόταση είναι ικανή να αντικαταστήσει επιτυχώς τους επαγγελματίες της δημόσιας ασφάλειας [221]. Άλλο χαρακτηριστικό παράδειγμα που αναδεικνύει την τάση να χρησιμοποιηθούν αποδοτικά τα μέσα κοινωνικής δικτύωσης στη δημόσια ασφάλεια είναι αυτό που παρουσιάζεται στο [225] και αφορά στην πρωτοβουλία της Αστυνομίας του Βερολίνου να παρακινήσει τους πολίτες να χρησιμοποιήσουν το Twitter δημοσιεύοντας περιστατικά δημόσιας ασφάλειας στα οποία είναι μάρτυρες. Επιπλέον, η Αστυνομία χρησιμοποιώντας το Twitter ενημερώνει τους πολίτες για διάφορα ζητήματα δημόσιας ασφάλειας και μέσα από στοχευμένες ενημερωτικές καμπάνιες προβάλλει το έργο της και τις δράσεις της.

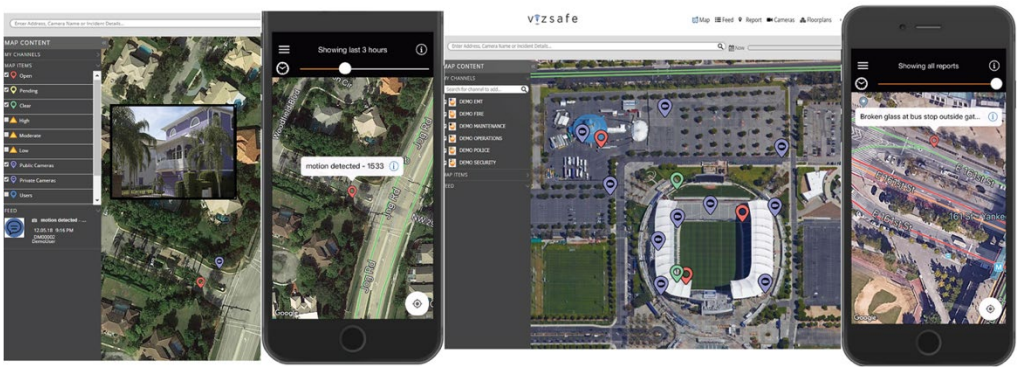
Άλλωστε στην ίδια λογική κινούνται πλέον, εδώ και αρκετά χρόνια και οι υπηρεσίες της δημόσιας ασφάλειας της χώρας μας, καθώς συμμετέχουν ενεργά στις διάφορες πλατφόρμες κοινωνικής δικτύωσης, οι οποίες αποτελούν ανοιχτές πηγές πληροφόρησης, αλλά και φιλόξενους φορείς προβολής του έργου και των δράσεων τους.



Εικόνα 77. Έξυπνο πλαίσιο δημόσιας ασφάλεια SPSF [221].

Με στόχο να καλύψει το χάσμα επικοινωνίας μεταξύ των επίσημων αρχών και των εθελοντών πολιτών που προστρέχουν σε βοήθεια ή παρέχουν οργανωμένη εθελοντική υποστήριξη (ομάδες διασωστών), η Ευρωπαϊκή Ένωση δημιούργησε το τριετούς διάρκειας πρόγραμμα ENGAGE (2020 - 2023), το οποίο υιοθέτησε συγκεκριμένες λύσεις για τη βελτίωση της αλληλεπίδρασης μεταξύ των πρώτων ανταποκριτών, των αρχών και της κοινωνίας των πολιτών [226]. Στις λύσεις αυτές ξεχωριστή θέση καταλαμβάνει η διερεύνηση της χρήσης τεχνολογιών επικοινωνίας και μέσων κοινωνικής δικτύωσης, η οποία αναλύεται διεξοδικά στην έκθεση [227].

Όσον αφορά τη δημόσια ασφάλεια, είναι επιβεβαιωμένο ότι η αλληλεπίδραση με τους πολίτες και η ενθάρρυνσή τους να αναφέρουν προβλήματα ασφάλειας έχει ιδιαίτερη αξία στην καλύτερη λειτουργία των έξυπνων πόλεων. Στη βάση αυτής της παραδοχής, μια ενδιαφέρουσα και καινοτόμος ιδέα υλοποιείται από την εταιρεία Vizsafe[16], η οποία με σκοπό να βελτιώσει την ασφάλεια δημιούργησε μια πλατφόρμα που στοχεύει να δώσει κίνητρα στους πολίτες και συνδέει τη δύναμη του πληθοπορισμού (crowdsourcing[17]) και των τεχνολογιών smartphone με ένα σύστημα επιβράβευσης που βασίζεται σε blockchain [228]. Οι δυνατότητες που παρέχονται μέσα από την πλατφόρμα αποτυπώθηκαν στην Εικόνα 79 ενώ χαρακτηριστικά στιγμιότυπα της συγκεκριμένης πλατφόρμας στην Εικόνα 78. Στην ίδια λογική κινούνται και τα συμπεράσματα της έρευνας των [229], που αποδεικνύει τη δυναμική του crowdsourcing με συγκεκριμένα παραδείγματα. Ένα εξ αυτών αφορά στην περίπτωση του φονικού σεισμού που έπληξε την πρωτεύουσα της Αιτής τον Ιανουάριο του 2010 ύψους 7,1 βαθμών της κλίμακας ρίχτερ. Στην προσπάθεια ανεύρεσης θυμάτων, χιλιάδες μηνύματα αποτυπώθηκαν σε έναν χάρτη κρίσης και βοήθησαν τις αρχές να βρουν επιζώντες (Εικόνα 80)

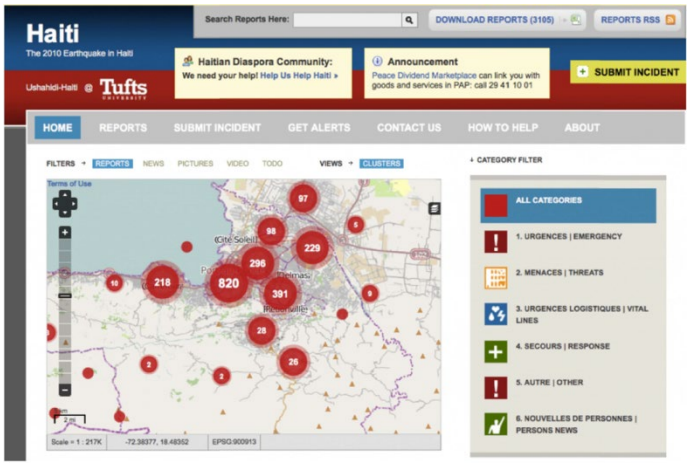


Εικόνα 78. Στιγμιότυπο της πλατφόρμας Vizsafe's Geoaware Network [230]

Εικόνα 79. Διαχείριση περιστατικών και επίγνωση της κατάστασης [230]

[16] https://www.vizsafe.com

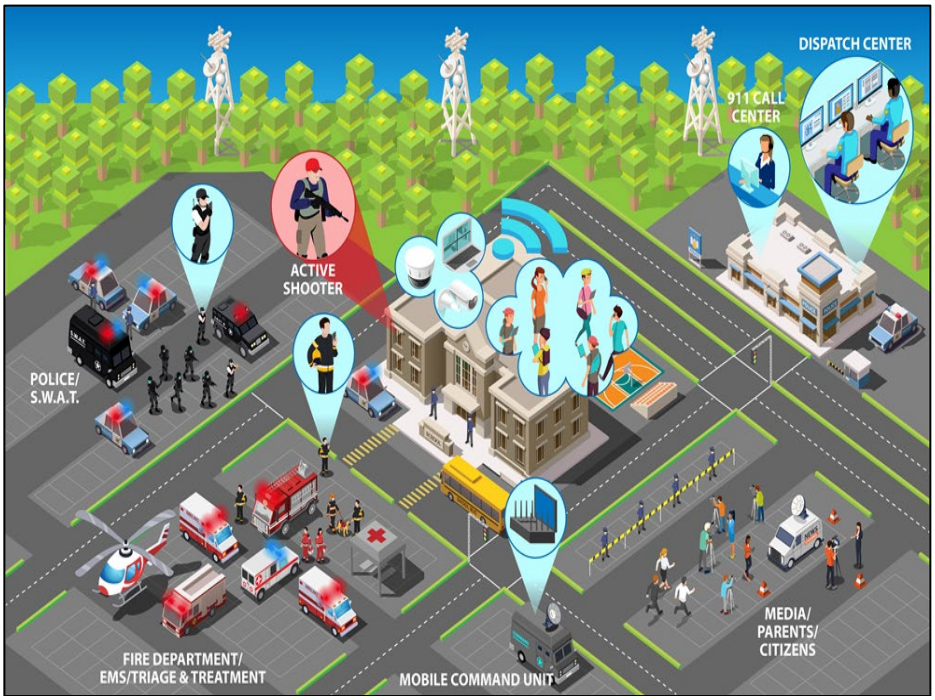
[17] Ο πληθοπορισμός είναι μία μορφή συλλογικής διαδικτυακής δραστηριότητας στην οποία ένα άτομο, ένα ίδρυμα, ένας μη κερδοσκοπικός οργανισμός ή μία εταιρεία προτείνει σε μία ομάδα ατόμων με ποίκιλες γνώσεις, ετερογένεια και αριθμό, μέσω μίας ανοιχτής πρόσκλησης, να αναλάβουν εθελοντικά μια εργασία (https://el.wikipedia.org/wiki/Πληθοπορισμός)



Εικόνα 80. Χάρτης αποτύπωσης αναφορών για ανθρώπους που χρειάζονατι βοήθεια – Σεισμός Αιτή [229]

5.1.2.2 Ενιαίος αριθμός κλήσης έκτακτης ανάγκης

Επανερχόμαστε στην περίπτωση του περιστατικού μαζικών πυροβολισμών σε σχολείο που παρουσιάζεται πλέον σε φυσικό περιβάλλον στην Εικόνα 81 [220]. Η πρώτη πληροφόρηση φτάνει από πολίτη, αυτόπτη μάρτυρα, στο τηλεφωνικό κέντρο έκτακτης βοήθειας και όσο το περιστατικό είναι σε εξέλιξη, ώστε στη συνέχεια να κινητοποιηθεί ο μηχανισμός της δημόσιας ασφάλειας που με κάθε τρόπο θα επιληφθεί σ` αυτό. Ο αριθμός αυτός διαφέρει από χώρα σε χώρα. Ο Ευρωπαϊκός αριθμός κλήσης έκτακτης ανάγκης είναι το «112», ο αντίστοιχος στις Η.Π.Α. είναι ο «911», στην Αυστραλία το «000», κ.ο.κ.. Είναι βέβαιο ότι ασχέτως χώρας, το σύνολο των ζητημάτων που σχετίζονται με την επικοινωνία, τους πρώτους ανταποκριτές και τους επαγγελματίες που στελεχώνουν τα κέντρα πρώτης ανταπόκρισης ομοιάζουν.



Εικόνα 81. Περίπτωση μαζικών πυροβολισμών σε σχολείο [220]

5.1.2.2.1 Ευρωπαϊκός Αριθμός Κλήσης Έκτακτης Ανάγκης «112»

Στο όραμα της EENA εντάσσεται η συμβολή στη βελτίωση της ασφάλειας των ανθρώπων και η προώθηση της χρήσης της Υπηρεσίας Επικοινωνίας Έκτακτης Ανάγκης (Public Safety Answering Point - PSAP «112»). Από το 1991 λειτούργησε ο Ευρωπαϊκός Αριθμός Κλήσης Έκτακτης Ανάγκης «112», σύμφωνα με όσα προβλέπονται από το άρθρο 109 του Ευρωπαϊκού Ηλεκτρονικού Κώδικας Επικοινωνιών (European Electronic Communications Code - EECC). Οι χώρες στις οποίες λειτουργεί δικό τους PSAP έχουν την υποχρέωση να διασφαλίζουν ότι οι κλήσεις στο «112» θα μεταφέρονται αποτελεσματικά και θα διεκπεραιώνονται από την καταλληλότερη υπηρεσία έκτακτης ανάγκης (Εικόνα 82). Εκτός από τη συγκεκριμένη υποχρέωση, τα κράτη μέλη πρέπει να υποβάλλουν ετησίως έκθεση αξιολόγησης, εκ της οποίας στη συνέχεια εκδίδεται η συνολική ετήσια αποτίμηση (για παράδειγμα η αποτίμηση για το 2021 είναι η [231]), να διασφαλίζουν την προσβασιμότητα για άτομα με αναπηρία, να διαθέτουν πληροφορίες για την τοποθεσία του καλούντος και να προωθούν τη χρήση του 112.

Εικόνα 82. Αρμόδιοι φορείς παροχής υπηρεσιών έκτακτης ανάγκης [232]

Για την Ελλάδα, η Γενική Γραμματεία Πολιτικής Προστασίας είναι ο αρμόδιος φορέας για την υλοποίηση και λειτουργία της Υπηρεσίας Επικοινωνιών Έκτακτης Ανάγκης «112» (άρθρο 70 του Ν.4070/2012). Όλες οι κλήσεις προς τον αριθμό «112» (από σταθερό ή κινητό τηλέφωνο) που λαμβάνει το Κέντρο Λήψης Κλήσεων Έκτακτης Ανάγκης «112» με πανελλαδική κάλυψη με ανάδοχο τον ΟΤΕ Α.Ε, το οποίο είναι στελεχωμένο με κατάλληλο προσωπικό (ομιλούν ελληνικά, αγγλικά και γαλλικά) και λειτουργεί σε μόνιμη βάση (24/7/365). Η διεκπεραίωση υλοποιείται με την τηλεπικοινωνιακή σύνδεση των καλούντων

το «112» με τους κατά περίπτωση και κατά τόπους αρμόδιους φορείς παροχής υπηρεσιών έκτακτης ανάγκης, ανάλογα με το περιστατικό που αναφέρει ο καλών και ειδικότερα:

- την Ελληνική Αστυνομία («100»)
- το Πυροσβεστικό Σώμα («199»)
- το Εθνικό Κέντρο Άμεσης Βοήθειας - ΕΚΑΒ («166»)
- το Λιμενικό Σώμα («108»)
- την Εθνική Τηλεφωνική Γραμμή SOS «1056» για την αντιμετώπιση φαινομένων κάθε είδους βίας που αντιμετωπίζουν τα παιδιά
- την Ευρωπαϊκή Γραμμή για Εξαφανισμένα Παιδιά «116000», για την αναφορά περιστατικών παιδιών που έχουν εξαφανιστεί)
- την Ευρωπαϊκή Γραμμή «116111» για τη διαχείριση έκτακτων σοβαρών περιστατικών παιδιών και εφήβων, που αφορούν σε φαινόμενα βίας

Η κλήση στο 112 είναι χωρίς χρέωση και μπορεί να γίνει από σταθερό ή κινητό τηλέφωνο (ακόμα και χωρίς κάρτα SIM) και από δημόσιους τηλεφωνικούς θαλάμους (χωρίς τηλεκάρτα), ακόμα και στην περίπτωση που το δίκτυο του καλούντα δεν έχει κάλυψη ή βρίσκεται εκτός δικτύου (εθνική περιαγωγή). Επιπλέον, υπάρχει η δυνατότητα αποστολής SMS στο 112. Μάλιστα, από 1-1-2020 το σύστημα εκσυγχρονίστηκε και πλέον των άλλων έχει τη δυνατότητα να διαχειρίζεται δεδομένα πολυμέσων, πραγματοποιεί άμεσο και ασφαλή εντοπισμό των καλούντων και γεωγραφική αποτύπωση της θέσης τους, ενώ έχει δυνατότητα συστήματος συναγερμού, για άμεση ενημέρωση κατοίκων μια γεωγραφικής περιοχής και υποστηρίζει την υπηρεσία eCall, σύμφωνα με την οποία από το 2010 όλα τα οχήματα έχουν μια ενσωματωμένη συσκευή στο αμάξωμα όπου σε περίπτωση ατυχήματος καλείται αυτόματα το «112» [233], [234].

Για το έτος 2021, σε πανευρωπαϊκό επίπεδο από την έκθεση [231] προκύπτουν αξιόλογα δεδομένα για τις κλήσεις που δέχεται ο ενιαίος αριθμός «112». Συγκεκριμένα, για το 2021 οι κλήσεις στο «112» αυξήθηκαν κατά 3% και συγκεκριμένα σε 153 εκατομμύρια σε σύγκριση με το 2019. Εν τω μεταξύ, ο συνολικός αριθμός των κλήσεων έκτακτης ανάγκης, συμπεριλαμβανομένων των εθνικών παρέμειναν σταθεροί στα 270 εκατομμύρια, επομένως 56% όλων των κλήσεων έκτακτης ανάγκης για το 2021 έγινε στο «112».

Την παρούσα χρονική στιγμή βρισκόμαστε στην περίοδο μετάβασης στην επόμενη γενιά του ευρωπαϊκού αριθμού έκτακτης ανάγκης (Next generation 112 – NG112), η οποία τίθεται σε λειτουργία τον Μάρτιο του 2023 και λαμβάνει εννιάμηνη προθεσμία καταγραφής προβλημάτων (Δεκέμβριος 2023). Ακολούθως, σε ένα έτος από τη λειτουργία του θα οριστικοποιηθούν και νομοθετικά τα κριτήρια και λεπτομέρειες λειτουργίας του (Μάρτιος 2024). Στο πλαίσιο της συγκεκριμένης μετάβασης υλοποιήθηκε το έργο NG112, το οποίο ολοκληρώθηκε το 2020 και τα αποτελέσματα αυτού αποτέλεσαν τη βάση για την επόμενη

ημέρα. Η αρχιτεκτονική NG112 επιτρέπει τον εκσυγχρονισμό των επικοινωνιών έκτακτης ανάγκης, επιτρέποντας πολύ περισσότερη συλλογή δεδομένων (κείμενο, βίντεο, τοποθεσία ή πρόσθετα δεδομένα), που θα έχει ως αποτέλεσμα μια πιο αποτελεσματική απόκριση. Το NG112 βοηθά επίσης στη διασφάλιση ισοδύναμης πρόσβασης για όλους τους πολίτες, συμπεριλαμβανομένων των ατόμων με αναπηρία. Επιπλέον, τα δίκτυα IP υπηρεσιών έκτακτης ανάγκης (ESInet) θα αναπτυχθούν για να υποστηρίξουν κατάλληλα τα κέντρα έκτακτης ανάγκης, παρέχοντας νέες δυνατότητες και βελτιώνοντας τις υφιστάμενες [235].

Στο πλαίσιο αυτό το ETSI, το χρονικό διάστημα από 2016 έως 2020, σε συνεργασία με την EENA και την αντίστοιχη Αμερικάνικη Ένωση Αριθμού Έκτακτης Ανάγκης (National Emergency Number Association – NENA 911) διοργάνωσε ερευνητικά έργα για την ομαλή μετάβαση σε δίκτυα επικοινωνίας επόμενης γενιάς, στα οποία συμμετείχαν οργανισμοί από Ασία, Ευρώπη και Βόρεια Αμερική. Οι συμμετέχοντες συνδέθηκαν στο εξοπλισμό στο πλαίσιο δοκιμών διαφόρων σεναρίων με στόχο την επικύρωση της διαλειτουργικότητας διαφορετικών λύσεων και την αξιολόγηση του επιπέδου συμμόρφωσης με τις προδιαγραφές αυτών [236] [237] [238].

5.1.2.2.2 Αριθμός Κλήσης Έκτακτης Ανάγκης Η.Π.Α. «911»

Στην ίδια λογική λειτουργίας ο ενιαίος αριθμός κλήσης έκτακτης ανάγκης για τις Η.Π.Α. είναι ο «911» από το 1956. Την προώθηση και εξυγχρονισμό αυτού έχει αναλάβει η NENA και ήδη από το 2000 προτάθηκε η μετάβαση στο NG911, το οποίο υποστηρίζει νέες ασύρματες και βασιμένες σε IP συσκευές επικοινωνίας, που παρέχουν γρήγορους ρυθμούς και επικοινωνία πολυμέσων.

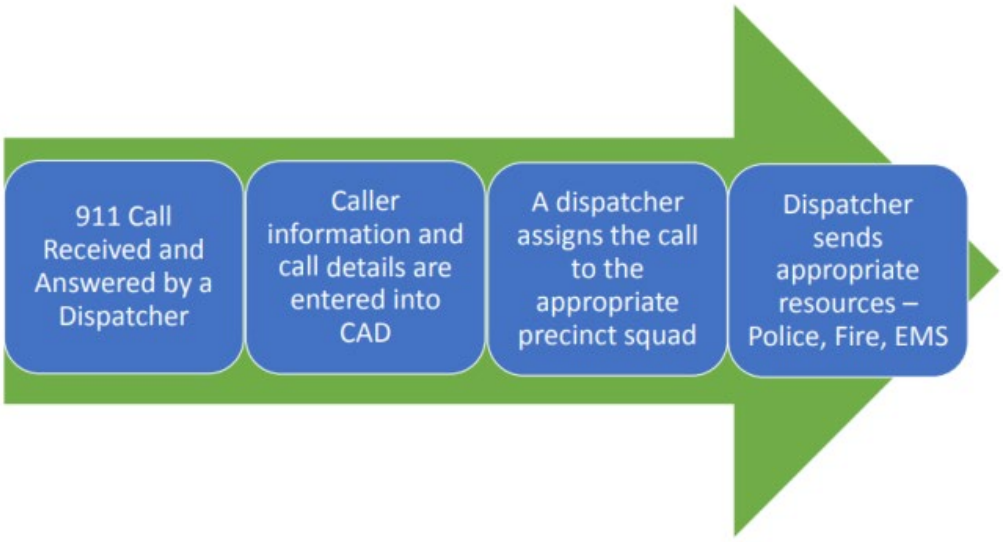
Ο τρόπος λειτουργίας του «911» ομοιάζει με αυτόν του «112», καθώς ο αποστολέας (dispatcher) αναδιανέμει την κλήση στην κατάλληλη υπηρεσία (Εικόνα 83). Σε έρευνα που διεξήχθη από το NIST το 2020 και της οποίας τ` αποτελέσματα καταγράφηκαν στο [239] οι βασικές προκλήσεις για τους επαγγελματίες που στελεχώνουν το 911 είναι η αδιάλειπτη επικοινωνία, αλλά και τα ζητήματα ένταξης στα υπάρχοντα συστήματα των νέων τεχνολογιών. Με βάση αυτά, το προσωπικό επικοινωνίας ανησυχεί ότι οι νέες τεχνολογίες θα απαιτήσουν πρόσθετη εστίαση που θα αυξήσει το γνωστικό τους φορτίο. Επομένως, από το σύνολο σχεδόν των επαγγελματιών υπερτονίσθηκε η ανάγκη οι νέες τεχνολογίες να χαρακτηρίζονται από χρηστικότητα, διαλειτουργικότητα και αξιοπιστία. Αξίζει βέβαια ν` αναφερθεί ότι παρόμοια έρευνα πραγματοποιείται ετησίως, με τη συμμετοχή μεγάλου και αντιπροσωπευτικού αριθμού επαγγελματιών της δημόσιας ασφάλειας και τ` αποτελέσματα τροφοδοτούν και σε κάποιες περιπτώσεις ανακατευθύνουν τη στόχευση των αρχών και τη σχεδίαση λύσεων.

Για να διασφαλίσουν τα PSAP την επιχειρησιακή τους συνέχεια πρέπει να είναι εξοπλισμένα ως ακολούθως [57]:

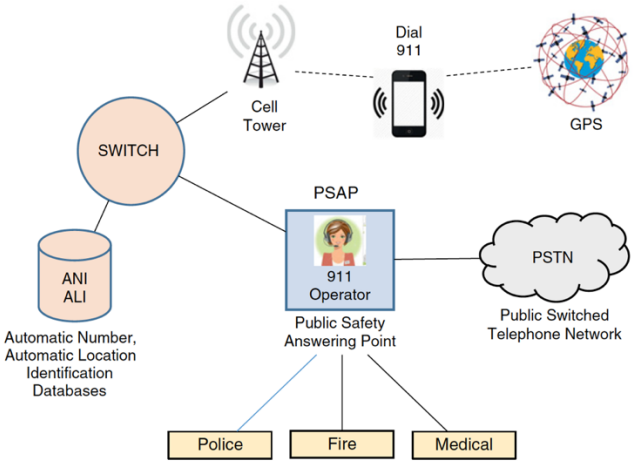
- Υπολογιστικό σύστημα για την ταχεία ενημέρωση των της κατάλληλης κάθε φορά Υπηρεσίας (Αστυνομία, Πυροσβεστική, ΕΚΑΒ, Λιμενικό, κ.λπ.), ανάλογα με το περιστικό αναφοράς.
- Πρόγραμμα χαρτογράφησης, Computer-Aided Dispatch (CAD), για παροχή οδηγιών μαζί με σχετικές πληροφορίες διαδρομής και οδού, καθώς και τυχόν πληροφορίες για τον καλούντα
- Εξοπλισμός εγγραφής και αποθήκευσης για την καταγραφή τηλεφωνικών κλήσεων και όλων των ραδιοεπικοινωνιών μέσα και έξω από το κέντρο
- Εφεδρικές γεννήτριες και αδιάλειπτα τροφοδοτικά (UPS)

Εκτός από τη ροή της κλήσης που προκύπτει από την Εικόνα 83, ο χειρισμός αυτών από το PSAP «911» περιγράφεται στην Εικόνα 84. Κάποια από τα βασικά στοιχεία που προσδιορίζουν τη λειτουργία του είναι:

- Αυτόματη Αναγνώριση Αριθμού (Automatic Number Identification - ANI)
- Αυτόματη Αναγνώριση Τοποθεσίας (Automatic Location Identification - ALI)
- Οδηγός διεύθυνσης (Master Street Address Guide - MSAG) που καθορίζει πληροφορίες σχετικές με την περιοχή του καλούντος
- Πλησιέστερος πύργος κινητής τηλεφωνίας, καθώς η συντριπτική πλειοψηφία των κλήσεων γίνεται από κινητά, στην πρώτη φάση εντοπίζεται ο πύργος που βρίσκεται τουλάχιστον σε απόσταση έως 30 μίλια (περίπου 50 Km), ενώ στη δεύτερη φάση η ακρίβεια φτάνει στα 50-300 m.
- Στον προσδιορισμό της θέσης συμμετέχουν και πληροφορίες από το Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS).
- Τηλέφωνα που λειτουργούν με τεχνολογία Voice over Internet Protocol (VoIP), διαφορετικά από παραδοσιακά ενσύρματα τηλέφωνα, μέσω σύνδεσης διαδικτύου.



Εικόνα 83. Ροή κλήσης στο 911 [240]



Εικόνα 84. Χειρισμός κλήσης από το κέντρο έκτακτης ανάγκης "911" [57]

5.2 Επίπεδο δικτύου

Στο επίπεδο αυτό λαμβάνουν χώρα διεργασίες που αναλαμβάνουν τη μεταφορά και επεξεργασία των δεδομένων που συλλέγονται από το επίπεδο αντίληψης, αλλά και το επίπεδο χρήστη, ώστε να υλοποιηθεί η συνδεσιμότητα των πρώτων ανταποκριτών με τα κέντρα ελέγχου και λήψης αποφάσεων. Για να πραγματοποιηθεί η συγκεκριμένη ενέργεια αποδοτικά είναι απαραίτητο να παρέχονται εξαιρετικά αξιόπιστες υπηρεσίες επικοινωνίας. Πως διασφαλίζεται όμως αυτό; Ποιες υλοποιήσεις δίνουν την καλύτερη απάντηση στο συγκεκριμένο ερώτημα; Οι απαντήσεις εμφανίζουν έναν ιδιαιτέρως ενδιαφέροντα τεχνολογικό πλουραλισμό.

5.2.1 Επίγεια δίκτυα

Λαμβάνοντας υπόψη μας ότι ο αριθμός των συσκευών που είναι συνδεδεμένες στο διαδίκτυο αυξάνεται εκθετικά, με τα πραγματικά αριθμητικά δεδομένα να έχουν ξεπεράσει ήδη κατά πολύ τον πληθυσμό της Γης και ότι οι αντίστοιχες προβλέψεις, είτε βραχυπρόθεσμες (εντός του 2023), είτε μακροπρόθεσμες (ορίζοντας το 2050) δείχνουν να ακολουθούν τους ίδιους γοργούς ρυθμούς, τα επίγεια δίκτυα επικοινωνίας αποτελούν τη βασική τεχνολογική υποδομή που υποστηρίζει τεχνολογικά τη συγκεκριμένη ανάπτυξη. Ενδεικτικά, η CISCO σε σχετική της έκθεση καταγράφει την πρόβλεψη ότι στα τέλη του 2023, σε παγκόσμιο επίπεδο, ο μέσος αριθμός των συσκευών και συνδέσεων ανά άτομο θα φτάσει τις 3,6, ενώ πέντε χρόνια πριν ο αντίστοιχος μέσος όρος ήταν 2,4 [241]. Ενσύρματα ή ασύρματα δίκτυα και υβριδικός συνδυασμός αυτών συνθέτουν ένα πλέγμα επίγειων δικτύων που εξυπηρετεί τις υφιστάμενες επικοινωνιακές ανάγκες. Η στόχευσή μας αφορά στο κομμάτι αυτών που εξυπηρετεί τις κρίσιμες επικοινωνίες και υποστηρίζει το έργο των επαγγελματιών της δημόσιας ασφάλειας.

Για την καλύτερη μελέτη και κατανόηση των αρχιτεκτονικών των δικτύων αυτών, των δυνατοτήτων τους και των τεχνολογικών προοπτικών που δημιουργούν, θα αναλύσουμε τις επικοινωνίες των επίγειων δικτύων δημόσιας ασφάλειας σε σχέση με το εύρος ζώνης (bandwidth) που αξιοποιούν. Διαχωρίσαμε λοιπόν τις επικοινωνίες σε τρεις μεγάλες κατηγορίες: στενής ζώνης (narrowband), ευρείας ζώνης (wideband) και πλήρως ευρυζωνικές (broadband). Είναι αλήθεια ότι η πιο συνηθισμένη διάκριση που συναντούμε στη βιβλιογραφία με βάση το εύρος ζώνης, αναφέρεται στο δίπολο στενής ζώνης και ευρυζωνικές. Επιλέξαμε να διαφοροποιήσουμε αυτή την τάση, ώστε να προκύπτει ξεκάθαρα και σε διακριτά βήματα η σταδιακή μετάβαση από την αναλογική τεχνολογία επικοινωνίας, στην πλήρως ψηφιακή και στην ευρυζωνική, που αναμφίβολα αποτελεί το ενεργό παρόν και το μέλλον των επικοινωνιών αυτών. Χωρίς να υπάρχουν απόλυτα στεγανά, αναφορικά με την κατηγοριοποίηση και αντίστοιχη ένταξη, θα παρουσιάσουμε στη συνέχεια τα πιο αντιπροσωπευτικά έργα που αναπτύχθηκαν και μετουσίωσαν την υπάρχουσα τεχνολογία της κάθε κατηγορίας σε λύσεις επικοινωνίας. Έργα που το καθένα στην εποχή του επιχείρησε να καλύψει τις τρέχουσες απαιτήσεις των δικτύων δημόσιας ασφάλειας, καλύπτει αυτές σήμερα και προβλέπεται να το πράξει και στο μέλλον. Μέσα από το «ταξίδι» αυτό της παρουσίασης των σπουδαιότερων, κατά γενική ομολογία, έργων τα οποία στην πλειοψηφία τους αφορούν πλέον σε τεχνολογικά πρότυπα, θα γνωρίσουμε τις εξελίξεις των υλοποιημένων εφαρμογών στο πεδίο, παράλληλα και σε σχέση με τις αντίστοιχες εξελίξεις των διαθέσιμων τεχνολογικών λύσεων, που αναφέραμε ήδη στο προηγούμενο κεφάλαιο.

Στη βιβλιογραφία, τα συστήματα κρίσιμων επικοινωνιών αναφέρονται συλλογικά υπό τον όρο Επίγεια Κινητά Ραδιοφωνικά Συστήματα (Land Mobile Radio Systems - LMRSs), τεχνολογίες που έχουν χρησιμοποιηθεί εκτενώς για την ανάπτυξη των Ιδιωτικών Κινητών Ραδιοδικτύων (Private Mobile Radio - PMR) [43], τα οποία αποτέλεσαν με τη σειρά τους τα πρώτα PSNs. Τα συστήματα αυτά έχουν εξελιχθεί και παρά το γεγονός ότι βασίστηκαν αρχικά εξ ολοκλήρου στις αναλογικές επικοινωνίες, σταδιακά αντικαταστάθηκαν από πλήρως ψηφιακές τηλεπικοινωνιακές λύσεις που στηρίζονται στη μετάδοση στενής ζώνης, καθώς και στην ευρυζωνικότητα [43], [57].

5.2.1.1 Επικοινωνίες στενής ζώνης (Narrowband)

Εξ ορισμού, αναφερόμαστε σε ασύρματες επικοινωνίες που πραγματοποιούνται με μεταφορά σήματος εντός στενής ζώνης συχνοτήτων. Κάθε ραδιοτεχνολογία καταλαμβάνει ένα συγκεκριμένο τμήμα φάσματος, ώστε αφενός να είναι λειτουργική και αφετέρου να αποφεύγονται οι παρεμβολές. Η εισαγωγή νέων υπηρεσιών και η αύξηση των απαιτήσεων επέφερε περιορισμούς στη διαθεσιμότητα του φάσματος. Στη ραδιοεπικοινωνία, οι επικοινωνίες στενής ζώνης λαμβάνουν χώρα σε περιοχές συχνοτήτων που το κέρδος

παραμένει το ίδιο για όλες τις συχνότητες της περιοχής. Αυτό κατέστησε τις επικοινωνίες στενής ζώνης την καλύτερη επιλογή για οποιαδήποτε εφαρμογή απαιτούσε αξιόπιστες, χαμηλής ισχύος και μεγάλης εμβέλειας επικοινωνίες.

Υπάρχουν τρεις κύριες ψηφιακές τεχνολογίες επικοινωνίας στενής ζώνης που χρησιμοποιούνται σήμερα. Τα πρότυπα Έργο 25 (Project 25 - P25), Επίγειο Ραδιόφωνο Κορμού (Terrestrial Trunked Radio - TETRA) και Ψηφιακό Κινητό Ραδιόφωνο (Digital Mobile Radio - DMR). Κοινό χαρακτηριστικό τους αποτελεί το γεγονός ότι υποστηρίζουν ένα ευρύ φάσμα φωνητικών λειτουργιών και ένα περιορισμένο σύνολο εφαρμογών δεδομένων [57] [44].

5.2.1.1.1 Project 25 (P25)

a. Ιστορικά στοιχεία

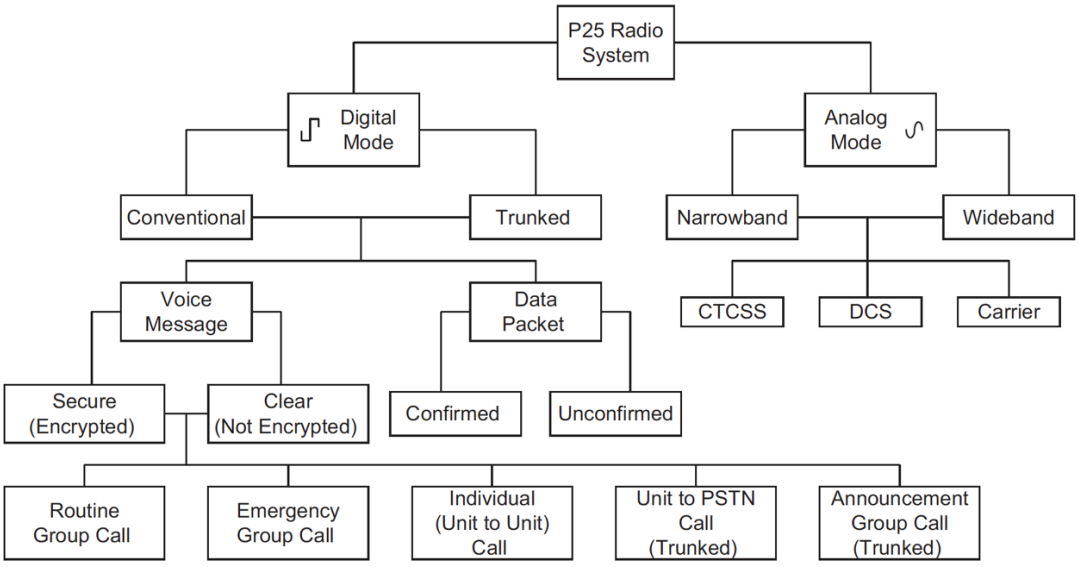
Το πρότυπο επικοινωνίας P25 αναπτύχθηκε από την Ένωση Επικοινωνιών Δημόσιας Ασφάλειας των Η.Π.Α. (Association of Public-Safety Communications Officials - APCO[18]) και έγινε ευρέως γνωστό, ενώ απαντάται και με την ονομασία APCO-25. Το 1988 ξεκίνησε η προσπάθεια ανάπτυξης του P25, στην οποία συμμετείχαν έντεκα ξεχωριστές ενώσεις, φορείς και υπουργεία των Η.Π.Α.. Εκτός από την APCO, σημαντικότερες εξ αυτών ήταν η Ένωση Κρατικών Τηλεπικοινωνιών (National Association of State Technology Directors - NASTD[19]), η Εθνική Διοίκηση Τηλεπικοινωνιών και Πληροφοριών (National Telecommunications and Information Administration - NTIA[20]), η Εθνική Υπηρεσία Ασφαλείας (National Security Agency - NSA [21]), τα Υπουργεία Εσωτερικής Ασφάλειας και Άμυνας (Department of Homeland Security - DHS[22] και Defense Department - USDoD[23]) ο Σύνδεσμος Τηλεπικοινωνιών Βιομηχανίας (Telecommunications Industry Association - TIA[24]) και το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology - NIST[25]). Το αποτέλεσμα αυτής της πολυσυμμετοχικής συνεργασίας ήταν το P25 να γίνει πλέον αποδεκτό ως εθνικό πρότυπο στις Η.Π.Α. για κρίσιμες επικοινωνίες και σκοπούς δημόσιας ασφάλειας. Το P25 όμως ξεπέρασε τα όρια των Η.Π.Α. και πλέον εξυπηρετεί πολλές χώρες ανά τον κόσμο. Αναπτύχθηκε σε τρεις φάσεις, τις 0, 1 και 2. Η Φάση 0 αποτελεί την εναρκτήρια προσέγγιση και αφορά σε απαιτήσεις και πρότυπα που

[18] https://www.apcointl.org
[19] https://www.nastd.org/home
[20] https://ntia.gov
[21] https://www.nsa.gov
[22] https://www.dhs.gov
[23] https://www.defense.gov
[24] https://tiaonline.org
[25] https://www.nist.gov

αναφέρονται στις αναλογικές επικοινωνίες και ουσιαστικά δεν σχετίζεται με το κυρίως έργο, το οποίο αναπτύχθηκε στις Φάσεις 1 και 2.

Τα συστήματα του προτύπου που αναπτύχθηκαν στη Φάση 1 υποστηρίζουν αναλογική, ψηφιακή ή μικτή λειτουργία. Το κύριο χαρακτηριστικό της πρώτης φάσης είναι ότι βασίσθηκε σε FDMA, με χρήση καναλιού 12,5 KHz, χρησιμοποιώντας τη μέθοδο πρόσβασης ενός χρήστη ανά κανάλι. Στο πλαίσιο της Φάσης 2 του έργου χρησιμοποιήθηκε πλέον διαίρεση συχνότητας δύο θυρίδων TDMA, γεγονός που βελτίωσε αισθητά τη χρήση του φάσματος, αν και κατέστησε τον εξοπλισμό μη συμβατό προς τα πίσω με τον αντίστοιχο της Φάσης 1, εκτός εξαιρετικών περιπτώσεων.

Το P25 σήμερα παρέχει την επιλογή στο χρήστη μεταξύ δύο διαφορετικών λειτουργιών, της ψηφιακής και της αναλογικής. Η ψηφιακή με τη σειρά της παρέχει τη δυνατότητα επιλογής συμβατικής (conventional) ή επίγειας (trunked) λειτουργίας, τα κύρια χαρακτηριστικά των οποίων αποτυπώνονται στην Εικόνα 85, ενώ η αναλογική λειτουργία παρέχει τη δυνατότητα επιλογής στενής ή ευρείας ζώνης.



Εικόνα 85. Επιλογή τεχνολογίας λειτουργίας του Project 25 [242]

Μάλιστα, μελετώντας την ψηφιακή λειτουργία, προκύπτει ένας ευρύς κατάλογος χαρακτηριστικών που ικανοποιεί κάθε μία από τις δύο λειτουργίες επιλογής (P25 Conventional / P25 Trunked). Τα χαρακτηριστικά αφορούν στις δυνατότητες φωνητικών κλήσεων που παρέχονται και τα είδη αυτών, στη δυνατότητα ψηφιακής και αναλογικής λειτουργίας, τους τύπους υποστηρικτικών λειτουργιών, τη συνδεσιμότητα με IP, τη δυνατότητα ταυτόχρονων μεταδόσεων, πολλαπλών τοποθεσιών, απομακρυσμένων λειτουργιών, τη δυνατότητα φωνητικών κλήσεων (ομαδικές, ιδιωτικές, επείγουσες, αναγνώριση καλούντος, αναμονής ή απόρριψης κλήσεων, κ.λπ.), ανταλλαγής δεδομένων και διαθέσιμων διεπαφών. Στην πλειοψηφία τους, τα υποστηριζόμενα χαρακτηριστικά δεν

διαφέρουν. Αξίζει όμως να επισημανθεί ότι υφίστανται διαφορές στον τρόπο ενέργειας της συμβατικής λειτουργίας έναντι της επίγειας σχετικά με την εναλλαγή πολλών τοποθεσιών, με τις παρεχόμενες διεπαφές και με την αναμονή κλήσεων, όπως προκύπτει και από τον Πίνακας 17 που ακολουθεί.

Feature	P25 Conventional	P25 Trunked
IP backbone	Available	Available
Analog and digital operation (repeaters/ subscribers)	Yes/yes	No/yes
Simplex/half-duplex/duplex (repeaters)	Yes/yes/yes	Half duplex/duplex
Access Control/subscriber registration	Yes	Yes
Supports analog and digital consoles	Yes	Yes
Dispatch console support	Analog and digital	Analog and digital
End-to-end encryption	Yes	Yes
Distributed, centralized or switched voting	Yes	Yes
Simulcast	Yes	Yes
Multisite(automatic roaming)	Yes	Yes
Self-calibration (simulcast)	Yes	Yes
Rx voting	Yes	Yes
Multi-site switching	Distributed/centralized	Centralized/distributed
Advanced remote monitoring and diagnostics	Yes	Yes
Analog line interface	Yes	Yes
MDC1200 interface support	Yes	Yes
Multiple linking options including RF	Yes	Yes (stricter requirements)
OTAR	Yes	Yes
Packet data support	Yes	Yes
Voice call types	Group, individual, announcement, broadcast, emergency	
Non-voice call types	All standardized P25 supplementary services – status, radio check, monitor, call alert, inhibit/uninhibit, short message	
Talk Group ID	Yes	Yes
Individual ID	Yes	Yes
Emergency ID	Yes	Yes
Emergency Alarm	Yes	Yes
Call addressing	Yes	Yes
Cancel P25 Unit Call (dispatcher interrupt)	Yes	Yes
Automatic working channel assignment (trunking)	No	Yes
Talk group scanning	Yes	Yes
Interfaces	ISSI, PSTN, DFSI	ISSI, PSTN, CSSI
Late entry	Yes (limited)	Yes
Call queuing	No	Yes

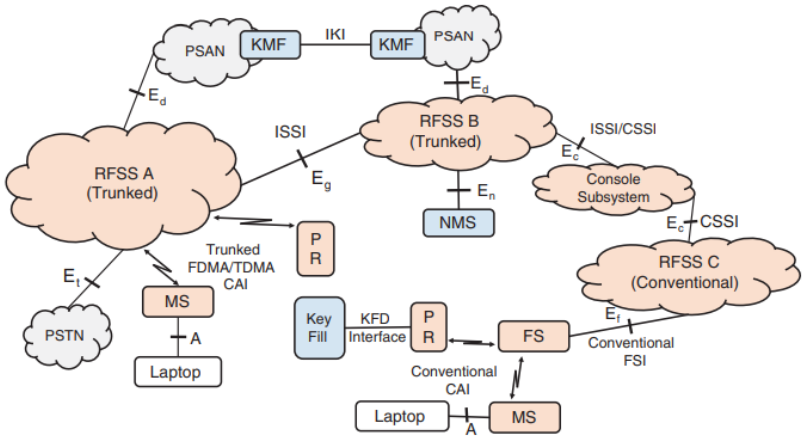
Πίνακας 17. Χαρακτηριστικά που ικανοποιεί η συμβατική και επίγεια λειτουργία του P25 [243]

b. Βασικά στοιχεία αρχιτεκτονικής του P25

Το P25 είναι μια ανοιχτή αρχιτεκτονική, τα βασικά δομικά συστατικά της οποίας φαίνονται στην Εικόνα 86 και η οποία περιλαμβάνει τις ακόλουθες τέσσερις βασικές ομάδες διεπαφών, στις οποίες εντάσσεται το σύνολο των διεπαφών της αρχιτεκτονικής και οι οποίες τυποποιούνται για να συνδέσουν ένα υποσύστημα ραδιοσυχνοτήτων (Radio Frequency Sub System - RFSS), που αποτελεί το κύριο δομικό στοιχείο ενός μεγάλου δικτύου P25, με τα υπόλοιπα στοιχεία:

- Διεπαφή αέρα (Common Air Interface - CAI), καθορίζουν τον τύπο και τον αριθμό των σημάτων που μεταδίδονται μεταξύ των συμβατών χρηστών μέσω ενός καναλιού FDMA ή TDMA, με μέγιστο ρυθμό δεδομένων τα 9,6 Kbps. Η CAI αναλαμβάνει τη σύνδεση μεταξύ χρηστών απ‘ ευθείας, έμμεσα μέσω επαναλήπτη, μέσω σταθερού σταθμού βάσης ή μέσω αναμεταδότη.
- Ενσύρματες διεπαφές**,** στις οποίες εντάσσονται οι: Διασύνδεση υποσυστήματος (Inter Sub-System Interface – ISSI), Κονσόλα διασύνδεσης υποσυστήματος (Console Sub-System Interface – CSSI), Σταθερή διεπαφή σταθμού (Fixed Station Interface – FSI), Διεπαφή Διαχείρισης Δικτύου (Network Management Interface – NMI), Διεπαφή τηλεφωνικής διασύνδεσης (Telephone Interconnect Interface – TII). Οι διεπαφές αυτές παρέχουν τη δυνατότητα σε διαφορετικούς κατασκευαστές να διασυνδέονται απ` ευθείας μέσω ελεγκτή, επιτυγχάνοντας την απρόσκοπτη ενδοεπικοινωνία μεταξύ συστημάτων, την περιαγωγή και τη διαχείριση της κινητικότητας από δίκτυο σε δίκτυο, δηλαδή την πλήρη διαλειτουργικότητα, την υποστήριξη τυπικών πρωτοκόλλων για να συνδεθούν οι κονσόλες αποστολής, τη σύνδεση συμβατικών σταθμών βάσης με επαναλήπτες, την υποστήριξη διαχείρισης δικτύου σε επίπεδο λειτουργίας και συντήρησης, την υποστήριξη αναλογικών και ψηφιακών συνδέσεων και την εν γένει διαχείριση και υποστήριξη φωνητικής επικοινωνίας.
- Διεπαφές δεδομένων**,** στις οποίες εντάσσονται οι: Διεπαφή δικτύου δεδομένων (Data Network Interface – DNI) και η Περιφερειακή διεπαφή δεδομένων κινητής τηλεφωνίας (Mobile Data Peripheral Interface – MDPI). Οι διεπαφές αυτές αναλαμβάνουν την επικοινωνία με κέντρα ή δίκτυα δεδομένων, μέσω συγκεκριμένων πρωτοκόλλων (π.χ. IP), καθώς επίσης και τη διασύνδεση μεταξύ συνδρομητών κινητής τηλεφωνίας.
- Διεπαφές ασφαλείας**,** στις οποίες εντάσσονται οι: Διεπαφή διαχείρισης εσωτερικού κλειδιού (Inter Key Management Interface – IKI) και Διεπαφή διασύνδεση συσκευής πλήρωσης κλειδιού (Key Fill Device Inteface – KDI). Είναι διεπαφές που είναι επιφορτισμένες με την ασφάλεια και την τήρηση των αλγορίθμων κρυπτογράφησης και ανταλλαγής κλειδιών.

Εκτός από τις διεπαφές και το υποσύστημα RFSS που ήδη αναφέρθηκε, η αρχιτεκτονική περιλαμβάνει το υποσύστημα συμβατικής κονσόλας (Conventional Sub-System) και το υποσύστημα επίγεια κονσόλας (Trunked Sub-System). Επιπλέον, περιλαμβάνει σταθερούς συμβατικούς και κεντρικούς σταθμούς βάσης, οι οποίοι παρέχουν έλεγχο και επεξεργασία κλήσεων για την υποστήριξη των επαφών και πρωτοκόλλων που χρησιμοποιούνται στη διασύνδεση των διαφόρων στοιχείων που συμμετέχουν στην αρχιτεκτονική. Επίσης, περιλαμβάνει επαναλήπτες, φορητές και κινητές συσκευές χρηστών, κεντρικούς υπολογιστές διαχείρισης δικτύου και δεδομένων, μεταξύ των οποίων παρέχεται τυποποιημένη συνδεσιμότητα [59].



CAI	Common Air Interface	MDP	Mobile Data Peripheral
CSSI	Console Sub-System Interface (Ec)	MDPI	Mobile Data Peripheral Interface
DNI	Data Network Interface (Ed)	MS	Mobile Station
FDMA	Frequency Division Multiple Access	NMI	Network Management Interface (En)
FS	Fixed Station	NMS	Network Management System
FSI	Fixed Station Interface (Ef)	PR	Portable Radio
IKI	Inter Key Management Facility Interface	PSAN	Public Safety Application Network
ISSI	Inter Sub-System Interface (Eg)	PSTN	Public Switched Telephone Network
KDI	Key Fill Device Interface	RFSS	Radio Frequency Sub System
KFD	Key Fill Device	TDMA	Time Division Multiple Access
KMF	Key Management Facility	TII	Telephone Interconnect Interface (Et)

Εικόνα 86. Αρχιτεκτονική του δικτύου P25 [57]

c. Τεχνικά χαρακτηριστικά του P25

Πριν απαριθμήσουμε τα τεχνικά χαρακτηριστικά, είναι σκόπιμο ν‘ αναφερθούμε στις υπηρεσίες και ειδικότερες λειτουργίες που παρέχει και καλύπτει η τεχνολογία P25, οι οποίες φαίνονται στην Εικόνα 87 και αφορούν στ` ακόλουθα:

- Διαλειτουργικότητα
- Πολλαπλοί προμηθευτές
- Ομαδική ομιλία
- Επιλογή λειτουργίας (conventional/trunked)
- Ασφάλεια

- Αποδεκτή παγκόσμια προτυποποίηση
- Ευέλικτη κάλυψη
- Φωνητικές λειτουργίες και λειτουργίες μεταφοράς δεδομένων
- Διαχείριση από τον χρήστη
- Αποδοτικότητα φάσματος
- Επεκτασιμότητα

Αναφορικά δε με τα τεχνικά χαρακτηριστικά και τις βασικές προδιαγραφές του P25, στη Φάση 1, όπως ήδη αναφέρθηκε βασίσθηκε σε FDMA, με χρήση καναλιού 12,5 KHz, χρησιμοποιώντας τη μέθοδο πρόσβασης ενός χρήστη ανά κανάλι. Μάλιστα, λειτουργεί αναλογικά σε εύρος συχνοτήτων 136-174 MHz για VHF, 403-512 MHz και 806-870 MHz για UHF, ψηφιακά σε εύρος συχνοτήτων 746-806 MHz και μικτά. Αρχικά, η υλοποίηση της Φάσης 2 είχε προγραμματιστεί να χωρίσει το κανάλι 12,5 KHz σε δύο υποδοχές 6,25 KHz, ή FDMA. Ωστόσο, αποδείχθηκε πιο αποδοτικό να χρησιμοποιηθούν οι υπάρχουσες εκχωρήσεις συχνοτήτων 12,5 kHz στη λειτουργία TDMA, με βασικότερο όφελος τη βελτίωση της διάρκεια ζωής της μπαταρίας. Η κίνηση φωνής σε ένα σύστημα Φάσης 2 εκπέμπει με τα πλήρη 12,5 kHz ανά εκχώρηση συχνότητας, όπως κάνει ένα σύστημα Φάσης 1, ωστόσο το κάνει με ταχύτερο ρυθμό δεδομένων 12 Kbit/s επιτρέποντας δύο ταυτόχρονες μεταδόσεις φωνής. Ως τέτοια, οι ασύρματοι πομποδέκτες συνδρομητών εκπέμπουν επίσης με πλήρη 12,5 KHz, αλλά με επαναλαμβανόμενο τρόπο ενεργοποίησης/απενεργοποίησης με αποτέλεσμα τη μισή μετάδοση και επομένως ισοδύναμο 6,25 KHz ανά κάθε ραδιόφωνο. Στη Φάση 2 χρησιμοποιείται πλέον ο αποκωδικοποιητής φωνής Προηγμένης Διέγερσης Πολλαπλών Ζωνών (Advanced Multi-Band Excitation - AMBE+2) για να μειώσει τον απαιτούμενο ρυθμό μετάδοσης bit, έτσι ώστε ένα κανάλι φωνής να απαιτεί μόνο 6.000 bit ανά δευτερόλεπτο (συμπεριλαμβανομένης της διόρθωσης σφαλμάτων και της σηματοδότησης), έναντι του διπλού απαιτούμενου ρυθμού του κωδικοποιητή φωνής Βελτιωμένη Διέγερση Πολλαπλών Ζωνών (Improved Multi-Band Excitation – IMBE) της Φάσης 1. Η συνολική απόδοση του καναλιού είναι 9.600 bit ανά δευτερόλεπτο [242].

Εικόνα 87. Υπηρεσίες του P25 [244]

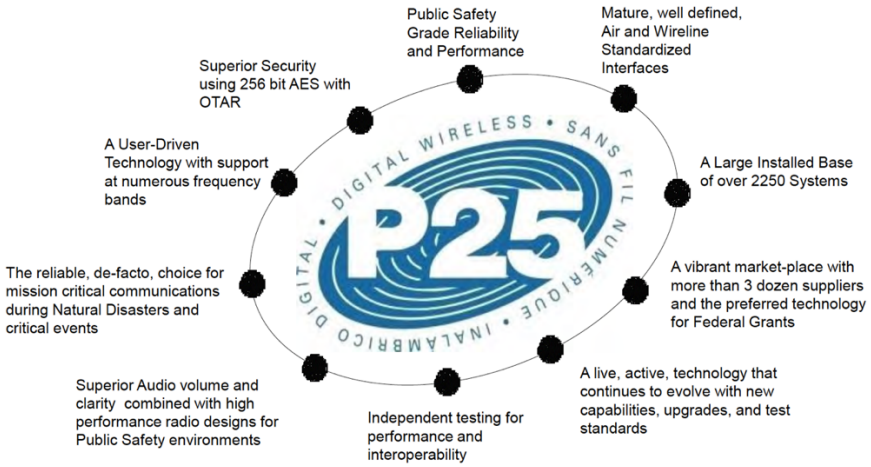
d. Πλεονεκτήματα και μειονεκτήματα του P25

Τα δέκα κορυφαία οφέλη του P25 όπως παρουσιάστηκαν από την Ομάδα Ενδιαφέροντος της Τεχνολογίας P25 (Project 25 Technology Interest Group - PTIG) στη διεθνή έκθεση τηλεπικοινωνιών το 2018, αποτυπώνονται στην Εικόνα 88 και αναλύονται ως ακολούθως:

- Αξιοπιστία και απόδοση στη δημόσια ασφάλεια
- Καλά καθορισμένες, τυποποιημένες διεπαφές αέρα και ενσύρματης σύνδεσης
- Πληθώρα συστημάτων που ξεπερνούν τα 2250 και πλήρως λειτουργική βάση
- Ζωντανή αγορά με περισσότερους από 3 δωδεκάδες προμηθευτές και την προτιμώμενη τεχνολογία για ομοσπονδιακές επιχορηγήσεις
- Διαρκώς εξελίξιμη τεχνολογία σε νέες δυνατότητες, αναβαθμίσεις και πρότυπα
- Απόδοση και διαλειτουργικότητα (εκ των ανεξάρτητων δοκιμών)
- Εξαιρετική ποιότητα ήχου (ένταση και ευκρίνεια) σε συνδυασμό με υψηλής απόδοσης ραδιοεπικοινωνίες για περιβάλλοντα δημόσιας ασφάλειας
- Αξιόπιστη, σίγουρη επιλογή για κρίσιμες επικοινωνίες κατά τη διάρκεια φυσικών καταστροφών και κρίσιμων γεγονότων
- Τεχνολογία καθοδηγούμενη από τον χρήστη με υποστήριξη σε πολλές ζώνες συχνοτήτων

Επομένως, τα πλεονεκτήματα του προτύπου P25 είναι σαφή και αφορούν κύρια τα δίκτυα δημόσιας ασφάλειας και τις λειτουργικές απαιτήσεις καθώς παρέχουν:

- Βελτιστοποιημένη για κάλυψη ευρύτερης περιοχής με χαμηλή πυκνότητα πληθυσμού
- Μεγαλύτερο εύρος από το TETRA στη Φάση I (FDMA), αλλά σχεδόν το ίδιο στη Φάση II (TDMA)
- Υποστήριξη για ταυτόχρονη μετάδοση
- Αποδεδειγμένη λειτουργικότητα (βρίσκονται στο χώρο περισσότερες από δύο δεκαετίες)
- Αποδεδειγμένη διαλειτουργικότητα
- Πολλές εταιρείες παράγουν προϊόντα P25 με αποτέλεσμα να προκύπτουν ανταγωνιστικές τιμές για τα προϊόντα
- Καλύπτουν ένα εκτεταμένο σύνολο χαρακτηριστικών δημόσιας ασφάλειας και κρίσιμων επικοινωνιών
- Δυνατότητα για κλιμακωτή ανάπτυξη, κατά τις απαιτήσεις και τις ανάγκες του φορέα
- Διευκολύνει την προς τα πίσω λειτουργικότητα σε κρίσιμα για την αποστολή περιβάλλοντα



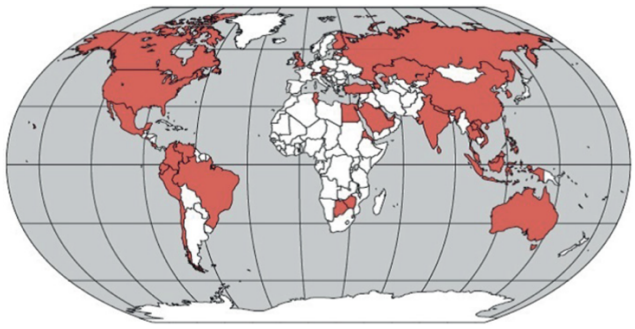
Εικόνα 88. P25: Δέκα κορυφαία οφέλη [245]

Αντίστοιχα τα μειονεκτήματά του αφορούν κυρίως:

- Περιορισμένη δυνατότητα μετάδοσης δεδομένων (έως 9,6 Kbps) και καθυστερήσεις στο πρότυπο της Φάσης ΙΙ.
- Αυξημένο κόστος προμήθειας του υλικού, παρά τον υφιστάμενο ανταγωνισμό
- Χαμηλή ανοχή για παρεμβολές
- Η διαλειτουργικότητα απαιτεί προσεκτικό σχεδιασμό και χειρισμό
- Σημαντικές καθυστερήσεις ήχου και ποιότητας αυτού, ειδικότερα συγκριτικά με αναλογική λειτουργία

e. Περιπτώσεις χρήσης του P25

Αναφέρθηκε ήδη ότι το P25 πολύ γρήγορα ξεπέρασε τα σύνορα των Η.Π.Α. και έγινε το αντίπαλο δέος στις κρίσιμες επικοινωνίες, μαζί με το TETRA που θα δούμε στη συνέχεια. Στην Εικόνα 89 παρουσιάζεται μια παγκόσμια αποτύπωση των Χωρών που χρησιμοποιούν σήμερα την πλατφόρμα P25 για τα δίκτυα δημόσιας ασφάλειας, είτε ως βασική τεχνολογία, είτε εναλλακτικά και υποστηρικτικά μιας βασικής.



Australia	Canada	El Salvador	Kazakhstan	Philippines	Trinidad
Austria	Chile	Eritrea	Kuwait	Russia	Tunisia
Azerbaijan	China	Finland	Latvia	Saudi Arabia	Turkey
Bahrain	Colombia	India	Laos	Singapore	United Kingdom
Bermuda	Costa Rica	Indonesia	Malaysia	Slovenia	USA
Botswana	Czech Republic	Hong Kong	Mexico	South Korea	United Arab Emirates
Brazil	Ecuador	Jamaica	Nepal	Sri Lanka	Venezuela
Brunei	Egypt		Peru	Switzerland	Vietnam
				Thailand	Zimbabwe

Εικόνα 89. Χώρες που χρησιμοποιούν την πλατφόρμα P25 για δίκτυα δημόσιας ασφάλειας

5.2.1.1.2 Terrestrial Trunked Radio (TETRA)

a. Ιστορικά στοιχεία

Το πρότυπο επικοινωνίας TETRA αναπτύχθηκε από το ETSI και έγινε ευρέως γνωστό. Αφορά ένα σύνολο σχετικών προτύπων, στα οποία αναφερόμαστε με τον όρο πρότυπο TETRA. Από την πρώτη του έκδοση έως και σήμερα, χρησιμοποιήθηκε και χρησιμοποιείται τόσο στις κρίσιμες επικοινωνίες, όσο και για εμπορικούς σκοπούς.

Το έργο TETRA ξεκίνησε τη δεκαετία του 1980 και συγκεκριμένα το 1989 εμφανίστηκε ως Κινητό Ψηφιακό Ράδιο Σύστημα (Mobile Digital Trunked Radio System - MDTRS) και ακολούθως, στα μέσα της δεκαετίας του 1990 μετονομάστηκε σε TETRA. Αρχικά, το πρότυπο που προβλέφθηκε ήταν γνωστό ως πρότυπο TETRA Voice plus Data (V+D). Λόγω της ανάγκης περαιτέρω εξέλιξης και βελτίωσης του TETRA, το αρχικό πρότυπο V+D είναι πλέον γνωστό ως TETRA Release 1 (ETSI ETS 300 392-1/1996-02-15) [246]. Οι πρώτες επικοινωνίες του προτύπου αυτού έγιναν πραγματικότητα το 1996. Στην έκδοση αυτή τυποποιήθηκαν υπηρεσίες φωνής και στοιχειώδεις υπηρεσίες δεδομένων. Το πρότυπο προέβλεπε τις δυνατότητες διεκπεραίωσης υπηρεσιών φωνής και ειδικότερα ατομικής κλήσης (επικοινωνία ένας προς ένα – βασική σε όλα τα δίκτυα επικοινωνίας), ομαδικής κλήσης (επικοινωνία ένας προς πολλούς), κλήσης έκτακτης ανάγκης – προτεραιότητας, τη διατήρηση της κλήσης ώστε να διασφαλίζεται να μην απορριφθεί αυτή σε περίπτωση κατειλημμένου δικτύου, την παροχή δεκαέξι διαφορετικών επιπέδων προτεραιότητας, τη Δυναμική Ομαδοποίηση των Συμμετεχόντων σε Κλήση (Dynamic Group Number Assignment - DGNA), τη ρύθμιση του δέκτη σε λειτουργία ακρόασης του περιβάλλοντος χωρίς να είναι γνωστό στον χρήστη, τον καθορισμό περιοχής λειτουργίας των χρηστών και την ετεροχρονισμένη είσοδο ενός σταθμού σε ένα κανάλι όπου ήδη πραγματοποιείται μία επικοινωνία. Οι υπηρεσίες δεδομένων ήταν σαφώς πιο περιορισμένες και συγκεκριμένα επέτρεπαν την αποστολή σύντομων δεδομένων (με μέγιστο εύρος δεδομένων τα 256bytes) γνωστή ως Υπηρεσία Σύντομων Δεδομένων (Short Data Service - SDS) και την αποστολή πακέτων δεδομένων που δημιουργούσε τις προϋποθέσεις το δίκτυο TETRA να μετατρέπεται σε υποδίκτυο IP (Πρωτόκολλο Πακέτου Δεδομένων –Packet Data Protocol -PDP) [247].

Η ανάγκη για περαιτέρω εξέλιξη και διαρκή βελτίωση των τεχνολογιών, ώστε να καλύπτει τις απαιτήσεις των χρηστών στο πλαίσιο μελλοντικών επενδύσεων, αλλά και της διασφάλισης της μακροζωίας οδήγησε το 2016 στη δεύτερη έκδοση του προτύπου και συγκεκριμένα TETRA Release 2 [248]. Στην δεύτερη έκδοση προβλέφθηκε η δυνατότητα του TETRA να λειτουργεί πέρα από το αρχικό όριο εμβέλειας των 58 Km και ειδικότερα έως τα 83 Km, η Λειτουργία Κορμού (Trunk Mode Operation -TMO), η κωδικοποίηση Προσαρμοστικού Πολλαπλού Ρυθμού (Adaptive Multiple Rate -AMR) [249], ο φωνητικός αποκωδικοποιητής

μικτής διέγερσης που λόγω της καταλληλότητάς του κάλυψε επιτυχημένα στρατιωτικές εφαρμογές του ΝΑΤΟ και τέλος μία ολωσδιόλου νέα υπηρεσία, η Βελτιωμένη Υπηρεσία Δεδομένων TETRA (TETRA Enhanced Data Service - TEDS) που φιλοδοξούσε, τη δεδομένη εποχή, να επιτύχει καλύτερη μεταφορά δεδομένων.

b. Βασικά στοιχεία αρχιτεκτονικής TETRA

Το TETRA είναι ένα ψηφιακό φορητό ραδιοσύστημα επικοινωνίας που περιορίζεται ουσιαστικά στα τρία πρώτα επίπεδα του μοντέλου OSI [52]. Τα βασικά δομικά συστατικά της αρχιτεκτονικής που συνθέτουν το πρότυπο TETRA φαίνονται στην Εικόνα 90. Μια τυπική αρχιτεκτονική δικτύου TETRA περιλαμβάνει τους κόμβους (nodes), τους οποίους συναντούμε στη βιβλιογραφία και με τον όρο Υποδομή Μεταγωγής και Διαχείρισης (Switching and Management Infrastructure – SwMI), οι οποίοι διασυνδέονται – υποστηρίζουν τους κινητούς σταθμούς βάσης (Mobile Stations - MS) και τους διανομείς (Line Station – Dispatchers). Ένας ή περισσότεροι κόμβοι είναι δυνατό να υπάρξουν σε μία δομή δικτύου TETRA. Οι κόμβοι συνδέονται με το Κέντρο Διαχείρισης Δικτύου (Network Management) που εξασφαλίζει την απρόσκοπτη λειτουργία, τη συνολική διαχείριση και συντήρηση αυτού. Επίσης, παρέχεται η δυνατότητα απ‘ ευθείας σύνδεσης των φορητών σταθμών, ακόμη και ενσύρματα, με τον τερματικό εξοπλισμό (Terminal Equipment), ο οποίος μπορεί να περιλαμβάνει φορητούς υπολογιστές ή υπολογιστές χειρός [59]. Οι κόμβοι αποτελούνται από τ‘ ακόλουθα βασικά δομικά στοιχεία:

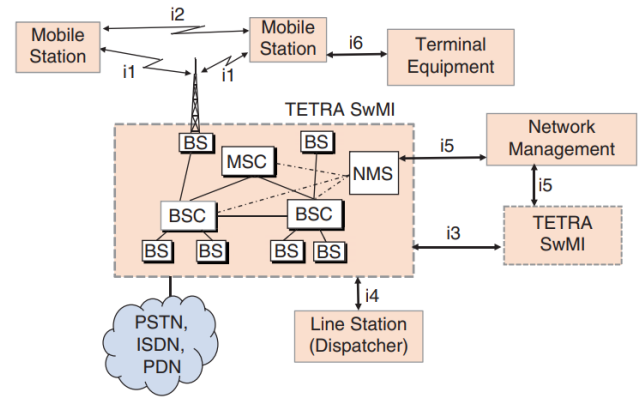
- Σταθμός Βάσης (Base Station - BS)
- Ελεγκτής Σταθμών Βάσης (Base Station Controller - BSC)
- Σύστημα Διαχείρισης Δικτύου (Network Managements System – NMS)
- Κέντρο Μεταγωγής Φορητών (Mobile Switching Center – MSC)

Μεταξύ των οντοτήτων αυτών υπάρχουν ιεραρχικές συνδέσεις που ποικίλλουν ανάλογα με το μέγεθος του δικτύου, αλλά και τον κατασκευαστή, οπότε είναι πιθανό να συναντήσουμε διάφορες παραλλαγές και συνδυασμούς. Το σημαντικό όμως ως προς τη λειτουργία του κόμβου είναι ότι εκτελεί εναλλαγή και μετάδοση πληροφοριών (φωνής και δεδομένων), καθώς επίσης ότι περιλαμβάνει πύλη διασύνδεσης με άλλα δίκτυα και δεδομένα (PSTN, ISDN, GSM, VoIP, IP κ.λπ.) [250]. Επιπλέον, στην αναφερόμενη αρχιτεκτονική παρατηρούμε ότι τυποποιούνται έξι σημαντικές διεπαφές [251]:

- Διεπαφή αέρα (Air Interface – i1), που αναφέρεται στον ραδιοδίαυλο μεταξύ της κινητής μονάδας του συστήματος MS και του BS. Στην περίπτωση αυτή εξασφαλίζεται η πλήρης συνεργασία και συμβατότητα των τερματικών συσκευών διαφορετικών κατασκευαστών με ένα οποιοδήποτε ραδιοδίκτυο TETRA.

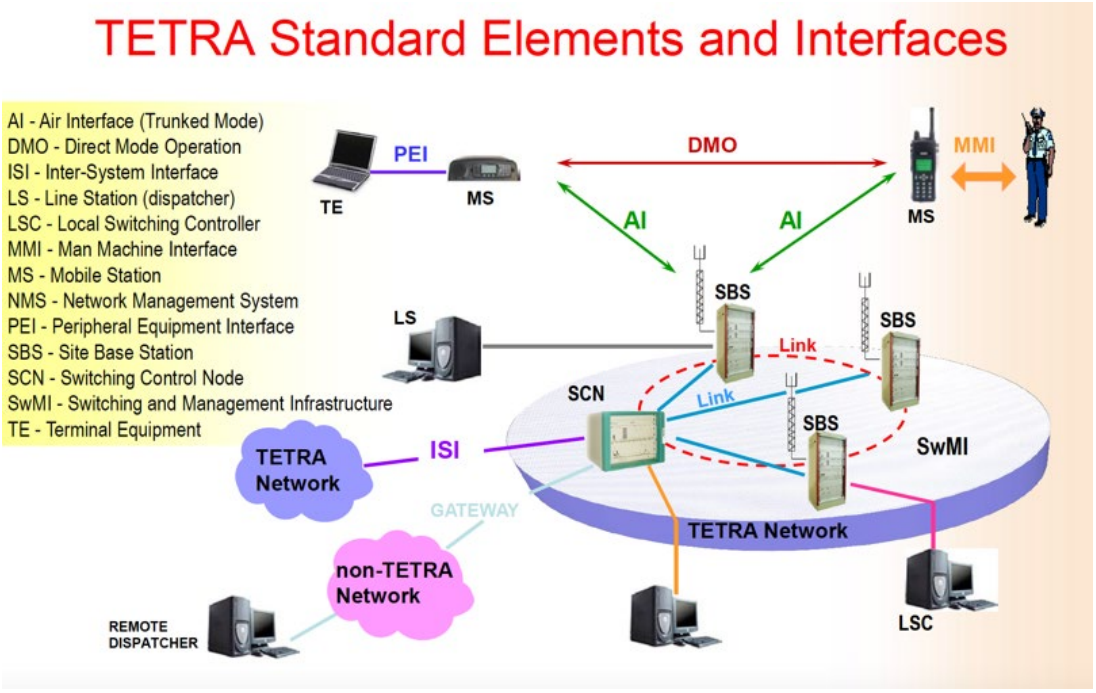
- Διεπαφή απ' ευθείας επικοινωνίας (Direct Mode Interface – i2), που επιτρέπει σε δύο κινητές μονάδες TETRA να επικοινωνούν μεταξύ τους, χωρίς την υποχρέωση διαμεσολάβησης ενός BS. Η συγκεκριμένη διεπαφή καθιστά το TETRA ιδιαιτέρως χρηστικό στις απαιτήσεις της δημόσιας ασφάλειας και των κρίσιμων επικοινωνιών και διαφοροποιεί σημαντικά αυτό από τα κυψελοειδή δίκτυα δημόσιας χρήσης.
- Ενδογενής διεπαφή (Intersystem Interface – ISI – i3), που παρέχει τη δυνατότητα ενδο-διαλειτουργικότητας. Συγκεκριμένα, δίκτυα TETRA διαφορετικών κατασκευαστών, που πληρούν τις προδιαγραφές του ETSI, μπορούν να διασυνδεθούν μεταξύ τους κατά τέτοιο τρόπο ώστε να εξασφαλίζεται η μέγιστη δυνατή συμβατότητα και συνεργασία.
- Διεπαφή (Line Station Dispatcher Interface – i4), που παρέχει τη δυνατότητα σύνδεσης των κόμβων με τους διανομείς
- Διεπαφή διαχείρισης δικτύου (Network Management Interface – i5), που παρέχει τη δυνατότητα σύνδεσης του κέντρου διαχείρισης δικτύου με τους κόμβους της υποδομής
- Διεπαφή τερματικού εξοπλισμού (Terminal Equipment Interface – i6), που παρέχει την δυνατότητα ανεξάρτητης ανάπτυξης των κινητών εφαρμογών του ραδιοδικτύου.

Τα δομικά στοιχεία που συμπληρώνουν την αρχιτεκτονική TETRA, εκτός των όσων αναφέρθηκαν ήδη είναι ο εξοπλισμός του χρήστη, είτε αυτό αφορά σε φορητά και κινητά τερματικά, είτε σε κονσόλες εκφωνητών και διαχειριστών των επιχειρησιακών κέντρων. Η συνολική αρχιτεκτονική, με αποτυπωμένα στο σύνολό τους τα στοιχεία και τις διεπαφές TETRA παρουσιάζονται στην Εικόνα 91.



i1: Air Interface
i2: Direct Mode Interface
i3: Intersystem Interface (ISI)
i4: Line Station (Dispatcher) Interface
i5: Network Management Interface
i6: Terminal Equipment Interface
PSTN: Public Switched Telephone Network
MSC: Mobile Switching Center
BS: Base Station
BSC: Base Station Controller
NMS: Network Management System
SwMI: Switching and Management Infrastructure
PDN: Public Data Network

Εικόνα 90. Αρχιτεκτονική του δικτύου TETRA [59]



Εικόνα 91. Κύρια στοιχεία και διεπαφές δικτύου TETRA [252]

c. Τεχνολογικά χαρακτηριστικά TETRA

Κάποια από τα στοιχεία που συνθέτουν την αρχιτεκτονική είναι τυποποιημένα, για άλλα υπάρχει ένα σύνολο οδηγιών, ώστε να αφήνεται στους κατασκευαστές η ελευθερία στο πλαίσιο της υλοποίησης. Σε κάθε περίπτωση όμως, αξίζει ν' αναφερθούν στο σημείο αυτό τα κύρια τεχνολογικά χαρακτηριστικά και προδιαγραφές του προτύπου. Όλοι οι πάροχοι TETRA πρέπει να προσφέρουν υπηρεσίες και τερματικές συσκευές που πληρούν τις αναφερόμενες προδιαγραφές, οι οποίες εμφανίζονται στον Πίνακα 18 [250].

ΒΑΣΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ	
Περιοχή συχνοτήτων	380 - 400 MHz για δημόσια ασφάλεια και 410 - 430 MHz, 450-470 MHz, 870-876/915-921 MHz για εμπορικές εφαρμογές – επαγγελματική χρήση
Αμφίδρομη επικοινωνία	Frequency Division Duplex FDD
Εύρος αμφίδρομης επικοινωνίας	10 MHz κατερχόμενη ζεύξη
Εύρος ζώνης φερουσών συχνοτήτων	25 KHz
Πολυπλεξία καναλιών	TDMA με 4 χρονοθυρίδες ανά πλαίσιο και 18 πλαίσια ανά πολλαπλό πλαίσιο
Διάρκεια χρονοθυρίδας, πλαισίου, πολλαπλού πλαισίου	14.167 msec, 56.667 msec, 1.02 sec
Ισχύς εκπομπής	Φορητή συσκευή: 15 – 45 dBm (0.03 – 30W) σε βήματα των 5dB Σταθμός Βάσης: 28 – 46 dBm (0.6 – 40W) ανάλογα με την κλάση ισχύος της κινητής μονάδας
Ρυθμός μετάδοσης	36 Kbps
Διαμόρφωση	π/4-QPSK με συντελεστή roll-off a=0.35
Κωδικοποίηση ομιλίας	A-CELP (Algebraic Code – Excited Linear Predictive Codec , 4.8 Kbps)
Ρυθμός μετάδοσης δεδομένων (Data Rate)	Έως 7.2 Kbps ανά κανάλι (Time Slot) και 28.8 Kbps με τη δέσμευση ενός ολόκληρου πλαισίου

Πίνακας 18. Βασικές προδιαγραφές ραδιοδικτύου TETRA

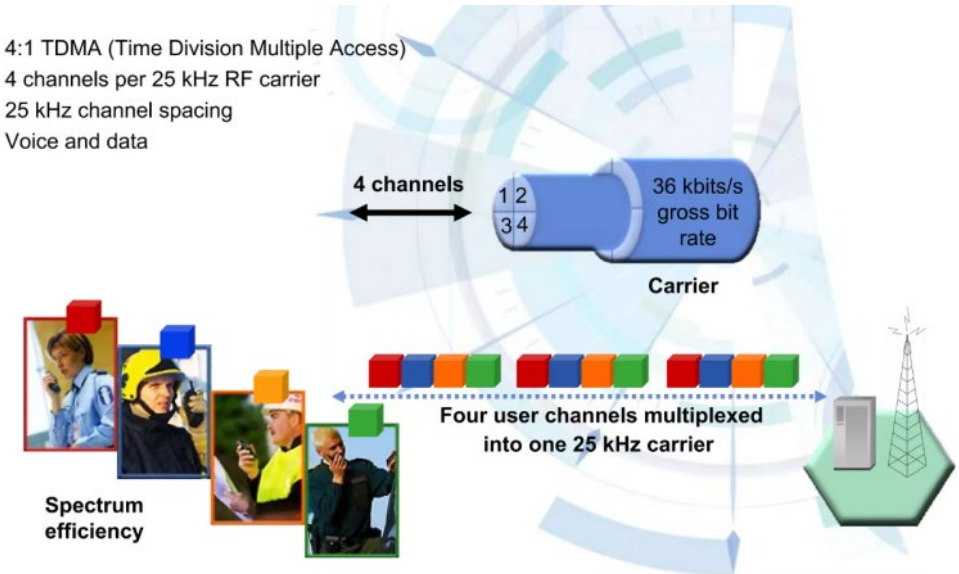
d. Πλεονεκτήματα και μειονεκτήματα του TETRA

Τα πλεονεκτήματα του προτύπου TETRA είναι σαφή και αφορούν κύρια τα δίκτυα δημόσιας ασφάλειας και τις λειτουργικές απαιτήσεις των οποίων καλύπτουν:

- Υψηλή ποιότητα και υψηλή ασφάλεια στις επικοινωνίες
- Διπλή φασματική απόδοση και ιδιαιτέρως αποδοτικό για περιοχές υψηλής πυκνότητας πληθυσμού (4 χρονοθυρίδες στα 25MHz - Εικόνα 92)
- Ευέλικτο εύρος ζώνης δεδομένων (φτάνει έως 28,8 kbps)
- Πολλαπλές υπηρεσίες δεδομένων σε πραγματικό χρόνο (κατάσταση, σύντομα δεδομένα, δεδομένα λειτουργίας κυκλώματος, δεδομένα λειτουργίας πακέτου)
- Half-duplex και full-duplex επικοινωνίες
- Διαλειτουργικό με άλλα δίκτυα (TETRA, ISDN, IP, GSM)
- Συνεχής κάλυψη
- Κλήσεις έκτακτης ανάγκης
- Γρήγορη ρύθμιση κλήσης
- Ταυτόχρονη φωνή και δεδομένα
- Τεχνολογία ανοιχτών προτύπων

Στα μειονεκτήματα θα μπορούσαμε να εντάξουμε:

- Δεν διατίθεται στη ζώνη VHF
- Δεν παρέχει ταυτόχρονη μετάδοση
- Δεν μπορεί να καλύψει τις απαιτήσεις μετάδοσης δεδομένων, καθώς οι ρυθμοί είναι χαμηλοί και σε κάθε περίπτωση μη ικανοί να ικανοποιήσουν τις ήδη αυξημένες ανάγκες



Εικόνα 92. Αποτελεσματικότητα TDMA στο TETRA [253]

e. Περιπτώσεις χρήσης του TETRA

Όπως είναι αναμενόμενο υπάρχει πληθώρα περιπτώσεων χρήσης του TETRA τόσο στις κρίσιμες επικοινωνίες, όσο και στις εμπορικές δραστηριότητες. Τα δίκτυα TETRA που χρησιμοποιούνται από τις κυβερνήσεις για τη δημόσια ασφάλεια, τις στρατιωτικές, αμυντικές και άλλες δημόσιες υπηρεσίες και τις κρίσιμες υποδομές ξεπερνούν σήμερα τα 250 ανά τον κόσμο. Χαρακτηριστικό παράδειγμα αποτέλεσε η εταιρεία Airwave στη Μεγάλη Βρετανία, η οποία ανέλαβε τις επικοινωνίες για όλους τους χώρους κατά τη διάρκεια των Ολυμπιακών Αγώνων του 2012 στο Λονδίνο, χρησιμοποιώντας TETRA. Σήμερα, το δίκτυο αυτό διαθέτει 3600 σταθμούς βάσης και περίπου 350.000 χρήστες. Οι εθνικές υπηρεσίες δημόσιας ασφάλειας πολλών χωρών χρησιμοποιούν τα δίκτυα TETRA. Μερικές μόνο εξ αυτών είναι: Αίγυπτος, Ανδόρα, Αυστρία, Βατικανό, Βουλγαρία, Γερμανία, Δανία, Ελλάδα, Ηνωμένο Βασίλειο, Ισραήλ, Ιρλανδία, Ιορδανία, Κροατία Μπαχρέιν, Νορβηγία, Πορτογαλία, Ρουμανία και Σουηδία. Επίσης, οι σιδηροδρομικές συγκοινωνίες (υπόγειες ή υπέργειες) της Ελλάδας, Ρωσίας, Ισπανίας, Χιλής, Αλγερίας, Μεξικού, Βραζιλίας, τα μέσα μαζικής μεταφοράς σε Ισπανία, Ουγγαρία, Κολομβία και Ηνωμένες Πολιτείες Αμερικής, τα αεροδρόμια του Ελευθέριος Βενιζέλος στην Αθήνα και της Βιέννης στην Αυστρία. Ο κατάλογος όπως είναι αναμενόμενο είναι μακροσκελής και αποδεικνύει ότι το TETRA χρησιμοποιείται σήμερα ως μία από τις βασικές τεχνολογίες επικοινωνίας δημόσιας ασφάλειας, είτε κατ' αποκλειστικότητα, είτε υποστηρικτικά σε συνδυασμό με άλλες τεχνολογίες. Μάλιστα, περισσότερες από 120 χώρες παγκοσμίως χρησιμοποιούν αποκλειστικά δίκτυα TETRA για τις κρίσιμες επικοινωνίες τους [254]. Στο πλαίσιο αυτό, από την έκδοση του TETRA Release 2 έως και σήμερα έχουν αναληφθεί ποικίλες πρωτοβουλίες και γίνεται πολύ δουλειά ώστε το πρότυπο TETRA να εξακολουθήσει να βρίσκεται στη θέση που κατάφερε να βρεθεί. Το σύνολο των εταιρειών παραγωγής τεχνολογιών επικοινωνίας που παράγουν προϊόντα TETRA σε συνεργασία με παγκόσμιους οργανισμούς προτυποποίησης κρίσιμων επικοινωνιών που αφορούν τα δίκτυα δημόσιας ασφάλειας εργάζονται προς την κατεύθυνση εκσυγχρονισμού του. Θεωρείται σχεδόν βέβαιο ότι το πρότυπο TETRA και τα διάφορα προϊόντα του θα μας απασχολήσουν, κύρια στο εγγύς μέλλον αυτή την κατεύθυνση.

5.2.1.1.3 Digital Mobile Radio (DMR)

a. Ιστορικά στοιχεία

Το DMR είναι ένα ακόμη ανοικτό πρότυπο ραδιοεπικοινωνίας που καθορίστηκε από το ETSI το 2005, ως μια άμεση ψηφιακή αντικατάσταση του αναλογικού PMR [255], το οποίο έτυχε ευρείας χρήσης και αποδοχής από κατασκευαστές παγκοσμίως. Σημαντικό ρόλο σ` αυτό διαδραμάτισε και το γεγονός ότι το πρότυπο DMR συμμορφώνεται με τις προδιαγραφές που καθορίζει στις ραδιοεπικοινωνίες και η Ομοσπονδιακή Επιτροπή Επικοινωνιών των Η.Π.Α.

(Federal Communications Commission, - FCC[26]), επομένως διευρύνθηκε δυνητικά η αγορά και το ενδιαφέρον για τη νέα τότε τεχνολογία ξεπέρασε γρήγορα τα ευρωπαϊκά σύνορα. Ο πρωταρχικός στόχος του DMR ήταν να αναπτύξει οικονομικά και προσιτά ψηφιακά συστήματα με σχετικά χαμηλή πολυπλοκότητα [57]. Το πρωτόκολλο DMR καλύπτει τρεις τρόπους λειτουργίας, τους επονομαζόμενους Tier I, II και III.

Τα προϊόντα DMR Tier I προορίζονται για χρήση σε μη αδειοδοτημένες ζώνες των 446 MHz και γι' αυτό περιγράφονται ως μη αδειοδοτημένα (unlicensed). Παρέχουν εμπορικές εφαρμογές χαμηλής κατανάλωσης και περιορισμένο αριθμό καναλιών. Οι συσκευές της συγκεκριμένης λειτουργίας είναι κατάλληλες κατά βάση για προσωπική χρήση και αναψυχή και δεν απαιτούν κάλυψη ευρείας περιοχής, ή προηγμένα χαρακτηριστικά [256].

Το Tier II καλύπτει αδειοδοτημένες ζώνες φάσματος, κατά βάση συμβατικά ραδιοφωνικά συστήματα, είτε κινητά, είτε φορητά που λειτουργούν σε ζώνες συχνοτήτων Private Mobile Radio, PMR από 66-960 MHz. Το πρότυπο ETSI DMR Tier II ονομάζεται συμβατικό αδειοδοτημένο (licensed conventional) και απευθύνεται σε χρήστες που χρειάζονται φασματική απόδοση, προηγμένες λειτουργίες φωνής και ενσωματωμένες υπηρεσίες δεδομένων IP σε αδειοδοτημένες ζώνες για επικοινωνίες υψηλής ισχύος. Το πρότυπο αυτό καθόρισε επικοινωνία TDMA δύο θυρίδων σε κανάλια 12,5 KHz, γεγονός που επί της ουσίας προσφέρει διπλασιασμό χωρητικότητας έναντι της αντίστοιχης αναλογικής επικοινωνίας. [256].

Το DMR Tier III καλύπτει τη λειτουργία κορμού σε ζώνες συχνοτήτων 66-960 MHz και ονομάζεται επίγειο αδειοδοτημένο (licensed trunked). Το πρότυπο Tier III καθορίζει επικοινωνία TDMA δύο θυρίδων σε κανάλια 12,5 kHz. Το Tier III υποστηρίζει χειρισμό φωνητικών και σύντομων μηνυμάτων, με ενσωματωμένα μηνύματα κατάστασης 128 χαρακτήρων και σύντομα μηνύματα έως και 288 bit δεδομένων σε διάφορες μορφές. Υποστηρίζει επίσης υπηρεσία πακέτων δεδομένων σε διάφορες μορφές, συμπεριλαμβανομένης της υποστήριξης για IPv4 και IPv6 [256].

b. Βασικά στοιχεία αρχιτεκτονικής DMR

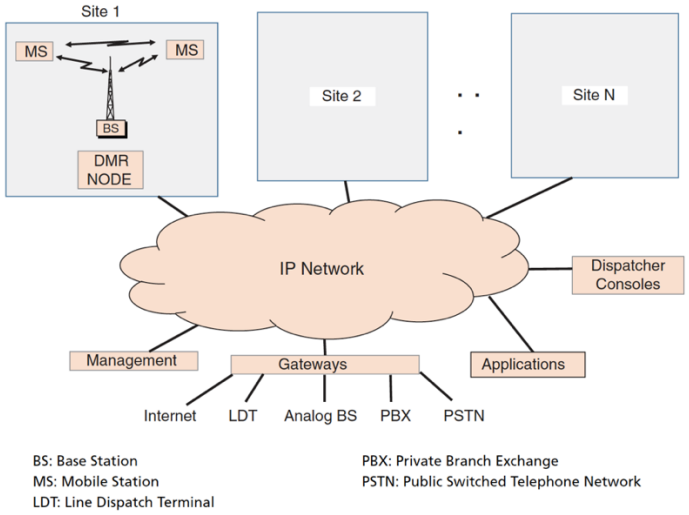
Το DMR είναι πιο κατάλληλο για μεγάλες αγροτικές περιοχές με χαμηλή κίνηση, όπου η ταυτόχρονη μετάδοση λειτουργεί καλύτερα. Τα βασικά στοιχεία της αρχιτεκτονικής, όπως παρουσιάζονται και σχηματικά στην Εικόνα 93 και περιλαμβάνουν [57]:

- Δίκτυο IP (IP network): Είναι η ραχοκοκαλιά ενός δικτύου DMR, που συνδέει τοποθεσίες και πύλες, διακομιστές και εφαρμογές, χρησιμοποιώντας δρομολογητές δικτύωσης που βασίζονται σε IP.

[26] https://www.fcc.gov/

- Πύλες (Gateways): Χρησιμοποιούνται για τη σύνδεση ενός δικτύου DMR με συσκευές και εξωτερικά συστήματα, τα οποία μπορεί να είναι το δημόσιο τηλεφωνικό δίκτυο (PSTN), ένα Ιδιωτικό Ανταλλακτήριο Υποκαταστημάτων (Private Branch Exchange – PBX) που παρέχει εσωτερική επικοινωνία σε έναν οργανισμό ή υποστηρίζει τη διαχείριση εισερχόμενων και εξερχόμενων τηλεφωνικών κλήσεων αυτού, αναλογικούς σταθμούς βάσης δια του οποίου υποστηρίζεται ο έλεγχος κλήσεων, μεταγωγής και πλήρους ενσύρματης λειτουργίας, το διαδίκτυο, ή Τερματικός Αποστολής Γραμμής (Line Dispatch Terminal – LDT) που παρέχει τη δυνατότητα επικοινωνίας με μεγάλο αριθμό χρηστών ραδιοφώνου.
- Κονσόλα αποστολέα (dispatcher console): Περιγράφει στοιχεία που βασίζονται σε υπολογιστή και παρέχουν δυνατότητες ευρείας εμβέλειας για επικοινωνία με όλους τους χρήστες του δικτύου για την εκτέλεση εργασιών αποστολής.
- Διαχείριση δικτύου (management): Περιλαμβάνει ένα ή περισσότερα συστήματα που βασίζονται σε υπολογιστή και αλληλεπιδρούν για την παροχή ποικίλων λειτουργιών όπως η διαμόρφωση των στοιχείων δικτύου και των συσκευών του χρήστη, η παρακολούθηση και η αναφορά χρήσης, απόδοσης και η καταγραφή σφαλμάτων.
- Διακομιστές εφαρμογών (applications): Η διαχείριση δικτύου DMR βασίζεται στην πανταχού παρούσα IP. Επομένως, η διασύνδεση των στοιχείων του και εν τέλει η ανάπτυξή του καθίσταται σχετικά εύκολη.
- Κόμβος DMR: Που περιγράφει τη διασύνδεση των σταθμών βάσης με τους κινητούς σταθμούς ενός δικτύου. Στην αναφερόμενη επικοινωνία εμπλέκονται τρείς ξεχωριστές διεπαφές: (α) διεπαφή αέρα, (β) διεπαφή κορμού και (γ) διεπαφή εφαρμογής δεδομένων.

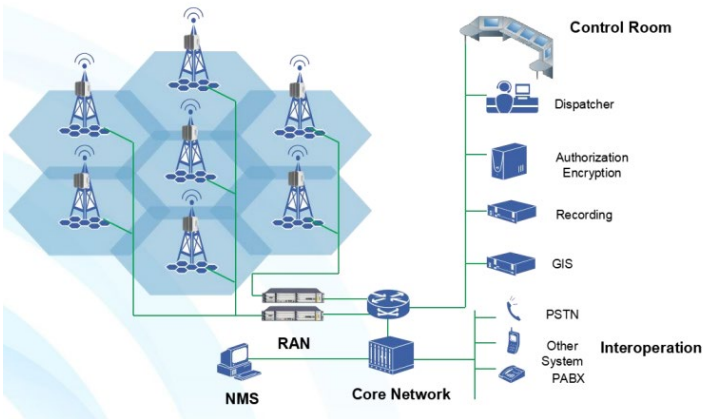
Η διεπαφή αέρα DMR (air interface) και τα πρωτόκολλα σε αυτήν υποστηρίζουν τις επικοινωνίες μεταξύ BS και ραδιοφωνικών σταθμών (κινητοί, φορητοί, σταθεροί), καθώς και μεταξύ δύο σταθμών απ' ευθείας για άμεση λειτουργία.



Εικόνα 93. Αρχιτεκτονική προτύπου DMR [57]

Η διεπαφή κορμού DMR (trunking interface) και τα πρωτόκολλα σ' αυτήν καθορίζουν τη δρομολόγηση, όπως διεξοδικά αναλύεται στο πρότυπο του ETSI TS 102 361-4 [257] και ειδικότερα τις διαδικασίες που σχετίζονται με τον κορμό και αφορούν τον έλεγχο κλήσεων και τις εκχωρήσεις καναλιών στη διεπαφή αέρα. Οι διεπαφές μεταξύ των τοποθεσιών μέσω του δικτύου IP υλοποιούνται κυρίως με λύσεις των προμηθευτών [57]. Μάλιστα, η κατανομή καναλιών σε μια δεδομένη κλήση γίνεται αυτόματα, μέσα από μια διαδικασία που προβλέπει εκχώρηση καναλιών ελέγχου και κυκλοφορίας (αποκλειστικά ή μη). Μια ενδιαφέρουσα οπτική της αρχιτεκτονικής του συστήματος κορμού του DMR (Trunking) παρουσιάζεται στην Εικόνα 94 από την εταιρεία Caltta Communications, θυγατρική του κινεζικού κολοσσού ZTE, όπου προκύπτει ο κυρίαρχος ρόλος του διακομιστή διαχείρισης του δικτύου [258].

Η διεπαφή εφαρμογής δεδομένων DMR (data application interface) επιτρέπει στις κονσόλες αποστολής να επικοινωνούν με τον εξοπλισμό του ιστότοπου (MS, BS, επαναλήπτες, κόμβους). Η διεπαφή αυτή αναπτύχθηκε από μέλη της Ένωσης DMR (Digital Mobile Radio Association) με στόχο να επιτρέψει στις εφαρμογές να επωφεληθούν από τη διαλειτουργικότητα μεταξύ μιας εφαρμογής και υποδομών DMR από διαφορετικούς προμηθευτές [256]. Το πρωτόκολλο είναι γνωστό ως Προδιαγραφές Διεπαφής Εφαρμογής (Application Interface Specification – AIS) και αφορά σε μια συλλογή ανοιχτών προδιαγραφών που ορίζουν τις διεπαφές προγραμματισμού εφαρμογών [57]. Ένα από τα πλεονεκτήματα που παρέχει το πρωτόκολλο είναι ότι επιτρέπει στις κονσόλες αποστολής να συνδέονται σε μια θύρα Ethernet σε BS ή σε επαναλήπτες και να επικοινωνούν χρησιμοποιώντας IP. Αυτή η μέθοδος απλοποιεί σημαντικά την εγκατάσταση και παρέχει αξιοσημείωτη εξοικονόμηση κόστους [259]. Η πλήρης λειτουργία, οι προδιαγραφές αυτού, η αρχιτεκτονική των διεπαφών του και η συνολική επισκόπηση της λειτουργικότητας που παρέχει περιγράφονται στο [260]. Σε σύγκριση με μια ασύρματη διεπαφή, το AIS έχει σημαντικά πλεονεκτήματα. Η ενσύρματη διεπαφή παρέχει ευελιξία για τη διαχείριση μεγάλου αριθμού ομάδων και μειώνει την πιθανότητα ο χειριστής της κονσόλας να χάσει μια κλήση ή μια ένδειξη έκτακτης ανάγκης [259].

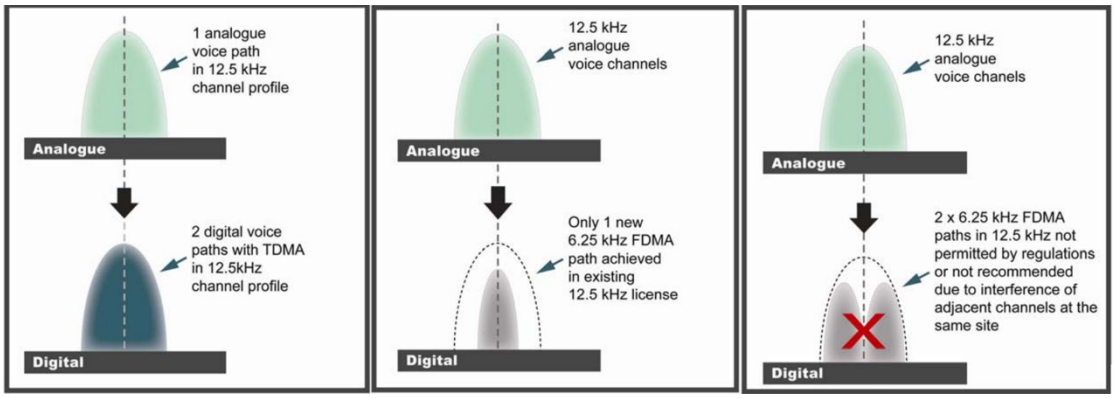


Εικόνα 94. DMR αρχιτεκτονική συστήματος κορμού [258]

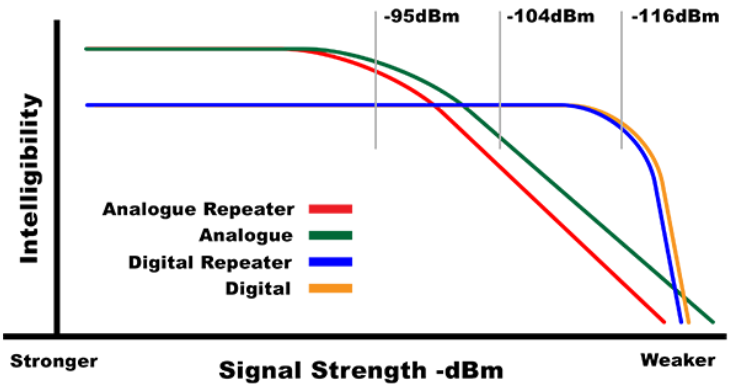
c. Βασικά τεχνικά χαρακτηριστικά του προτύπου DMR

Τα περισσότερα από τα κομβικής σημασίας τεχνικά χαρακτηριστικά του προτύπου έχουν ήδη αναφερθεί, καθώς ήδη αποτυπώθηκε ότι στις Tier II και III η μέθοδος πρόσβασης στο κανάλι είναι η TDMA, το εύρος του καναλιού είναι στα 12,5 KHz και ο αριθμός των χρονοθυρίδων είναι δύο, γεγονός που επιτρέπει σε ένα κανάλι να υποστηρίζει δύο ταυτόχρονες και ανεξάρτητες κλήσεις. Η αποδοτική αξιοποίηση του διαθέσιμου φάσματος προκύπτει γραφικά και στην Εικόνα 95.

Πλέον των άλλων, με τον τρόπο αυτό επιτυγχάνεται απόδοση 6,25 kHz ενώ ελαχιστοποιούνται οι ανάγκες σε προμήθεια εξοπλισμού (επαναλήπτες). Χρησιμοποιεί Διαμόρφωση Συχνότητας Τεσσάρων Επιπέδων (Four Frequency Shift Keying - 4FSK) και κωδικοποιητή ομιλίας AMBE+2. Η φασματική απόδοση είναι 0,768 bit/Hz που επιτυγχάνει ιδανικά ρυθμό μετάδοσης δεδομένων 9,6 Kbps. Η ψηφιακή τεχνολογία DMR διατηρεί την ποιότητα φωνής σε μεγαλύτερο εύρος από την αναλογική (Εικόνα 96), ειδικά στα πιο απομακρυσμένα άκρα του εύρους μετάδοσης. Σ` αυτό εμπλέκονται συνολικά 14 διαφορετικοί κωδικοποιητές του προτύπου, που χρησιμοποιούνται αναλόγως τις απαιτήσεις, που καταφέρνουν να εξαλείφουν τον θόρυβο σε σημαντικό βαθμό και να αναδομούν σήματα υποβαθμισμένων μεταδόσεων παρέχοντας έτσι ποιοτικές φωνητικές λειτουργίες σε ικανοποιητική εμβέλεια και σε μεταβαλλόμενες καταστάσεις πεδίου [256].



Εικόνα 95. Αξιοποίηση φάσματος - καναλιών ψηφιακής και αναλογικής λειτουργίας του DMR [261]



Εικόνα 96. Βελτίωση εύρους με DMR σε σύγκριση με αναλογικό [256]

d. Πλεονεκτήματα και μειονεκτήματα του προτύπου DMR

Από την ανάλυση των τεχνικών χαρακτηριστικών και τη σκιαγράφηση της αρχιτεκτονικής του ανοιχτού προτύπου DMR, έχουν φανεί ήδη τα βασικά πλεονεκτήματα αυτού, όπως αναλυτικά παρατίθενται στη συνέχεια και αναλύονται στα [57] [261]:

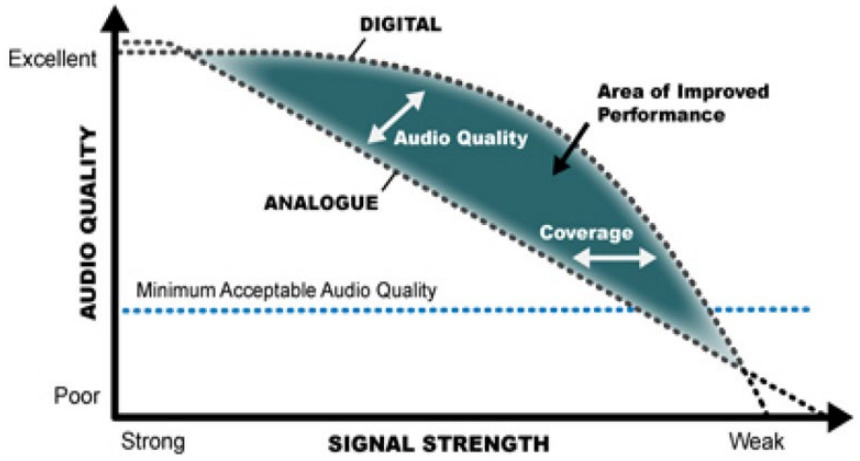
- Στιβαρό, αξιόπιστο και διαλειτουργικό, με αυξημένα επίπεδα ασφάλειας λόγω της κρυπτογράφησης από άκρο σε άκρο
- Διπλασιασμός της χωρητικότητας σε υπάρχοντα αδειοδοτημένα κανάλια, καθώς η λειτουργία TDMA επιτρέπει σε ένα μόνο κανάλι των 12,5 KHz να υποστηρίζει ταυτόχρονα δύο ανεξάρτητες κλήσεις. Επιτυγχάνει μέχρι 1.200 χρήστες σε έναν ιστότοπο και μπορεί να καλύψει έως 15 τοποθεσίες
- Συμβατότητα φάσματος προς τα πίσω με αναλογικά συστήματα παλαιού τύπου (UHF Band)
- Αποτελεσματική χρήση εξοπλισμού υποδομής, καθώς με τη χρήση ενός μόνο επαναλήπτη, μιας κεραίας και ενός απλού εξαρτήματος (duplexer) λαμβάνει ταυτόχρονα δύο κανάλια επικοινωνίας, γεγονός που το καθιστά αποδοτικότερο και οικονομικότερο έναντι της αναλογικής λειτουργίας.
- Μεγαλύτερη διάρκεια ζωής της μπαταρίας και μεγαλύτερη απόδοση ισχύος. Αξιοσημείωτο είναι ότι για κάθε ώρα λειτουργίας, η χρήση TDMA έναντι της FDMA αποφέρει κέρδος μπαταρίας από 19% έως 34% και αντίστοιχα η διάρκεια ζωής της μπαταρίας στο χρόνο ομιλίας είναι συνολικά 40% βελτιωμένος
- Ευκολία στη χρήση και δημιουργία εφαρμογών δεδομένων, απλή εφαρμογή χρήστη με δυνατότητα διαμόρφωσης. Η από άκρο σε άκρο ψηφιακή επικοινωνία του προτύπου επιτρέπει την αποστολή απλών μηνυμάτων έως 40 χαρακτήρες, μετάδοσης IP δεδομένων, εύκολη εγκατάσταση απλών εφαρμογών
- Ευελιξία συστήματος μέσω ταυτόχρονων κλήσεων φωνής και δεδομένων, καθώς ενώ η φωνή χρησιμοποιεί την πρώτη χρονοθυρίδα, η δεύτερη μπορεί να διατεθεί για τη μετάδοση δεδομένων
- Προηγμένες δυνατότητες ελέγχου. Και στην περίπτωση αυτή, ενώ η πρώτη χρονοθυρίδα είναι απασχολημένη σε υπηρεσίες φωνής, η δεύτερη μπορεί να διατεθεί για υπηρεσίες ελέγχου κλήσεων προτεραιότητας ή κλήσεων έκτακτης ανάγκης
- Ανώτερη απόδοση ήχου, ειδικότερα στα άκρα, λόγω της ψηφιακής λειτουργίας και της χρήσης κατάλληλων κωδικοποιητών Διόρθωσης Σφαλμάτων Προώθησης (Forward Error Correction – FEC) και Κυκλικού Έλεγχου Απόρριψης (Cyclic Redundancy Check - CRC). Κατ` αναλογία του γραφήματος της Εικόνα 96, παρατίθεται διάγραμμα που αποτυπώνει την ποιότητα της φωνής συγκριτικά με τη δύναμη του σήματος (Εικόνα 97)

- Παρέχει έλεγχο ταυτότητας, εμφάνιση και αναγνωριστικό καλούντος / ομιλητή
- Εμφάνιση ιστορικού και αναπάντητων κλήσεων
- Αναμονή κλήσης

Το πρότυπο DMR εμφανίζει δύο βασικά μειονεκτήματα. Πρωτίστως ότι είναι επιρρεπές σε παρεμβολές, κύρια λόγω του μεγαλύτερου εύρους συχνοτήτων που αξιοποιεί. Παράλληλα, οι δυνατότητες αποστολής δεδομένων δεν επαρκούν να καλύψουν τις αυξημένες απαιτήσεις των επαγγελματιών δημόσιας ασφάλειας, που ενεργούν στο πεδίο.

e. Περιπτώσεις χρήσεων του DMR

Ως ένα πλήρως δημόσιο ανοικτό πρότυπο, υποστηρίζεται από μεγάλη ποικιλία προμηθευτών που σημαίνει ότι παρέχει ασφάλεια και εμπορική συνέχεια που αναζητούν, καθώς επίσης και της ποικιλίας προϊόντων σε ανταγωνιστικές τιμές. Συναντούμε σήμερα το πρότυπο DMR σε ενεργή χρήση σε περισσότερες από 100 χώρες. Ένας μακρύς και σημαντικός κατάλογος εταιρειών που παρέχουν προϊόντα προτύπου DMR παγκοσμίως εμφανίζεται στο [262] της Ένωσης DMR.



Εικόνα 97. Βελτίωση εύρους με DMR σε σύγκριση με αναλογικό [261]

5.2.1.1.4 TETRAPOL, NXDN, dPMR

Οι τεχνολογίες στενής ζώνης σαφώς και δεν εξαντλούνται με τα πρότυπα που ήδη παρουσιάσθηκαν. Παράλληλα με τα TETRA, P25 και DMR εμφανίσθηκαν και άλλες προσπάθειες που είχαν τον ίδιο πρωτεύοντα στόχο, δηλαδή να καλύψουν τις ανάγκες των επαγγελματιών της δημόσιας ασφάλειας και των κρίσιμων επικοινωνιών εν γένει. Άλλωστε, οι προσπάθειες αυτές λαμβάνουν χώρα την εποχή της μετάβασης από τις αναλογικές στις ψηφιακές τεχνολογίες για την υποστήριξη των δικτύων δημόσιας ασφάλειας. Απ` αυτές θα αναφερθούμε, σαφώς πιο συνοπτικά, σε τρεις ακόμη και συγκεκριμένα στο TETRAPOL, το οποίο παρά το γεγονός ότι παραπέμπει ονομαστικά στο TETRA, αφορά σε ένα εντελώς διαφορετικό πρωτόκολλο επικοινωνίας, στο Ψηφιακό Στενής Ζώνης Επόμενης Γενιάς (Next

Generation Digital Narrowband – NXDN) και στο Ψηφιακό Ιδιωτικό Κινητό Ραδιόφωνο (digital Private Mobile Radio – dPMR), τα οποία παρουσιάζουν σημαντικές ομοιότητες.

a. TETRAPOL

Το TETRAPOL ξεκίνησε την πορεία του πολύ νωρίτερα από το TETRA. Το 1980, οι γαλλικές αστυνομικές δυνάμεις ανέθεσαν στην εταιρία Matra Communication (η οποία σήμερα είναι μέρος του Airbus Group) ν` αναπτύξει ένα μοναδικό δίκτυο δημόσιας ασφάλειας για τις επικοινωνίες τους και έτσι γεννήθηκε το TETRAPOL, που αποτέλεσε το πρώτο πρότυπο δημόσιας ασφάλειας στενής ζώνης στην Ευρώπη. Κύριος στόχος ήταν η απρόσκοπτη παροχή επικοινωνιών φωνής και ως εκ τούτου οι υπηρεσίες που παρέχει το TETRAPOL είναι κάθε είδους φωνητικές επικοινωνίες, υπηρεσίες ανταλλαγής μηνυμάτων, αλλά και περιορισμένες υπηρεσίες συνδεσιμότητας δεδομένων.

Το TETRAPOL χρησιμοποιεί τεχνολογία FDMA χρησιμοποιώντας ένα κανάλι ελέγχου ανά φορέα 12,5 kHz. Η κάλυψη που παρέχει βασίζεται σε σταθερή υποδομή δικτύου και συνεπώς εξαρτάται άμεσα από το εύρος ανάπτυξης ή επέκτασης της υποδομής αυτής. Ένας σταθμός βάσης παρέχει κάλυψη σε ακτίνα λίγων χιλιομέτρων και πάντοτε ανάλογα με τη γεωμορφολογία του εδάφους. Ένας σταθμός βάσης μπορεί να χειριστεί έως και 24 ραδιοφωνικά κανάλια. Ο ρυθμός μετάδοσης φτάνει στα 8 Kbps [41]. Η σύγκριση του TETRAPOL με το TETRA που επιχειρήθηκε από τους [263] ανέδειξε ξεκάθαρη υπεροχή του δεύτερου προτύπου.

Το TETRAPOL, καίτοι ξεκίνησε την πορεία του ως «απόρρητη» τεχνολογία, πολύ γρήγορα έγινε αντιληπτό ότι για να καταστεί ανταγωνιστικό θα πρέπει να εγκαταλείψει τη λογική του κλειστού προτύπου, όπως και έγινε. Μεταγενέστερα, αναγνωρίστηκε από τη Διεθνή Ένωση Τηλεπικοινωνιών (ITU) ως ανοικτό πρότυπο επικοινωνίας και σήμερα χρησιμοποιείται σε 34 χώρες σε όλο τον κόσμο από περίπου 1.850.000 χρήστες, οι περισσότεροι από τους οποίους στη δημόσια ασφάλεια. Εκτός από τη Γαλλία, η Τσεχία, το Μεξικό, η Ισπανία, η Ελβετία και η Βραζιλία, είναι κάποιες εξ αυτών, με την τελευταία να έχει θέσει το TETRAPOL στη διάθεση της Αστυνομίας της ενόψει της διοργάνωσης του Παγκοσμίου Κυπέλλου Ποδοσφαίρου της FIFA το 2014 [264], [265]. Το TETRAPOL προσπαθεί σήμερα να διατηρήσει τα κεκτημένα στην αγορά, μέσα από τη στροφή στην ευρυζωνικότητα και στα υβριδικά δίκτυα επικοινωνίας [46].

b. Next Generation Digital Narrowband (NXDN)

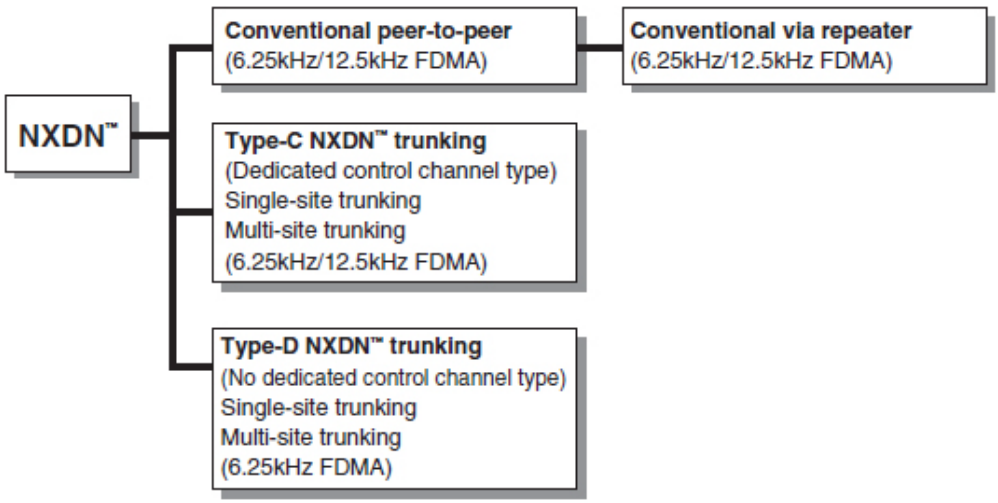
Η δημιουργία του NXDN ξεκίνησε το 2003 ως αποτέλεσμα μίας κοινοπραξίας της JVC Kenwood και της Icom και είναι ένα ψηφιακό πρωτόκολλο στενής ζώνης, το οποίο πλέον αποτελεί πρότυπο αναγνωρισμένο από την ITU. Το πρωτόκολλο ανακοινώθηκε το 2005 στο πλαίσιο της Διεθνής Έκθεση Ασύρματων Τηλεπικοινωνιών (International Wireless

Communications Expo - IWCE) και τα πρώτα προϊόντα εμφανίστηκαν το 2006. Η αρχική στόχευση εντάχθηκε στο πλαίσιο της συνολικής προσπάθειας που επιχειρούνταν τον καιρό εκείνο για χρήση των LMR στις ζώνες VHF, UHF και στη στενή ζώνη. Αρχικά, αφορούσε τους επαγγελματίες και τη βιομηχανία, ενώ στη συνέχεια εισήλθε και στο χώρο της δημόσιας ασφάλειας.

Το πρωτόκολλο λειτουργεί με χρήση της τεχνικής FDMA σε εύρος ζώνης 12,5 KHz, ή 6,25 KHz. Τα δύο κανάλια των 6,25 KHz μπορούν να ρυθμιστούν ώστε να συμπτυχθούν σε ένα των 12,5 KHz. Η αρχιτεκτονική του NXDN είναι τέτοια ώστε δύο κανάλια NXDN, τα οποία χωρούν σε ένα κανάλι 12,5 kHz, μπορούν να εκχωρηθούν σε υπηρεσίες φωνής / φωνής, φωνής / δεδομένων, ή δεδομένων / δεδομένων, κατά την επιλογή του χρήστη. Το πρωτόκολλο χρησιμοποιεί διαμόρφωση FSK τεσσάρων επιπέδων και ο ρυθμός μετάδοσης ανέρχεται σε 4,8 Kbps για εύρος ζώνης 6,25 KHz και το άλλο είναι 9,6 Kbps για εύρος ζώνης 12,5 KHz. Τα χρόνια που ακολούθησαν το πρωτόκολλο NXDN εμπλουτίστηκε με περαιτέρω λειτουργίες (Type-C trunking, Type-D trunking, 2011) και ισχυροποίησε την ασφάλειά του με την υιοθέτηση αλγορίθμων AES και DES (2011) (Εικόνα 98) [266] [267] [268].

Σε σύγκριση με το αναλογικό FM, η τεχνολογία παρέχει ευρύτερη κάλυψη και καλύτερα χαρακτηριστικά πολλαπλών διαδρομών και υποστηρίζει τη μικτή ψηφιακή/αναλογική λειτουργία και γι‘ αυτό προοριζόταν να βοηθήσει τις χώρες που δεν διαθέτουν επαρκείς πόρους συχνοτήτων για τους οργανισμούς δημόσιας ασφάλειας και τους επιχειρηματίες τους.

Το NXDN υλοποιείται από την Kenwood στη σειρά προϊόντων της NEXEDGE[27] και από την Icom στη σειρά προϊόντων της Icom Digital Advanced System, IDAS [269].



Εικόνα 98. Πρότυπο NXDN [267]

Τη συνολική επίβλεψη της ανάπτυξης του προτύπου έχει αναλάβει το NXDN Forum, το οποίο αποτελεί μια κοινότητα 30 μελών, συμπεριλαμβανομένων των εταιριών δημιουργίας

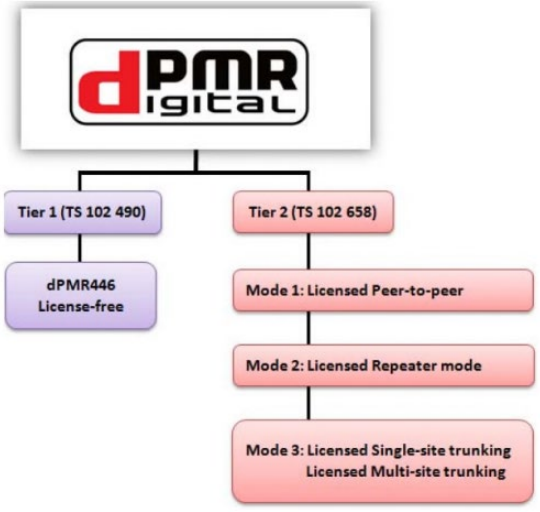
[27] https://comms.kenwood.com/en/products/list.php?func=nexedge

του, αλλά και άλλων μεγάλων εταιριών όπως η Hytera, Zetron, Komutel, Freedom, ενώ ο πλήρης κατάλογος βρίσκεται στο [270]. Τέλος, το 2010 ανακοινώθηκε μια άτυπη συνεργασία με την Ένωση dPMR.

c. digital Private Mobile Radio (dPRM)

Το dPMR είναι ένα ανοιχτό πρότυπο που αναπτύχθηκε από τον ETSI και οι τεχνικές προδιαγραφές του δημοσιεύτηκαν με τις εκθέσεις ETSI TS 102 490 (unlicensed) και ETSI TS 102 658 (licensed) [271] [272] [273]. Στο ίδιο πλαίσιο με το πρότυπο NXDN, η ψηφιακή ιδέα της υιοθέτησης της τεχνικής FDMA σε κανάλι 6,25 KHz εξελίχθηκε σε πρωτόκολλο, που στη συνέχεια έγινε ευρωπαϊκό πρότυπο, φιλοδοξώντας να δώσει απάντηση – αποδοτική λύση στην έλλειψη ραδιοδιαύλων. Χρησιμοποιεί διαμόρφωση 4FSK. Μπορεί να χρησιμοποιηθεί είτε σε μη αδειοδοτημένες φασματικές ζώνες (446 MHz)(Tier I -ETSI TS 102 490), είτε σε αδειοδοτημένες (Tier II -ETSI TS 102 658), προσφέροντας ποικιλία λειτουργιών (Εικόνα 99).

Τη συνολική επίβλεψη της ανάπτυξης του προτύπου έχει αναλάβει η Ένωση dPMR (dPMR Association) που ιδρύθηκε το 2007, η οποία διασφαλίζει τη συμμόρφωση με τα πρότυπα ETSI, οργανώνει και διαχειρίζεται το πρόγραμμα δοκιμών διαλειτουργικότητας και πιστοποίησης συμμόρφωσης, εγκρίνει τη χρήση του εμπορικού σήματος και του λογότυπου dPMR για εξοπλισμό συμβατό με τα πρότυπα ETSI, και προωθεί την ευαισθητοποίηση για τα οφέλη της τεχνολογίας και των ανοιχτών προτύπων στο ευρύτερο κοινό [274]. Οι εφαρμογές του προτύπου στις μέρες μας είναι αρκετές και σημαντικές [275]. Ο Γαλλικός Ερυθρός Σταυρός, οι Γαλλικές και Βελγικές Φυλακές, το αεροδρόμιο της Sharjah, Ηνωμένα Αραβικά Εμιράτα και τα Ηνωμένα Έθνη (UNHCR) σε Αφγανιστάν και Σουδάν εμπιστεύονται προϊόντα dPMR για τις κρίσιμες επικοινωνίες τους.



Εικόνα 99. Διαγραμματική απεικόνιση δυνατοτήτων dPMR

5.2.1.1.5 Σύγκριση των προτύπων στενής ζώνης

Το βασικό χαρακτηριστικό όλων των διαθέσιμων πρωτοκόλλων στενής ζώνης που είτε αναλυτικά, είτε λιγότερο περιγράφηκαν ήδη είναι ότι έχουν σχεδιαστεί για περιφερειακά, ή εθνικά δίκτυα και πληρούν τις βασικές απαιτήσεις φωνητικών επικοινωνιών των χρηστών δημόσιας ασφάλειας, με μικρές δυνατότητες μεταφοράς δεδομένων, λόγω των χαμηλών ρυθμών μετάδοσης αυτών. Είναι λογικό, λόγω και των ετών που οι τεχνολογίες στενής ζώνης δοκιμάζονται στο πεδίο, να έχουν υπάρξει διαφόρων ειδών συγκριτικές μελέτες, τόσο από βιβλιογραφική – ερευνητική προσέγγιση, όσο και από τον εταιρικό κόσμο. Αδιαμφισβήτητο και ταυτοχρόνως ιδιαιτέρως σημαντικό μετρήσιμο μέγεθος αποτελεί η ανταπόκριση της αγοράς και οι επιλογές των καταναλωτών.

Οι τεχνολογίες που εφαρμόζουν όλα τα πρότυπα στενής ζώνης είναι παρεμφερείς, πλην όμως τα ιδιαίτερα χαρακτηριστικά τους, οι τεχνικές και λειτουργικές λεπτομέρειες και τα εταιρικά προϊόντα δια των οποίων υλοποιούνται, δίνουν προβάδισμα επιλογής κάποιων, έναντι των υπολοίπων και πάντοτε κατά περίπτωση. Άλλωστε, οι απαιτήσεις είναι αυτές που οδηγούν τις λύσεις και οι απαιτήσεις είναι κάτι περισσότερο από την υποδομή. Η αποτελεσματικότητα κάθε πρωτοκόλλου αναφέρεται στο πόσο καλά ανταποκρίνεται στις ανάγκες των χρηστών. Επομένως, οι πλέον αρμόδιοι να καταδείξουν τα επικρατέστερα πρότυπα είναι οι χρήστες. Από τις επιλογές των χρηστών παγκοσμίως, στον τομέα της δημόσιας ασφάλειας, είτε αναφερόμαστε σε κυβερνητικές επιλογές, είτε σε μεμονωμένους χρήστες – επαγγελματίες, διαφαίνεται ένα ξεκάθαρο προβάδισμα του προτύπου TETRA έναντι των υπολοίπων, καθώς παρά το γεγονός ότι αναπτύχθηκε ως πρωτόκολλο επικοινωνίας της Ευρωπαϊκής Ένωσης, έγινε το παγκόσμιο «de facto» πρότυπο για κρίσιμες επικοινωνίες σε περισσότερες από 120 χώρες και περίπου 3 εκατομμύρια χρήστες παγκοσμίως, με εξαίρεση τη Βόρεια Αμερική, όπου την πρωτοκαθεδρία διατηρεί το P25.

Ωστόσο, δεν μπορούμε να προσδώσουμε αντίστοιχη τεχνολογική υπεροχή, καθώς τούτο αναφέρεται στην προτεραιοποίηση των αναγκών κάθε «πελάτη» της δημόσιας ασφάλειας για την κάλυψη των λειτουργικών του απαιτήσεων. Για άλλους είναι σημαντικότερο να καλύψουν τις ανάγκες υψηλής επισκεψιμότητας, έναντι της επαρκούς κάλυψης μια ιδιαιτέρως μεγάλης περιοχής. Σε πολλές περιπτώσεις κυρίαρχος οδηγός αποτελεί η δυνατότητα χρηματοδότησης του έργου προμήθειας και εγκατάστασης ενός δικτύου επικοινωνίας δημόσιας ασφάλειας. Το ίδιο σημαντικό μπορεί να θεωρηθεί από πολλούς το χαρακτηριστικό της διαχείρισης του δικτύου και των διαθέσιμων πόρων, ο βαθμός πολυπλοκότητας της υποδομής, η δυνατότητα και ευχρηστία στην τροποποίηση, επισκευή ή αναδιαμόρφωση, εφόσον απαιτηθεί και τους χρόνους και πόρους που τούτο απαιτεί. Σε άλλες περιπτώσεις

κυρίαρχο χαρακτηριστικό αποτελεί η διαλειτουργικότητα, τόσο με την κατεχόμενη υποδομή, όσο και με άλλη που λειτουργεί παράλληλα, ή υποστηρικτικά.

Ως κρίσιμα σημεία υπεροχής κάθε πρωτοκόλλου αναφέρονται τ` ακόλουθα [41], [276], [263], [277], [278], [279], [53]:

- Το P25 επιτρέπει στους επαγγελματίες της δημόσιας ασφάλειας να επικοινωνούν μεταξύ τους σε καταστάσεις έκτακτης ανάγκης, διατηρώντας παράλληλα τα ιδιωτικά τους δίκτυα σε καθημερινές επιχειρήσεις.
- Το P25 επιτρέπει σε κάθε κατασκευαστή να παράγει συμβατό εξοπλισμό. Ομοίως, θεωρείται δεδομένο ότι οι συσκευές που χρησιμοποιούν το DMR μπορούν να χρησιμοποιηθούν σε συνδυασμό μεταξύ τους. Αυτό παρέχει ευελιξία και υγιή ανταγωνισμό, προς όφελος της επιλογής των χρηστών.
- Το P25 έχει δυνατότητα εύκολης επιλογής των τριών τρόπων λειτουργίας του (αναλογική, συμβατική ψηφιακή, κορμού), ομοίως το DMR υποστηρίζει τη δυνατότητα επιλογής αναλογικής / ψηφιακής λειτουργίας, με εύκολη εναλλαγή. Το TETRA έχει χαμηλές δυνατότητες διαλειτουργικότητας μεταξύ ψηφιακών και αναλογικών τερματικών.
- Η διαλειτουργικότητα του TETRA είναι σε χαμηλά επίπεδα, καθώς η προσαρμογή ενός ευρωπαϊκού συστήματος TETRA σε αντίστοιχο της Μέσης Ανατολής, Αφρικής, Ασίας, Νότιας και Λατινικής Αμερικής είναι πολύπλοκη.
- Το P25 προσφέρει μια αξιόπιστη λύση για τους χρήστες που δεν χρειάζονται προηγμένες λειτουργίες, επιτρέπει την κάλυψη μεγάλων γεωγραφικών περιοχών, με χαμηλή πυκνότητα χρηστών, όπως και το πρότυπο DMR.
- Το P25 και το DMR προσφέρουν εύκολη ενσωμάτωση με παλαιού τύπου συστήματα, με δεδομένο ότι επιτρέπουν την αναλογική λειτουργία. Ανάλογη ενσωμάτωση είναι εφικτή και στο TETRA, με πιο τεχνολογικά περίπλοκη διαδικασία.
- Το TETRA επιτυγχάνει σημαντικά μεγαλύτερους ρυθμούς (έως και 4 φορές) μετάδοσης δεδομένων ανά φορέα από κάθε άλλο πρότυπο (Πίνακας 19).
- Το TETRA υποστηρίζει ταυτόχρονες υπηρεσίες φωνής και δεδομένων, καλύπτοντας τις δύο ανάγκες με ένα ενιαίο δίκτυο, σε αντίθεση με το P25 που για να ανταποκριθεί σε ανάλογη λειτουργία απαιτεί επιπρόσθετες τεχνολογικές ρυθμίσεις / εξοπλισμό.
- Το TETRA παρέχει λειτουργία full-duplex διαίρεσης χρόνου των τερματικών, η οποία προσφέρει ενδιαφέρουσες δυνατότητες στους χρήστες, διευκολύνει τη λειτουργία «hands-free», την ενσωμάτωση με την τηλεφωνία, και βελτιωμένη απόδοση σε περιπτώσεις κακής διάδοσης ραδιοσυχνοτήτων.
- Το TETRA δίνει έμφαση στην ασφάλεια του δικτύου, παρέχοντας κρυπτογραφημένες επικοινωνίες από άκρο σε άκρο και ελέγχοντας την ταυτότητα του χρήστη, έτσι ώστε

κάθε τερματικό που προσπαθεί να αποκτήσει πρόσβαση στο δίκτυο χωρίς εξουσιοδότηση εντοπίζεται αυτόματα (Πίνακας 19).

- Το TETRA έχει σχεδιαστεί να υποστηρίζει μεγάλους όγκους κίνησης με μικρές κυψέλες και μεγάλο αριθμό καναλιών, το DMR και το TETRAPOL λειτουργεί με μεγάλα κελιά παρόμοια με αναλογικά συστήματα. Αυτή η διαφορά της ακτίνας κυψέλης μπορεί να δημιουργήσει απαιτήσεις περισσότερων σταθμών βάσης για να καλύψουν την ίδια περιοχή και ν' αυξήσει το κόστος της υποδομής. Χαρακτηριστικό είναι δε ότι οι ακτίνες κάλυψης του TETRAPOL είναι κατά 50% ισχυρότερες από τις αντίστοιχες του TETRA (Πίνακας 19).
- Τα στοιχεία της υποδομής του TETRA (σταθμοί βάσης και κόμβοι μεταγωγής) εμφανίζουν πολυπλοκότητα και δυσκολίες στην κατανόηση, διαχείριση και επαναδιαμόρφωση.
- Η συντήρηση των δικτύων TETRA είναι πιο απαιτητική από τα υπόλοιπα, τόσο σε πόρους, όσο και σε εκπαίδευση.
- Το TETRA απαιτεί ένα κανάλι συνεχούς ελέγχου στον αέρα, επομένως οι απαιτήσεις τροφοδοσίας ενός σταθμού βάσης μπορεί να είναι αρκετές φορές μεγαλύτερες από ό,τι για τους σταθμούς βάσης DMR.
- Για τη διαμόρφωση σήματος, το TETRA απαιτεί γραμμικούς ενισχυτές υψηλής ισχύος που έχουν ως αποτέλεσμα αυξημένη κατανάλωση ρεύματος και χαμηλή απόδοση λόγω της συνδυασμένης διαμόρφωσης πλάτους και φάσης
- Τα TETRA και P25 εκμεταλλεύονται ένα ώριμο περιβάλλον πολλαπλών πωλητών, επομένως είναι εύκολο για τον χρήστη να επιλέξει τον καλύτερο προμηθευτή. Το DMR είναι αρκετά νέο για ένα τέτοιο περιβάλλον.
- Το TETRA είναι συχνά η καλύτερη επιλογή για μεσαίας έως υψηλής χωρητικότητας κεντρικά δίκτυα με μεγάλο όγκο κίνησης και περιοχές χαμηλής κάλυψης, όπως μεγάλες βιομηχανικές εγκαταστάσεις, μεγάλες πανεπιστημιουπόλεις, αεροδρόμια και ανάλογα περιβάλλοντα.

PPDR Technology	TETRA Release 1	TETRA Release 2	TETRAPOL	DMR
Frequency bands	Around 400 MHZ	Around 400 MHZ	Around 400 MHZ	UHF (406–470 MHz), VHF (137–174 MHz)
Data throughput	7.2–28.8 kbit/s	15.6–269 kbit/s	7.2 kbit/s	Up to 9.6 kbit/s
Range	Limited to 58 km Typically 8 km (urban)	Limited to 58 km Typically 8 km (urban)	Limited to 28 km Typically 6 km (urban)	Up to 40 km
Latency Delay	Around 250 ms	Around 200 ms	Around 250 ms	Below 100 ms
Protocol supported	Clear/encrypted speech, circuit mode, IP, short data service, supplementary services	As TETRA release 1 (fully compatible)	Teleservices, data services, supplementary services	All the ones defined in ETSI TR 102.361
Security capabilities	Terminal authentication with three classes of data encryption	Expansion of TETRA release 1 with AMR and MELPe	End-to-End encryption	40-bit ciphering
Location Capabilities	Location information protocol	TETRA location service	GPS-based positioning services	Supported

Πίνακας 19. Τεχνικά χαρακτηριστικά προτύπων επικοινωνίας TETRA, TETRAPOL, DMR

5.2.1.2 Επικοινωνίες ευρείας ζώνης (wideband)

Οι περισσότερες από τις ραδιοτεχνολογίες στενής ζώνης που είδαμε ήδη εξελίσσονται σταδιακά σε μια τεχνολογία με εφαρμογές αυξημένου ρυθμού δεδομένων (ευρεία ζώνη), παρασυρόμενες από την αναγκαιότητα κάλυψης νέων απαιτήσεων των επαγγελματιών της δημόσιας ασφάλειας [280]. Ως μεσοσταθμό της πορείας προς τις πλήρως ευρυζωνικές τεχνολογικές λύσεις, θεωρούμε τις επικοινωνίες ευρείας ζώνης. Το χαρακτηριστικότερο, αν και όχι το μοναδικό, παράδειγμα της κατηγορίας αποτελεί η επέκταση του TETRA και ο εμπλουτισμός του με την υπηρεσία Βελτιωμένη Υπηρεσία Δεδομένων TETRA (TETRA Enhanced Data Service - TEDS), η οποία εντάχθηκε στη δεύτερη έκδοση του προτύπου TETRA Release 2.

5.2.1.2.1 TETRA Enhanced Data Service (TEDS)

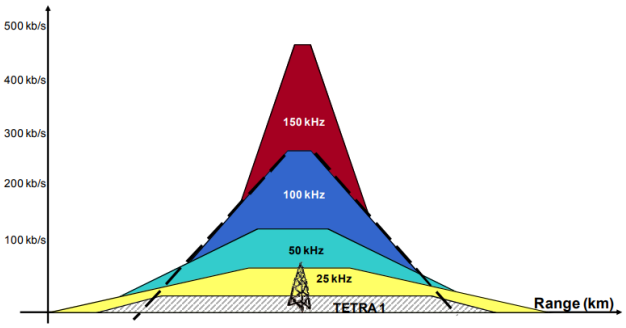
Η ανοδική τάση στην ταχύτητα δεδομένων των δικτύων κινητής τηλεφωνίας και η αυξανόμενη δημοτικότητα των δυνατοτήτων του διαδικτύου και των εφαρμογών πολυμέσων, οδήγησαν στην ανάπτυξη της δεύτερης έκδοσης του προτύπου TETRA, που είχε ως κυρίαρχο στόχο την επίτευξη τουλάχιστον δεκαπλάσιου ρυθμού δεδομένων. Το έργο της ανάπτυξης του TETRA Δεδομένων Υψηλής Ταχύτητας (TETRA High Speed Data - HSD), ως νέας υπηρεσίας του TETRA Release 2, κατάλληλο για εφαρμογές πολυμέσων υψηλής ταχύτητας που βασίζονται σε IP, ανατέθηκε στην Ομάδα Εργασίας 4 (WG4), μία από τις ομάδες εργασίας στο TC-TETRA. Το κύριο αποτέλεσμα αυτής της εργασίας τυποποίησης, που ολοκληρώθηκε στα τέλη του 2005, είναι το TEDS που έγινε διαθέσιμο από τον Σεπτέμβριο

του 2006, ως το ETSI Technical Standard TS 100 392-2 [281], [282]. Στην πορεία προς τις πλήρως ευρυζωνικές επικοινωνίες, οι οποίες θα παρέχουν σε πολύ μεγάλο βαθμό επίγνωση της κατάστασης, προέκυψε η ανάγκη για διαρκή συνδεσιμότητα με επαρκή ρυθμό μετάδοσης δεδομένων ώστε να λειτουργεί απρόσκοπτα η ταυτόχρονη εκπομπή φωνής και δεδομένων και η άμεση ανταλλαγή πληροφοριών με τον επαγγελματία που ενεργεί στο πεδίο. Η πορεία αυτή αποτυπώνεται σχηματικά στην Εικόνα 100 [253].

Η νέα υπηρεσία HSD χρησιμοποιεί διαφορετικά εύρη ζώνης ραδιοσυχνοτήτων (RF κανάλια) και επιτυγχάνει σημαντικά βελτιωμένους ρυθμούς δεδομένων [248]. Τα κύρια χαρακτηριστικά της είναι:

- Πλήρης και εύκολη συμβατότητα με την πρώτη έκδοση του προτύπου (TETRA Release 1). Έχει σχεδιαστεί για όλες τις εφαρμογές του τμήματος της αγοράς TETRA και η πρόσβαση στα κανάλια TEDS επιτρέπεται μόνο μέσω του καναλιού ελέγχου TETRA 1, χρησιμοποιώντας μια τεχνική TDMA 4 χρονοθυρίδων [282].
- Τα εύρη ζώνης ραδιοσυχνοτήτων που υποστηρίζονται είναι 25, 50, 100 και 150 KHz και η διαμόρφωση είναι πολλαπλών επιπέδων, ανάλογα με τις λειτουργίες που θέλουμε να εξυπηρετήσουμε, ώστε να ενισχυθεί η απόδοση δεδομένων του συστήματος και να ενεργοποιηθεί η πραγματική ικανότητα που παρέχει (HSD) [282]. Ο ρυθμός μετάδοσης δεδομένων που επιτυγχάνεται για κάθε εύρος συχνοτήτων και διαφορετική διαμόρφωση προσφέρει ευελιξία επιλογής όπως προκύπτει από τον Πίνακας 20. Οι ρυθμοί που επιτυγχάνονται κινούνται από 10 έως 500 Kbps και η βελτίωση αυτών συγκριτικά με την πρώτη έκδοση του πρωτοκόλλου είναι ξεκάθαρη και προφανής (Εικόνα 101) [283].
- Ισχυρός κωδικοποιητής turbo-code για κωδικοποίηση καναλιών
- Παρέχεται η δυνατότητα για τρεις διαφορετικές κατηγορίες μεταφοράς δεδομένων, δηλαδή μια σε πραγματικό χρόνο για ζωντανές μεταδόσεις ήχου και βίντεο, μια για εφαρμογές με διακοπτόμενες μεταδόσεις μικρών όγκων δεδομένων και μια παρασκηνίου για μεταφορά αρχείων και εφαρμογές περιήγησης στο διαδίκτυο. Για κάθε κατηγορία δεδομένων, το πρωτόκολλο TEDS επιτρέπει τη διαπραγμάτευση των χαρακτηριστικών QoS, όπως η απόδοση, η καθυστέρηση, η προτεραιότητα και η αξιοπιστία.
- Ύπαρξη μηχανισμού «προτεραιότητας δεδομένων» που επιτρέπει στον MS να υποδεικνύει μια προτεραιότητα λήψης από τον BS δεσμευμένες υποδοχές για μετάδοση δεδομένων πακέτων.
- Δυνατότητα ανάπτυξης τομεακών κεραιών ως μέσο επέκτασης της κάλυψης του καναλιού υψηλής ταχύτητας TEDS σε αυτήν του καναλιού ελέγχου TETRA 1, χωρίς την ανάγκη ανάπτυξης πρόσθετων σταθμών βάσης.

Εικόνα 100. Επιχειρησιακή εξέλιξη του TETRA [253]



Εικόνα 101. Συγκριτική αποτύπωση ρυθμού δεδομένων TETRA Release 1 και Release 2 [283]

Modulation	Channel Type (Bandwidth)			
	25kHz	50kHz	100kHz	150kHz
π/4-DQPSK	15.6			
π/8-D8PSK	24.3			
4-QAM	11	27	58	90
16-QAM	22	54	116	179
64-QAM (r=1/2)	33	80	175	269
64-QAM (r=2/3)	44	107	233	359
64-QAM (r=1)	66	160	249	538

Πίνακας 20. Ρυθμοί δεδομένων που υποστηρίζει το TEDS ανά εύρος καναλιών και διαμόρφωση [248]

Τα πρότυπα TETRA Release 2 είναι ήδη πλήρως ολοκληρωμένα και η πραγματική διαθεσιμότητα προϊόντων εξαρτάται από τα σχέδια ανάπτυξης των διαφόρων κατασκευαστών. Χαρακτηριστικό παράδειγμα υλοποίησης αποτελεί το δίκτυο δημόσιας ασφάλειας της Νορβηγίας, το Nødnett, το οποίο έχει θέσει στη διάθεση των επαγγελματιών της δημόσιας ασφάλειας της Νορβηγίας προϊόντα TETRA TEDS. Χαρακτηριστικά στιγμιότυπα των προηγμένων πλέον λειτουργιών που είναι στη διάθεσή τους φαίνονται στην Εικόνα 102. Το Nødnett παρέχει επικοινωνίες φωνής και δεδομένων και υποστηρίζει υπηρεσίες έκτακτης ανάγκης σε διάφορα αστικά και αγροτικά περιβάλλοντα. Στο Όσλο, το ψηφιακό σύστημα διεκπεραιώνει περισσότερες από 600.000 κλήσεις το μήνα. Το TEDS βελτιώνει τις υπηρεσίες στο πεδίο και τη διαλειτουργικότητα, η οποία υπερβαίνει πλέον τα νορβηγικά σύνορα και συνδέεται χωρίς προβλήματα με το γειτονικό Σουηδικό δίκτυο TETRA. Το Nødnett έχει περισσότερους από 2.100 σταθμούς βάσης που καλύπτουν τα 324.000 km^2 γης της Νορβηγίας [284].

Εικόνα 102. Περίπτωση χρήσης: Nødnett TEDS [285]

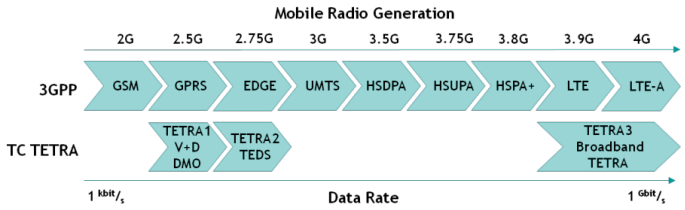
	TETRAPOL	TETRA Release 1	TEDS	P25 phase 1	P25 phase 2
Release date	1980s	1995	2005	1995	2010
Developing organization	Airbus Defence and Space	ETSI	ETSI	TIA	TIA
Vendor support	Single	Multiple	Multiple	Multiple	Multiple
Modulation	GMSK	$\pi/4$-DQPSK	4/16/64-QAM	C4FM	C4FM
Access method	FDMA	TDMA (4 slots)	TDMA (4 slots)	FDMA	TDMA (2 slots)
Frequency bands (MHz)	VHF, UHF, or 800	VHF, UHF, or 800	VHF, UHF, or 800	VHF, UHF, 700, 800, or 900	VHF, UHF, 700, 800, or 900
Channel bandwidth (KHz)	12.5	25	25, 50, 100, or 150	12.5	6.25
Peak data rate (Kbps)	8	28.8	473	9.6	9.6
Driven applications	Voice and NB data services	Voice and NB data services	Voice and WB data services	Voice and NB data services	Voice and NB data services
Professional use	only PS	PS and other professional uses	PS and other professional uses	only PS	only PS

Πίνακας 21. Τεχνικά χαρακτηριστικά προτύπων TETRA, TETRAPOL, TEDS, P25 [43]

Τα πλεονεκτήματα της ξεχωριστής αυτής υπηρεσίας του TETRA που εντάχθηκε στη δεύτερη έκδοσή του είναι εμφανή και ιδιαιτέρως σημαντικά και σε κάθε περίπτωση προδιαγράφουν την πορεία προς την ευρυζωνικότητα. Συμπληρώνοντας τη σύγκριση των προτύπων επικοινωνίας στενής ζώνης, προκύπτει η σαφέστατη υπεροχή του TEDS έναντι αυτών (Πίνακας 21) [43].

Ωστόσο, στα μειονεκτήματα θα μπορούσαμε να εντάξουμε κάποια χαρακτηριστικά, όπως η κακή κάλυψη σε απομακρυσμένες περιοχές, η συμφόρηση του δικτύου, ιδιαιτέρως σε απαιτητικά περιβάλλοντα και ενδεχομένως η αύξηση των επιπέδων στρες του χρήστη από την «υπερφόρτωσή» του με επιπλέον συσκευές.

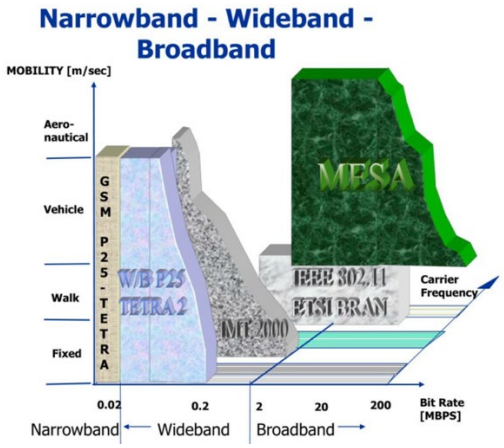
Σε όλη αυτή την πορεία προκύπτει αλληλεξάρτηση και αλληλεπίδραση των τεχνολογιών, κάτω από την ομπρέλα του κοινού σκοπού, που εν προκειμένω δεν είναι άλλος από την εκπλήρωση των ποιοτικά και τεχνολογικά αυξημένων απαιτήσεων της δημόσιας ασφάλειας. Υφίσταται παράλληλη πορεία εξέλιξης, όπως δηλαδή αποτυπώνεται στην Εικόνα 103, ως προς την αντίστοιχη των προτύπων της 3GPP που καλύπτουν τις τεχνολογικές γενιές ασύρματων επικοινωνιών, από αυτή του 2G έως τη γενιά του 4G.



Εικόνα 103. Αντιστοίχιση προτύπων 3GPP και εκδόσεων TETRA [286]

Η μετάβαση από τη δεύτερη έκδοση του TETRA Release 2 (2016) σε μια θεωρητική υλοποίηση της TETRA Release 3, σχεδιάστηκε να πραγματοποιηθεί σε τρεις φάσεις. Η πρώτη (2020) υλοποιείται με την ένταξη της τεχνολογίας LTE, η δεύτερη (2024) αντίστοιχα της LTE Advanced (4G / LTE-A) και η τρίτη (2028) οριοθετείται από την πλήρη μετάβαση στην ευρυζωνική τεχνολογία (4G / 5G). Η ίδια πρόβλεψη [286] θέλει την ανάπτυξη ενός ευρυζωνικού δικτύου TETRA 3 και την κάλυψη των κενών ευρυζωνικότητας από ένα εθνικό δίκτυο ευρείας ζώνης πακέτων δεδομένων TEDS, ως εναλλακτική λύση.

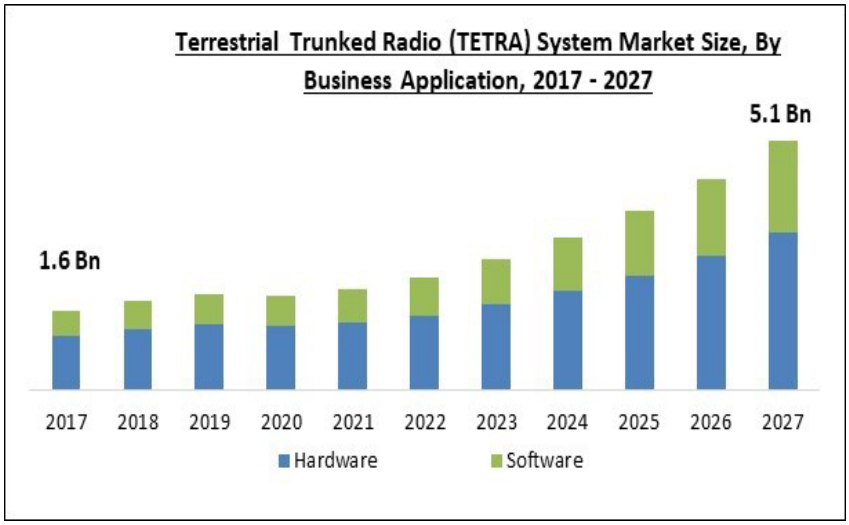
Αξίζει δε αναφοράς μια προσπάθεια που έγινε στο χώρο των επικοινωνιών της δημόσιας ασφάλειας, η οποία παρά το γεγονός ότι ξεκίνησε φιλόδοξα, δεν κατάφερε να αποφέρει τα αναμενόμενα αποτελέσματα. Τον Ιανουάριο του 2001, ο ETSI και ο Σύνδεσμος Βιομηχανίας Τηλεπικοινωνιών (Telecommunications Industry Association – TIA) οριστικοποίησαν συμφωνία συνεργασία για την ανάπτυξη τεχνικών προδιαγραφών επέκτασης του TETRA σε πλήρως ευρυζωνική λειτουργία. Το έργο ονομάστηκε MESA, αφενός από το γεγονός ότι η εναρκτήρια συμφωνία υπογράφηκε στην πόλη Μέσα της Αριζόνας των Η.Π.Α., αφετέρου διότι αποτελεί το ακρωνύμιο του όρου Κινητικότητα για Εφαρμογές Έκτακτης Ανάγκης και Ασφάλειας (Mobility for Emergency and Safety Applications – MESA), που περιγράφει τη στόχευση του έργου. Στο πλαίσιο υλοποίησης και για περίπου μία δεκαετία (έως 2009) έγιναν προσπάθειες να καθοριστεί ένα ενοποιημένο σύνολο απαιτήσεων που θα οδηγούσε σε ένα πρότυπο ευρείας ζώνης επόμενης γενιάς, ώστε να αξιοποιηθεί στη μετάδοση και λήψη δεδομένων φωνής, βίντεο και να παρέχει υψηλές ταχύτητες μετάδοσης σε δίκτυα ευρείας περιοχής που αναπτύσσονται από φορείς δημόσιας ασφάλειας [287], [288], [289]. Μια αποτύπωση της πρόκλησης που είχε ν` αντιμετωπίσει το έργο MESA στον τρισδιάστατο χώρο που προσδιορίζεται από τις μετρικές φάσμα (narrow/wide/broadband), ρυθμός μετάδοσης δεδομένων (bit rate) και κινητικότητα (mobility) προκύπτει σχηματικά στην Εικόνα 104 [290]. Το έργο σημείωσε κάποια πρόοδο και προσπάθησε μέσα από τις υλοποιήσεις να ευαισθητοποιήσει και προσελκύσει φορείς της δημόσιας ασφάλειας τόσο στην Αμερική, όσο και στην Ευρώπη, προτάσσοντας την αναγκαιότητα ικανοποίησης των αναγκών των επαγγελματιών χρηστών που επωμίζονται τη Δημόσια Προστασία Ανακούφιση από Καταστροφές (Public Protection Disaster Relief – PPDR) [291]. Παρόλο που γίνανε κάποια σημαντικά βήματα, το έργο δεν οδήγησε τελικά στην αρχική στόχευση.



Εικόνα 104. MESA Project [290]

5.2.1.2.2 Τάσεις, προοπτικές, μελλοντικές κατευθύνσεις

Τα διάφορα πρότυπα στενής ή ευρείας ζώνης έχουν ωριμάσει και υποστηρίζουν τεχνολογικά δισεκατομμύρια συσκευές τελικών χρηστών και υλικό υποδομής αυτών (σταθμούς βάσης, αναμεταδότες, κέντρα ελέγχου και συντονισμού, κ.λπ.), οι οποίες παρέχουν υπηρεσίες δημόσιας ασφάλειας και κρίσιμων επικοινωνιών ανά τον κόσμο. Αναμφίβολα οι εταιρίες παραγωγής των προϊόντων αυτών θέλουν να διατηρήσουν τα κεκτημένα και ιδανικά να μεγαλώσουν τα κέρδη τους. Προϋπόθεση αποτελεί η αγορά να εξακολουθήσει να ενδιαφέρεται για τα πρότυπα αυτά, ή έστω για τις βελτιώσεις τους. Ως ένδειξη της πορείας, η αγορά, αναφορικά με το TETRA αναμένεται να φτάσει τα 5,1 δισεκατομμύρια δολάρια έως το 2027, σημειώνοντας αύξηση κατά 16,3% του δείκτη CAGR κατά την περίοδο πρόβλεψης (Εικόνα 105) [292]. Κρίσιμης σημασίας ζήτημα αποτελεί εάν οι υπάρχουσες τεχνολογίες (πρωτόκολλα / πρότυπα) θα μπορέσουν να εντάξουν αποδοτικά τις νέες τεχνολογικές εξελίξεις, ώστε να καλύψουν τις αυξημένες πλέον ανάγκες των πελατών. Όποια τεχνολογία δεν καταφέρει να ακολουθήσει τις εξελίξεις και να υλοποιήσει τη συγκεκριμένη πρόκληση, εκτιμάται με υψηλό δείκτη βεβαιότητας ότι θα τείνει διαρκώς σε συρρίκνωση.



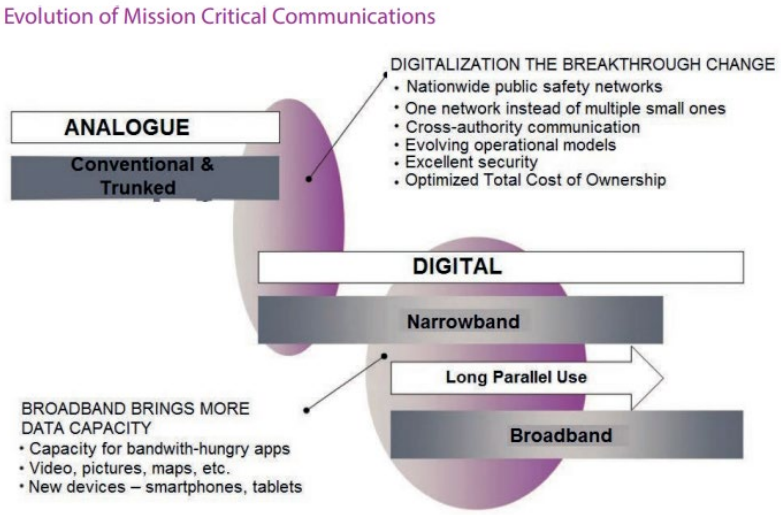
Εικόνα 105. Μέγεθος της αγοράς για το TETRA, το διάστημα 2017-2027 [292]

Μια σειρά από κολοσσούς του χώρου των τηλεπικοινωνιών παράγουν προϊόντα TETRA, P25, DMR, TETRAPOL κ.λπ.. Ενδεικτικά αναφέρονται κάποιες από τις εταιρίες που παίζουν πρωταγωνιστικό ρόλο: Motorola Solutions, Airbus DS, KENWOOD Corporation, Codan Radio, Icom, Hytera / PowerTrunk, Simoco, Harris Corporation, Sepura, Tait Communications, Selex ES S.p.A και Neolink.

5.2.1.3 Πλήρως ευρυζωνικές επικοινωνίες (broadband)

Ο καλύτερος ίσως τρόπος να περιγράψει κάποιος την τεχνολογική εξέλιξη στα δίκτυα δημόσιας ασφάλειας και τις κρίσιμες επικοινωνίες είναι ο εποπτικός. Αυτό παρατηρείται ξεκάθαρα στην Εικόνα 106, από όπου προκύπτει ότι η μετάβαση από τις αναλογικές, στις ψηφιακές επικοινωνίες ήταν μια επανάσταση, όμως η ευρυζωνικότητα αποτελεί πλέον μια αναγκαία εξέλιξη στο πεδίο [46]. Παρά το γεγονός ότι είναι αυταπόδεικτο ότι οι φωνητικές υπηρεσίες αποτελούν τον κορμό των κρίσιμων επικοινωνιών, οι εφαρμογές δεδομένων παρέχουν τεράστιες δυνατότητες στους πρώτους ανταποκριτές, ώστε να έχουν αυξημένη επίγνωση της κατάστασης και άμεση απομακρυσμένη πρόσβαση σε ποικιλία πολύτιμων υπηρεσιών και πληροφοριών, ώστε να λειτουργήσουν πιο γρήγορα και πιο αποτελεσματικά και να σώσουν ζωές.

Αυτή η μετάβαση πραγματοποιείται παράλληλα με τις τεχνολογικές εξελίξεις. Η σταδιακή βελτίωση των νέων τεχνολογικών λύσεων κάθε γενιάς και η δυνατότητα αποδοτικής πλέον ένταξής στους σε εφαρμογές, σηματοδοτεί τη δυνατότητα παραγωγής προϊόντων από τις εταιρίες, ή την υλοποίηση ρεαλιστικών έργων. Στις πλήρως ευρυζωνικές επικοινωνίες εντάσσονται έργα που έχουν υιοθετήσει τεχνολογικές λύσεις του προτύπου LTE και μεταγενέστερα αυτού. Το LTE είναι ένα ευρέως διαδεδομένο παγκόσμιο πρότυπο ευρυζωνικής επικοινωνίας που μπορεί να υποστηρίξει μια μεγάλη ποικιλία σεναρίων ανάπτυξης και αναγκών των χρηστών της δημόσιας ασφάλειας [53]. Αυτό φάνηκε ήδη από τις αρχές της δεκαετίας 2010. Χαρακτηριστικό παράδειγμα αποτελεί η συγκριτική μελέτη των παρεχόμενων υπηρεσιών του TETRA και του LTE που επιχειρήθηκε στο [293], από όπου προκύπτει ότι με σωστή εφαρμογή των δυνατοτήτων του LTE, οι χρήστες δημόσιας ασφάλειας μπορούν να βασίζονται σε αυτό, με τον ίδιο τρόπο που βασίζονται στα πρότυπα στενής ζώνης. Μάλιστα, η ίδια μελέτη καταλήγει ότι είναι ρεαλιστικό το σενάριο της παράλληλης χρήσης των παραδοσιακών συστημάτων PMR που παρέχουν φωνητικές υπηρεσίες και των συστημάτων LTE που εξασφαλίζουν τη μετάδοση πολυμεσικών δεδομένων.



Εικόνα 106. Πορεία από την αναλογική στην ψηφιακή τεχνολογία [46]

Η κατεύθυνση στην οποία τη δεδομένη χρονική στιγμή οδηγείται η τεχνολογία των δικτύων δημόσιας ασφάλειας γίνεται πλήρως αντιληπτή. Η αυλαία της ευρυζωνικότητας ανοίγει με το LTE, για να ακολουθήσουν στη συνέχεια το LTE-Advanced, το 4G και το 5G, που μας απασχολεί την παρούσα χρονική στιγμή και εκτιμάται ότι θα μας απασχολήσει και μελλοντικά. Την πορεία αυτή θα τη δούμε αναλυτικά μέσα από τρία διαφορετικά έργα. Το FirstNet, το BroadMap / BroadWay / BroadNet και το Respond-A. Οι αναφερόμενες δεν είναι οι μοναδικές υλοποιήσεις. Ωστόσο, το FirstNet ως εκπρόσωπος της μετάβασης των δικτύων δημόσιας ασφάλεια στην ευρυζωνική τεχνολογία αποτελεί πλέον μια δοκιμασμένη λύση, που μας προσφέρει τη δυνατότητα να μελετήσουμε τα σημεία υπεροχής του, αλλά και τις τρωτότητες και τα τυχόν προβλήματα. Τα άλλα δύο έργα, αφορούν σε πιλοτικές προσπάθειες χωρών μελών της Ευρωπαϊκής Ένωσης, οικονομικά ενταγμένες στο 7ο Πρόγραμμα – Πλαίσιο (FP7) δραστηριοτήτων έρευνας, τεχνολογικής ανάπτυξης και επίδειξης και ειδικότερα στο HORIZON2020, ένα ευρωπαϊκό πρόγραμμα για την έρευνα και την καινοτομία την περίοδο 2014-2020, με συνολικό προϋπολογισμό περίπου 80 δισ. ευρώ. Τα προγράμματα αυτά βρίσκονται πλέον σε ώριμο στάδιο δοκιμών και προσφέρονται για εξαγωγή χρήσιμων συμπερασμάτων. Τέλος, εντελώς περιληπτικά γίνεται μια αναφορά σε μια σειρά από αξιόλογα προγράμματα και υλοποιήσεις που είτε ολοκληρώθηκαν, είτε εξακολουθούν τη φιλόδοξη πορεία τους και εντάσσονται στην επιχειρούμενη μετάβαση στην ευρυζωνικότητα.

5.2.1.3.1 FirstNet

a. Ιστορικό

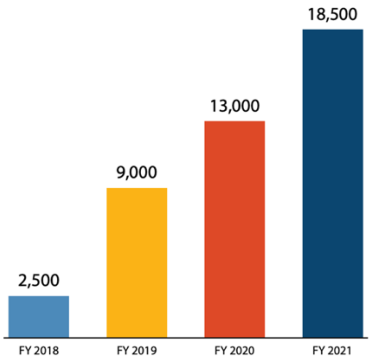
Η ιδέα του FirstNet γεννήθηκε στα χαλάσματα των δίδυμων πύργων, έπειτα από τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001 στο Παγκόσμιο Κέντρο Εμπορίου της Νέας Υόρκης. Η τραγωδία αποκάλυψε θεμελιώδη προβλήματα στα συστήματα επικοινωνιών που χρησιμοποιούσαν οι πρώτοι ανταποκριτές, καθώς δεν ανταποκρίθηκαν στις ακραίες

συνθήκες καταστροφής που κλήθηκαν να αντιμετωπίσουν [294]. Τα κενά στις επικοινωνίες έκτακτης ανάγκης αποτυπώθηκαν σε σχετική έκθεση του 2004 [295] και ταυτόχρονα έγινε ξεκάθαρη η αναγκαιότητα της δημιουργίας ενός αξιόπιστου δικτύου υψηλής ταχύτητας για τους πρώτους ανταποκριτές, που θα καλύπτει το σύνολο της χώρας.

Τότε ξεκίνησε μια μεθοδική δουλειά, με απώτερο στόχο την εξ υπαρχής οργάνωση των υπηρεσιών δημόσιας ασφάλειας σε επίπεδο επικοινωνίας, η οποία ανατέθηκε στην Εθνική Διοίκηση Τηλεπικοινωνιών και Πληροφοριών (National Telecommunications and Information Administration - NTIA[28]) του Υπουργείου Επικοινωνιών των Η.Π.Α., αρμόδια για παροχή συμβουλών σε θέματα πολιτικής τηλεπικοινωνιών και πληροφοριών. Έτσι, το 2012 ιδρύθηκε η Αρχή Δικτύου Πρώτων Ανταποκριτών (First Responder Network Authority - FirstNet Authority), η συνεργασία του οποίου με την εταιρία AT&T έφερε τη δημιουργία ενός ευρυζωνικού δικτύου για τους πρώτους ανταποκριτές των Η.Π.Α., το επονομαζόμενο FirstNet. Αποτελεί την πρώτη παγκοσμίως επιτυχημένη συνεργασία δημοσίου και ιδιωτικού τομέα για τη δημιουργία δικτύου επικοινωνίας δημόσιας ασφάλειας.

Το FirstNet έχει σχεδιαστεί ειδικά για τη δημόσια ασφάλεια και τους πρώτους ανταποκριτές και από την εναρκτήρια πρώτη του έως σήμερα εξελίσσεται διαρκώς, καθώς το FirstNet Authority συνεργάζεται με φορείς και εταιρίες, για να επιτύχει βελτιώσεις, όπου καταγράφονται δυσλειτουργίες ή καθυστερήσεις. Συγκεκριμένα, ανέπτυξε συνεργασία με τα (α)DHS, (β)DoD και (γ) NIST [51]. Μάλιστα, σε συνεργασία με το NIST λαμβάνει διαρκώς ανατροφοδότηση από τους πρώτους ανταποκριτές και εντάσσει στο δίκτυο τις νέες λειτουργικές τους ανάγκες. Μετά την παρέλευση πενταετίας και συγκεκριμένα το 2017 υπογράφηκε 25ετής σύμβαση συνεργασίας μεταξύ της FirstNet Authority και της AT&T [296]. Το δίκτυο κατασκευάστηκε εντός του αρχικού χρονοδιαγράμματος και ήταν έτοιμο και διαθέσιμο για τους πρώτους ανταποκριτές από το 2018. Έκτοτε σημείωσε κατακόρυφη ανάπτυξη - ζήτηση, αφού σε τέσσερα μόλις χρόνια η χρήση του επεκτάθηκε σε 18.500 υπηρεσίες και φορείς (Εικόνα 107), σε 50 πολιτείες των Η.Π.Α., πέντε περιοχές και την περιφέρεια της Κολούμπια, σημειώνοντας αύξηση της τάξης του 86%, έναντι της αρχικής του εμφάνισης [296], ενώ στα τέλη του 2022 αριθμεί ήδη περισσότερα από 4 εκατομμύρια συνδέσεις και εξυπηρετεί πλέον των 23.000 υπηρεσιών [297]. Την 22-8-2022 η FirstNet Authority υπέβαλε στην FCC αίτηση ανανέωσης της άδειας χρήσης του φάσματος Band 14 (758 – 769 / 788 – 799 MHz) [298]. Εν αναμονή της έγκρισης, η συνεργασία αυτή έχει ήδη ορίζοντα επιχειρησιακών εξελίξεων έως το 2027. Παράλληλα, από το 2021 και έπειτα έχει ξεκινήσει η ένταξης της τεχνολογίας του 5G [299].

[28] https://www.ntia.doc.gov

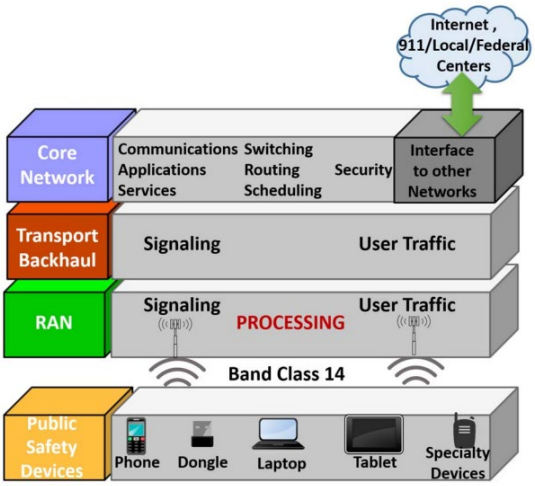


Εικόνα 107. FirstNet, υπηρεσίες εξυπηρέτησης ανά οικονομικό έτος

b. Βασικά στοιχεία αρχιτεκτονικής του FirstNet

Η βασική αρχιτεκτονική του δικτύου FirstNet αποτυπώνεται στην Εικόνα 108 και περιγράφει ουσιαστικά ότι το δίκτυο αυτό βασίστηκε στο πρότυπο LTE [300]. Τα επίπεδα που διαμορφώνουν την αναφερόμενη αρχιτεκτονική είναι:

- Βασικό δίκτυο (core network – CN), αποτελεί το κεντρικό τμήμα του τηλεπικοινωνιακού δικτύου που παρέχει διάφορες υπηρεσίες σε εφαρμογές δημόσιας ασφάλειας μέσω του δικτύου πρόσβασης. Ο πυρήνας διασυνδέεται με άλλα κρατικά, τοπικά και ομοσπονδιακά δίκτυα, συμπεριλαμβανομένου του 911 και του διαδικτύου, λειτουργώντας ως γιγάντια ομπρέλα που καλύπτει το σύνολο της χώρας.
- Οπισθοζέυξη μεταφοράς (transport backhaul), λειτουργεί ως ενδιάμεσο επίπεδο σύνδεσης με το δίκτυο κορμού. Ουσιαστικά αποτελεί το σύνδεσμο που μεταφέρει την κίνηση των χρηστών, όπως φωνή, δεδομένα και βίντεο, και σήματα από σταθμούς βάσης στο κεντρικό δίκτυο.
- Ραδιοδίκτυο πρόσβασης (radio access network – RAN), λειτουργεί και αυτό ως ενδιάμεσο επίπεδο σύνδεσης με το δίκτυο κορμού, αλλά σε ένα επίπεδο χαμηλότερα και εξασφαλίζει τη συνδεσιμότητα με τις συσκευές. Απαιτούνται δεκάδες χιλιάδες σταθμοί βάσης για να καλυφθεί τουλάχιστον το 99% του πληθυσμού, όμως και πάλι δεν είναι αρκετό, καθώς η δημόσια ασφάλεια δεν στοχεύει μόνο σε περιοχές πληθυσμιακής συγκέντρωσης, αλλά και σε απομακρυσμένες. Η FirstNet συνεργάστηκε με κάθε πολιτεία για να κατανοηθούν οι ανάγκες μιας εκάστης εξ αυτών και δημιούργησε ένα σχέδιο για κάθε πολιτεία και επικράτεια που ανταποκρίνεται καλύτερα σε αυτές τις ανάγκες.
- Συσκευές δημόσιας ασφάλειας (public safety devices – PSD), όπως έξυπνα κινητά τηλέφωνα, φορητοί υπολογιστές, tablet, ειδικές συσκευές, ή μικροσυσκευές με δυνατότητα ασύρματης σύνδεσης σε ευρυζωνικό δίκτυο που βασίζεται στο πρότυπο LTE. Ένας πλήρως επικαιροποιημένος κατάλογος των συσκευών που υποστηρίζουν το δίκτυο FirstNet βρίσκεται στο [301]. Βέβαια, στο συγκεκριμένο επίπεδο της αρχιτεκτονικής εντάσσονται και οι διαθέσιμες εφαρμογές.



Εικόνα 108. Αρχιτεκτονική LTE για το FirstNet [148]

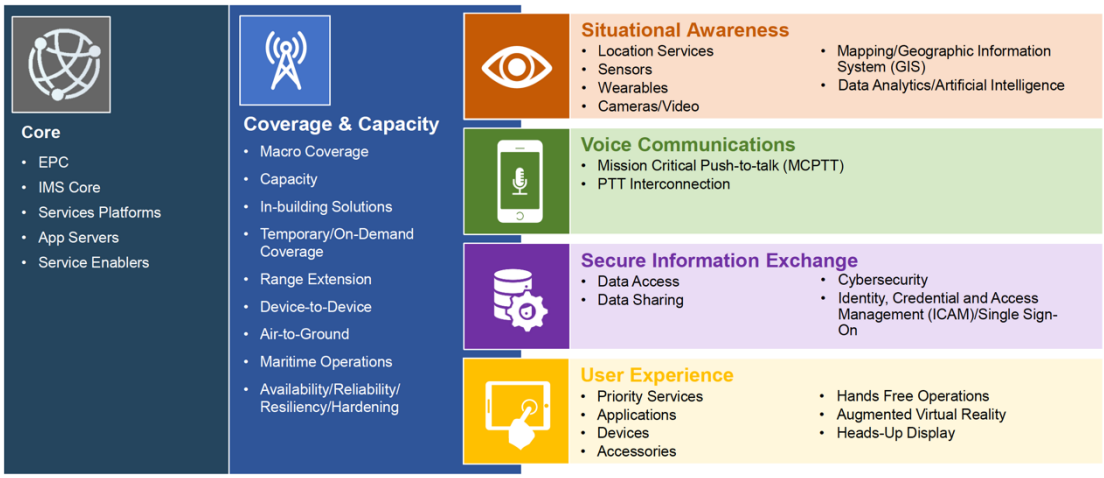
Στα κύρια χαρακτηριστικά το FirstNet δικτύου περιλαμβάνονται [302]:

- Λειτουργία άμεσης επικοινωνίας
- Ομιλία με το πάτημα πλήκτρου (Push-to-talk - PTT)
- Πλήρως διπλής κατεύθυνσης επικοινωνία (Full duplex)
- Ομαδικές κλήσεις
- Αναγνώριση καλούντος
- Κλήσεις έκτακτης ανάγκης
- Ροή δεδομένων μεγάλου όγκου μεταξύ του Κέντρου Επιχειρήσεων Έκτακτης Ανάγκης και του πεδίου
- Βελτιωμένη παρακολούθηση οχημάτων, εξοπλισμού, προσωπικού, κ.λπ.
- Δυνατότητα παρακολούθησης της κατάστασης του δικτύου σε σχεδόν πραγματικό χρόνο, συμπεριλαμβανομένων ειδοποιήσεων και λεπτομερούς προβολής της κάλυψης σε περιοχές όπου ανταποκρίνονται ενεργά ή αναπτύσσονται
- Λειτουργίες προτεραιότητας δικτύου στο πλαίσιο της συνεργασίας συνόλου εμπλεκομένων με τους πρώτους ανταποκριτές κατά τη διάρκεια μιας εκδήλωσης
- Κατάλογος ελεγμένων, ασφαλών εφαρμογών δημόσιας ασφάλειας και διαχείρισης έκτακτης ανάγκης. Ένας πλήρης κατάλογος των διαθέσιμων εφαρμογών βρίσκεται στο [303]. Επιπλέον, αξίζει να επισημανθεί ότι στους χρήστες της σουίτας FirstNet παρέχονται δύο επίπεδα: Επαλήθευσης (FirstNet Verified) και Πιστοποίησης (FirstNet Certified). Η FirstNet Verified σημαίνει ότι η εφαρμογή πληροί κριτήρια συνάφειας με τη δημόσια ασφάλεια και έχει υποβληθεί σε διαδικασία ελέγχου που περιλαμβάνει την ασφάλεια, το απόρρητο δεδομένων και τη διαθεσιμότητα (99,9% διαθέσιμο) που απαιτούνται για συμπερίληψη στον κατάλογο εφαρμογών FirstNet, ενώ η FirstNet Certified σημαίνει ότι η εφαρμογή πληροί τα κριτήρια συνάφειας, ασφάλειας και απορρήτου δεδομένων, αλλά έχει επίσης αυξημένη διαθεσιμότητα

(99,99% διαθέσιμο), κινητικότητα, ανθεκτικότητα και επεκτασιμότητα για την κάλυψη των απαιτήσεων δημόσιας ασφάλειας. Ο πηγαίος κώδικας για την εφαρμογή πρέπει να περάσει από μια ξεχωριστή διαδικασία ελέγχου ασφαλείας [304]

- Περισσότεροι από 150 αναπτυσσόμενα στοιχεία δικτύου (οχήματα, drones, επιχειρησιακά κέντρα, κ.λπ.) διαθέσιμα χωρίς κόστος για τους συνδρομητές του FirstNet, για το είδος των οποίων θα γίνει εκτενής αναφορά στη συνέχεια
- Ενοποίηση με δίκτυα LMR
- Κοινή πλατφόρμα επικοινωνίας στο πλαίσιο υλοποίησης της Συμφωνίας Διαχείρισης Βοήθειας Έκτακτης Ανάγκης (Emergency Management Assistance Compact – EMAC)

Η AT&T στο πλαίσιο της συμφωνίας με την κρατική FirstNet Authority δεσμεύτηκε να κατασκευάσει, λειτουργήσει, παραδώσει, συντηρεί και ενισχύει για 25 χρόνια ένα ευρυζωνικό δίκτυο δημόσιας ασφάλειας (Public Safety Broadband Network - PSBN) [296]. Το σύνολο των λειτουργικών απαιτήσεων πρέπει να έχει παραδοθεί έως τον Μάρτιο του 2023 [305]. Παράλληλα, οι βασικοί τομείς του οδικού χάρτη μέχρι την τελική παράδοση φαίνονται στην Εικόνα 109.



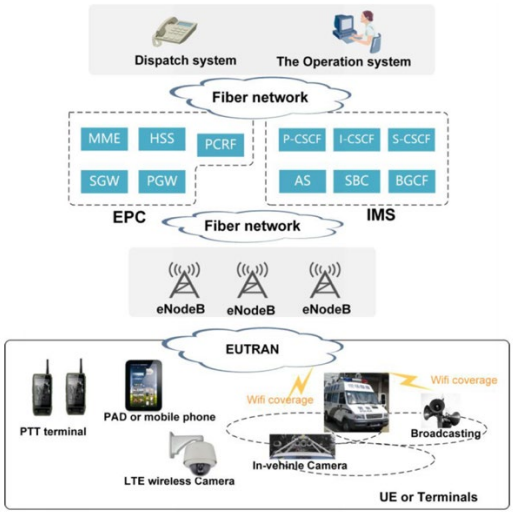
Εικόνα 109. Βασικοί τομείς του δικτύου FirstNet

Οι πυλώνες του οδικού χάρτη αφορούν:

- Τον πυρήνα, που περιλαμβάνει το EPC το οποίο μπορεί να αυξήσει τη χωρητικότητα και την ταχύτητα και αναφέρεται σε μια βασική αρχιτεκτονική δικτύου του LTE. Επιπλέον, περιλαμβάνει το Υποσύστημα Πολυμέσων (IP Multimedia Subsystem), IMS που αποτελεί μια υποδομή δικτύου κινητής τηλεφωνίας, για την παροχή υπηρεσιών επικοινωνίας σε πραγματικό χρόνο (φωνή, βίντεο, δεδομένα κ.λπ.) τόσο για τους καταναλωτές όσο και για τους επαγγελματίες χρήστες μέσω οποιουδήποτε δικτύου πρόσβασης, ειδικά του VoLTE, κλήσεις Wi-Fi και VoNR. Ο τρόπος που τα

δύο βασικά στοιχεία του πυρήνα παρέχουν βελτιωμένες υπηρεσίες επικοινωνίας περιγράφεται αναλυτικά στα [306], [307] και προκύπτει εποπτικά στην Εικόνα 110.

- Την κάλυψη και χωρητικότητα, που περιλαμβάνει τη χωρητικότητα, την κάλυψη, την επικοινωνία D2D, την επικοινωνία αέρα – εδάφους, τη διαθεσιμότητα, αξιοπιστία, ανθεκτικότητα και αντοχή
- Την επίγνωση της κατάστασης, που περιλαμβάνει υπηρεσίες τοποθεσίας, αισθητήρες, φορητές συσκευές, κάμερες, πληροφορίες γεω-προσδιορισμού και τεχνητή νοημοσύνη
- Τις φωνητικές υπηρεσίες, που περιλαμβάνει MCPTT
- Την ασφαλή ανταλλαγή πληροφοριών, που περιλαμβάνει κυβερνοασφάλεια, πιστοποιημένη πρόσβαση σε δεδομένα
- Εμπειρία χρήστη, που περιλαμβάνει υπηρεσίες προτεραιότητας, εφαρμογές, συσκευές, αξεσουάρ, λειτουργίες hands-free, επαυξημένη και εικονική πραγματικότητα και heads-up display



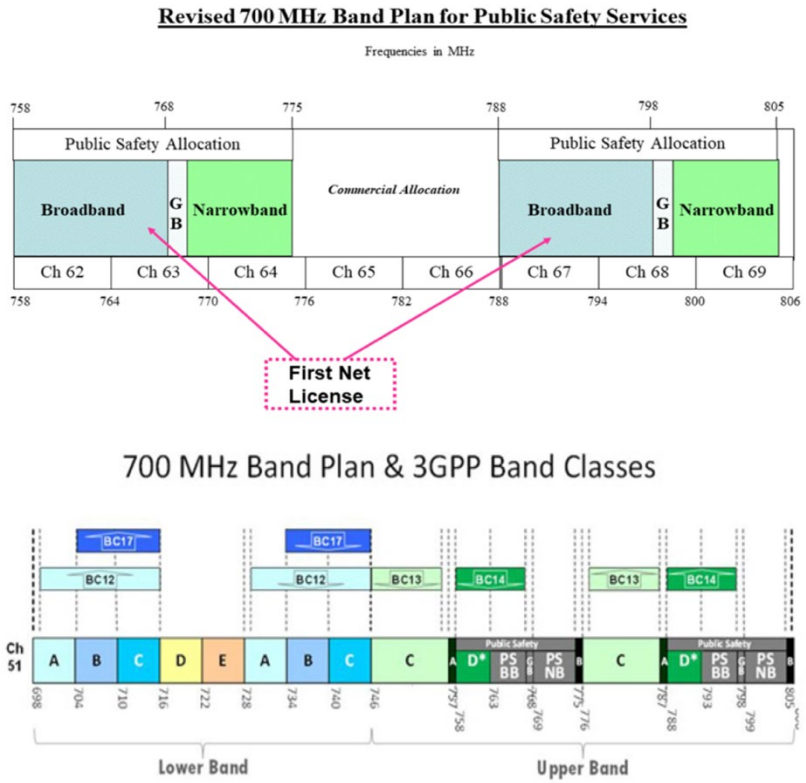
Εικόνα 110.Λύσεις ιδιωτικού δικτυου (PNS) [306]

c. Βασικά τεχνικά χαρακτηριστικά του FirstNet

Το κύριο ζήτημα που καθορίσθηκε εξ αρχής για τη λειτουργία του FirstNet ήταν η εκχώρηση άδειας χρήσης αποκλειστικού φάσματος για τις ανάγκες της δημόσιας ασφάλειας. Την 22-2-2012 με απόφαση του Κογκρέσο των ΗΠΑ διατέθηκε το D-Block (758-763 MHz / 788-793 MHz) στη δημόσια ασφάλεια για χρήση σε εθνικό ευρυζωνικό δίκτυο (Εικόνα 111) [308], [148].

Band class	Spectrum block	Uplink (MHz)	Downlink (MHz)	Band gap (MHz)
12	Lower block A Lower block B Lower block C	698 - 716	728 - 746	12
13	Upper C block	777 - 787	746 - 756	41
14	Upper D Block and Public safety allocation	788 - 798	758 - 768	40
17	Lower B block Lower C block	704 - 716	734 - 746	18

Πίνακας 22. Κατανομή φάσματος των 700 MHZ: Ζώνες 12, 13, 14, και 17 [148]



Εικόνα 111. Αδειοδοτημένη ζώνη φάσματος του FirstNet [308]

Τι έχουν στη διάθεσή τους οι χρήστες του FirstNet; Από τον Μάρτιο του 2022 οι χρήστες FirstNet έχουν στη διάθεσή τους περισσότερα από 150 αναπτυσσόμενα στοιχεία δικτύου που είναι τοποθετημένα σε στρατηγικά σημεία σε όλο το εύρος κάλυψης και συνεχώς διαθέσιμα στους συνδρομητές (24/7/365) [309].

Τα χαρ ακτηριστικότερα εξ αυτών είναι:

- Δορυφορικές κυψέλες σε ελαφρά φορτηγά (Satellite Cells on Light Trucks - SatCOLT), είναι επίγειες δορυφορικές κυψέλες σε ελαφριά φορτηγά, που συνδέονται μέσω δορυφόρου και δεν βασίζονται σε εμπορική παροχή ρεύματος (Εικόνα 113.b)
- Συμπαγείς συσκευές γρήγορης ανάπτυξης (Compact Rapid Deployables - CRD), είναι μικρές φορητές κυψέλες που μπορούν να αναπτυχθούν γρήγορα για να παρέχουν κάλυψη σε τοποθεσίες όπου δεν μπορούν να πάνε μεγαλύτερα οχήματα (τα

διαθέσιμα SatCOLTS μαζί με τα CRD είναι περισσότερα από 100). Την ανάτυξη αυτών μπορεί να αναλάβει και μόνο ένας άνθρωπος. Είναι αλλιώς γνωστά ως κελιά σε ρόδες (Cell on Wheels - COW) και παρέχουν εμβέλεια κάλυψης κινητής τηλεφωνίας έως 2 μίλια, δορυφορικό δίκτυο υψηλής ταχύτητας και γεννήτρια που υποστηρίζει τις ανάγκες ενέργειας για τουλάχιστον 60 ώρες [310] (Εικόνα 112)

- Υπτάμενα COW (Flying COW), το οποίο αποτελείται από δύο drone δεμένα σε τρέιλερ, που μπορούν να φτάσουν έως και 400 πόδια σε ύψος, να αντέξουν την ελαφριά βροχή και άνεμο ταχύτητα έως και 25 μίλια. Υπάρχουν τρία διαθέσιμα και θεωρούνται ιδανικά για πυρκαγιές ή αποστολές διάσωσης στο βουνό όπου το έδαφος μπορεί να κάνει τη προσβασιμότητα πρόκληση. Είναι ιδιαιτέρως ανθεκτικά για ακραία περιβάλλοντα και μπορούν να «βλέπουν» μέσα από καπνό, κορυφές δέντρων και άλλα εμπόδια [311] (Εικόνα 113.a).
- FirstNet One, ένα αερόστατο 55 ποδιών, ιδανικό για χρήση μετά από μεγάλες καταστροφές. όπως τα επακόλουθα ενός τυφώνα, όπου απαιτείται συνεχής συνδεσιμότητα για απόκριση και ανάκαμψη. Παρέχει μεγάλο αποτύπωμα κάλυψης και μπορεί να παραμείνει στον αέρα για περίπου 2 εβδομάδες και να πετάξει έως και 1.000 πόδια (Εικόνα 113.c)
- Οχήματα Επικοινωνίας. Υπάρχουν τρία τέτοια διαθέσιμα και αφορούν σε οχήματα διοίκησης και επικοινωνιών για επείγουσες περιπτώσεις που απαιτείται άμεση ανάπτυξη, για την κάλυψη εκδηλώσεων και εκπαιδευτικών ασκήσεων. Εντός των οχημάτων αυτών υπάρχει χώρος για δύο άτομα, πολλαπλές οθόνες, τηλεοράσεις και σταθμοί φόρτισης, καθώς και μεγάλη εξωτερική οθόνη και ηχεία για ενημερώσεις. Παρέχει συνδεσιμότητα μέσω LTE (Band 14) και Wi-Fi και είναι σε θέση να αξιοποιήσει μια ποικιλία επιλογών backhaul. Κάθε ένα εξ αυτών είναι εξοπλισμένο με γεννήτρια που μπορεί να λειτουργήσει για πολλές ημέρες πριν τον ανεφοδιασμό και περιλαμβάνει τουαλέτα, φούρνο μικροκυμάτων, μίνι ψυγείο και κουκέτα ύπνου. Παρέχεται η δυνατότητα αξιοποίησης της υπηρεσίας FirstNet Central για τη διαχείριση λογαριασμών χρηστών και συσκευών, επιπέδων προτεραιότητας χρηστών και χρηστών PTT.

Εικόνα 112. Compact Rapid Deployable (CRD) / Cell on Wheels (COW) -FirstNet

Εικόνα 113. (a) Flying COW, (b) SatCOLT, (c) FirstNet One

Σύμφωνα με την κατηγοριοποίηση των διαθέσιμων αναπτυσσόμενων στοιχείων δικτύου της FirstNet που επιχειρείται στο [148], αυτά κατατάσσονται σε πέντε (5) κατηγορίες:

- σύστημα δικτύου οχημάτων (vehicle network system -VNS),
- κελιά σε ελαφριά φορτηγά (cells on light trucks -COLTS),
- κελιά σε τροχούς (COW),
- συστήματα σε τροχούς (system on wheels - SOW),
- αναπτυσσόμενη αρχιτεκτονική εναέριων επικοινωνιών (deployable aerial communications architecture - DACA)

Τα χαρακτηριστικά αυτών αποτυπώθηκαν στον Πίνακας 23, όπου παρατίθενται συγκριτικά στοιχεία αναφορικά με την παρεχόμενη χωρητικότητα και κάλυψη, τις ενεργειακές απαιτήσεις, τη λειτουργική αυτονομία, τη διαθεσιμότητα και τα ζητήματα της ανάπτυξής τους (χρόνος, είδος οχήματος, ποσότητα).

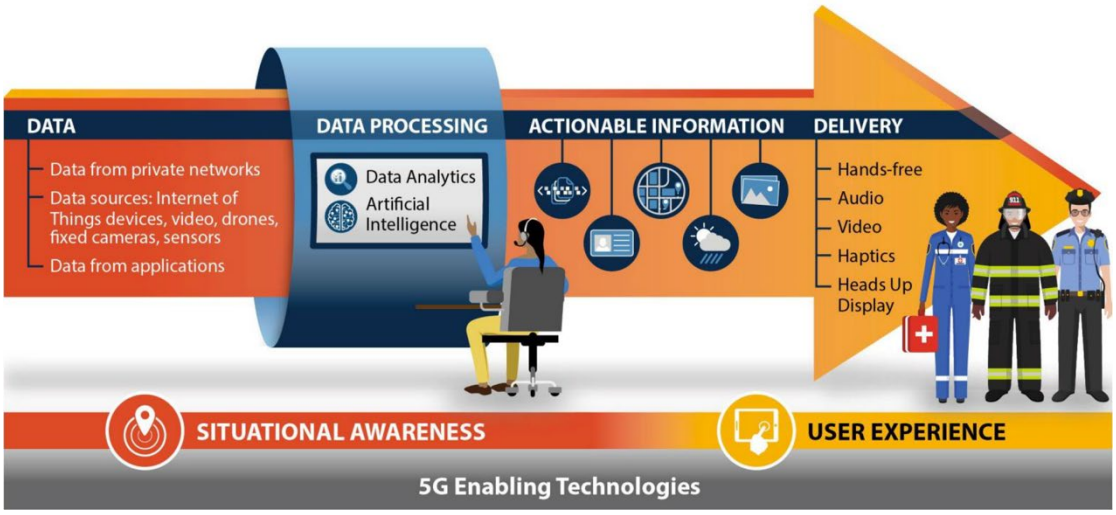
Characteristics	VNS	COLTS	COW	SOW	DACA
Capacity	Low/medium	Medium	High	High	Low/medium
Coverage	Small cells such as pico and femto	Cell size can be either macro, or micro, or pico, or femto	Cell size can be either macro, or micro, or pico, or femto	Cell size can be either macro, or micro, or pico, or femto	Small cells such as pico and femto
Band class 14 radio	Yes	Yes	Yes	Yes	Yes
Standalone	Yes	No	No	Yes	No
Availability	Immediate	Vehicular drive time	Vehicular drive time	Vehicular drive time and system deployment time	Aerial launch time
Power	Limited to vehicle battery	Generator	Generator	Generator	Limited to the airframe
Deployment time	Zero to low	Low	Medium	Long	Long
Deployment nature	EFR vehicles	Dedicated Trunks	Dedicated Trailers	Dedicated Trucks with Trailer	Aerial such as UAVs and balloons
Deployment quantity	Thousands	Hundreds	Hundreds	Dozens	Dozens (based on experimentations and simulations)
Incident duration	Low	Medium	Medium	Long	Long

Πίνακας 23. Είδη αναπτυσσόμενων στοιχείων του δικτύου FirstNet

Όπως προαναφέρθηκε, τον Απρίλιο του 2021 έγινε αναβάθμιση του αποκλειστικού πυρήνα δικτύου FirstNet, για να επιτραπεί η αξιόπιστη συνδεσιμότητα 5G [312]. Ωστόσο, η μετάβαση αυτή θα πρέπει να συντελεστεί με αργά και σταθερά βήματα, καθώς όταν οι επαγγελματίες της δημόσιας ασφάλειας καλούνται να ανταποκριθούν στο πεδίο, δεν υπάρχουν περιθώρια εκπτώσεων για την αξιοπιστία, καθώς κρίνονται ανθρώπινες ζωές. Συνεπώς είναι αναμενόμενη οι ρυθμοί εξέλιξης και ένταξης του 5G στις εφαρμογές της δημόσιας ασφάλειας να υστερούν σε σχέση με τα εμπορικά δίκτυα. Σύμφωνα με τη στόχευση της AT&T, που υλοποιεί το τεχνικό μέρος του FirstNet, η μετάβαση θα βασιστεί στην υπάρχουσα γνώση από το LTE και το 4G [299]. Από το ίδιο άρθρο και όσα αναφέρει ο αντιπρόεδρος της AT&T, προκύπτει ότι την παρούσα χρονική στιγμή οι χρήστες του FirstNet έχουν δυνατότητα χρήσης τριών διαφορετικών λειτουργικών φασματικών επιπέδων του 5G:

- Υψηλή ζώνη (High-Band 5G+: mmWave στη ζώνη των 36GHz [313]): Οι φορείς και οι οργανισμοί δημόσιας ασφάλειας σε περισσότερες από 45 πόλεις και περιοχές αυτών λαμβάνουν εξαιρετικά γρήγορες ταχύτητες και πρωτόγνωρες επιδόσεις σε περιοχές υψηλής κυκλοφορίας. Χαρακτηριστικά παραδείγματα αποτελούν το Διεθνές Αεροδρόμιο του Λος Άντζελες και το στάδιο Raymond James στην Τάμπα, όπου πραγματοποιούνται συναυλίες ή μεγάλα αθλητικά γεγονότα.
- Μεσαία ζώνη (Mid-Band 5G+:στη ζώνη των 3,45 – 3,7GHz [314]): Οι φορείς και οι οργανισμοί δημόσιας ασφάλειας σε περισσότερες από 40 πόλεις και περιοχές αυτών λαμβάνουν φάσμα 5G+ μεσαίας ζώνης που παρέχει έναν συνδυασμό εξαιρετικά γρήγορων ταχυτήτων και ευρείας γεωγραφικής κάλυψης.
- Χαμηλή ζώνη (Low-Band 5G: 850MHz [313], [314]): Οι φορείς και οι οργανισμοί δημόσιας ασφάλειας σε περισσότερες από 30 πόλεις και περιοχές αυτών μπορούν να συνδεθούν χρησιμοποιώντας φάσμα 5G χαμηλής ζώνης, το οποίο καλύπτει μεγάλες περιοχές και να διεισδύσει σε κτίρια και υποδομές καλύτερα από το 5G+ υψηλής ζώνης.

Σε κάθε περίπτωση, τα οφέλη από τη σταδιακή αυτή μετάβαση σε τεχνολογικές λύσεις 5G για το FirstNet αναπαρίσταται στην Εικόνα 114. Οι τεχνολογίες 5G θα βελτιώσουν σημαντικά την επίγνωση της κατάστασης, καθώς εμπλέκονται ενεργά πολλές νέες εφαρμογές στο πεδίο, συσκευές που υποστηρίζουν αυτές, αλλά και το σύνολο των τεχνολογιών του IoT. Περαιτέρω δε, η συλλογή και επεξεργασία των δεδομένων είναι σημαντικά βελτιωμένη και με τη συμβολή της τεχνητής νοημοσύνης σ‘ αυτό, με απώτερο σκοπό το σύνολο των υπηρεσιών που παρέχονται στους χρήστες, που στην περίπτωσή μας είναι οι πρώτοι ανταποκριτές, να είναι ακριβείς, στο σωστό χρόνο, με τον πιο φιλικό τρόπο και τον ευκολότερο στη διαχείριση, έχοντας πάντοτε υπόψη μας ότι την ίδια ώρα ενεργεί στο πεδίο [10].



Εικόνα 114. Τεχνολογίες ενεργοποίησης 5G για το FirstNet [10]

d. Πλεονεκτήματα και μειονεκτήματα του FirstNet

Τα πλεονεκτήματα της επιχειρησιακής λειτουργίας του FirstNet φάνηκαν από την πρώτη στιγμή και συνοψίζονται στ‘ ακόλουθα [315], [316]:

- Βελτιωμένη επικοινωνία μέσω διαλειτουργικού δικτύου
- Σύνδεση των ανταποκριτών ακόμη και με απομακρυσμένες περιοχές
- Ενίσχυση της επίγνωσης της κατάστασης σε περιπτώσεις έκτακτης ανάγκης
- Ουσιαστική προτεραιότητα στη δημόσια ασφάλεια
- Επαρκής χωρητικότητα για προγραμματισμένες πολυπληθείς εκδηλώσεις
- Παροχή ενεργών δεδομένων μέσω καινοτόμων εφαρμογών και συσκευών
- Παροχή αξιοπιστίας και ασφάλειας όταν λαμβάνουν χώρα καταστροφές
- Συντονισμένη απόκριση σε ανθρωπογενείς καταστροφές
- Αποδοτική αξιοποίηση της τεχνολογία στις επικοινωνίες δημόσιας ασφάλειας

Μερικά μειονεκτήματα του δικτύου FirstNet είναι [317]:

- Απώλεια πολιτειακής αυτονομίας και κατ‘ επέκταση κρατικής, καθώς για να καταστεί οικονομικά βιώσιμο απαίτησε την παραχώρηση της εκμετάλλευσης φάσματος σε ιδιωτική εταιρεία τηλεπικοινωνιών (AT&T), υπό τον έλεγχο και συνεργασία κρατικού φορέα (FirstNet Authority).
- Υφίσταται προβληματισμός σχετικά με το επίπεδο συνεργασίας του ιδιώτη (AT&T) και του κρατικού αντιπροσώπου, αναφορικά με τη δυνατότητα εισχώρησης στην αγορά από άλλες εταιρίες, τόσο σε τοπικό επίπεδο, όσο και σε ευρύτερο [297].
- Απώλεια ελέγχου και διαπραγματευτικής δύναμης των κρατών και κυβερνητικών εκπροσώπων στο ζήτημα του δικτύου δημόσιας ασφάλειας
- Κίνδυνος μονοπωλίου, αλλά και ζητήματα που περιλαμβάνουν λειτουργικούς κινδύνους και ασφάλεια

e. Περιπτώσεις χρήσης του FirstNet

Η σουίτα FirstNet αξιοποιήθηκε πολλές φορές έως σήμερα. Ενδεικτικά μόνο παρατίθενται περιπτώσεις χρήστης της [296]:

i. Πυρκαγιά στην κομητεία Μπόλντερ του Κολοράντο το 2021

Η πυρκαγιά επεκτάθηκε σε περισσότερα από 6.000 στρέμματα πυκνοκατοικημένης έκτασης. Πυροσβέστες από την ίδια την πολιτεία και γειτονικές ανταποκρίθηκαν δυναμικά για ν` αντιμετωπίσουν τη φωτιά, η οποία είχε ως σύμμαχο ανέμους με ταχύτητες τυφώνα κατηγορίας 2. Οι ανταποκριτές που χρησιμοποίησαν το FirstNet εκτός από την πυρκαγιά είχαν να αντιμετωπίσουν και τις εκτεταμένες ζημίες στην τοπική υποδομή οπτικών ινών, αλλά κατάφεραν να συνδεθούν στο δίκτυο και να παρέχουν τις υπηρεσίες τους χάρη στην

ταχύτητα ανάπτυξη πολλών SatCOLT, ενώ το όλο εγχείρημα υποστήριξε διοικητικά ένα κέντρο επικοινωνίας και CRD [304], [318].

ii. Green International Airport (επιχειρησιακή άσκηση)

Τον χειμώνα του 2020, η Υπηρεσία Διαχείρισης Έκτακτης Ανάγκης της πολιτείας του Ρόουντ Άιλαντ δοκίμασε τις δυνατότητες του δικτύου FirstNet κατά τη διάρκεια μιας προσομοίωσης αεροπορικού ατυχήματος με μαζικές απώλειες. Σύμφωνα με το σενάριο, οι εκπρόσωποι δημόσιας ασφάλειας και δημόσιας υγείας έπρεπε να είναι σε θέση να επικοινωνούν σε μεγάλη απόσταση, ήτοι από τη σκηνή της άσκησης μέχρι το κέντρο επικοινωνίας έκτακτης ανάγκης. Αντί να χρησιμοποιούν συσκευές LMR, στράφηκαν σε ευρυζωνικές επικοινωνίες για να διευκολύνουν τη μεταφορά σύνθετων μηνυμάτων σε εκτεταμένες αποστάσεις και την προβολή δεδομένων σε πραγματικό χρόνο [319].

iii. Πολιτεία της Ιντιάνα

Για να καλυφθούν οι επικοινωνιακές ανάγκες των ανταποκριτών εντός και πλησίον των κέντρων εμβολιασμού κατά της Covid-19, η Υπηρεσία Εκτάκτων Αναγκών της πολιτείας κατέφυγαν στη λύση του FirstNet. Ένα SatCOLT βελτιστοποίησε την κάλυψη εντός της επίμαχης περιοχής. Ο Διευθυντής της Υπηρεσίας δήλωσε: «*Όποτε έχετε τόσους πολλούς ανθρώπους σε μια περιοχή, η FirstNet είναι πραγματικά η μόνη υπηρεσία που μπορεί να προσφέρει στη δημόσια ασφάλεια*» [304].

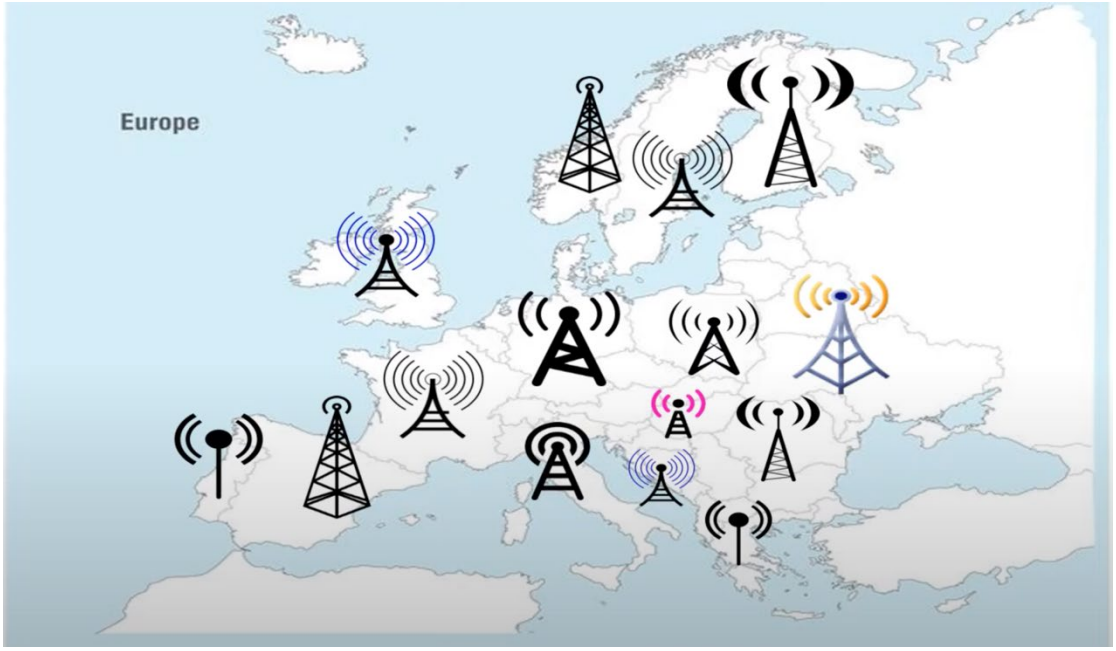
iv. Η πόλη Πάρμα της πολιτείας του Κλίβελαντ

Με πληθυσμό περίπου 80.000 κατοίκων σε μόλις 20 τετραγωνικά μίλια, ήταν πρωτοπόρος όταν το 1989 εγκατέστησε σύστημα επικοινωνιών για τις υπηρεσίες δημόσιας ασφάλειας, το Βελτιωμένο Σύστημα Επικοινωνιών Ψηφιακής Πρόσβασης (Enhanced Digital Access Communications System - EDACS) που ήταν ένα σύστημα LMR. Το 2018 ανέθεσε στις εταιρίες L3Harris and Cleveland Communications τον εκσυγχρονισμό του συστήματος και τη μετάβαση σε ευρυζωνικές επικοινωνίες. Αποτέλεσμα αυτού ήταν η συμφωνία των αρχών της πόλης με την FirstNet [320].

5.2.1.3.2 BroadWay, Respond-A

a. BroadMap / BroadWay / BroadNet

Η ιδέα του συγκεκριμένου ευρωπαϊκού έργου γεννήθηκε από την προβληματική ετερογένεια του χάρτη της Εικόνας 115 [321] και τις δυσκολίες που αυτή δημιουργεί στην ομαλή και ακώλυτη επικοινωνία των επαγγελματιών της δημόσιας ασφάλειας εντός των συνόρων της Ευρώπης.



Εικόνα 115. BroadMap [321]

Είναι σαφές ότι το ζήτημα δεν είναι να φτάσουμε στη δημιουργία ενός δικτύου για το σύνολο της Ένωσης, καθώς κάτι τέτοιο δεν θα ήταν ρεαλιστικό. Το κρίσιμο όμως είναι να υπάρχει η απαιτούμενη διαλειτουργικότητα μεταξύ των υφιστάμενων κρατικών ευρυζωνικών δικτύων που είναι ικανή να εξασφαλίσει την επιχειρησιακή συνέχεια, ανεξαρτήτως συνόρων. Υπό την εποπτεία και καθοδήγηση του PSCE και στο πλαίσιο του προγράμματος HORIZON2020, εκδηλώθηκε αρχικά μια πρωτοβουλία, η οποία μετουσιώθηκε σε πρόγραμμα, που περιλαμβάνει τρεις διακριτές φάσεις [322]:

- Το *BroadMap*, διάρκειας ενός έτους (από 1/5/2016 έως 30-4-2017), εντάσσεται στο στάδιο της προετοιμασίας. Αρχικά εκδηλώθηκε ενδιαφέρον από 11 χώρες της Ευρωπαϊκής Ένωσης, ανάμεσα στις οποίες και η χώρα μας, με εκπροσώπους υπουργεία, οργανισμούς, φορείς ή υπηρεσίες που είναι υπεύθυνοι ή καθ‘ οιονδήποτε τρόπο ασχολούνται με τη δημόσια ασφάλεια. Οι δράσεις που αναπτύχθηκαν είχαν ως στόχο:
  - ❖ Τη συλλογή, αξιολόγηση και επικύρωση των απαιτήσεων ασύρματης ευρυζωνικής επικοινωνίας των επαγγελματιών δημόσιας ασφάλειας
  - ❖ Τη δημιουργία ενός βασικού συνόλου προδιαγραφών για την εκπλήρωση των απαιτήσεων
  - ❖ Τον καθορισμό μεταβατικού χάρτη της πορείας για την έρευνα και τυποποίηση για τη μελλοντική εξέλιξη των ευρωπαϊκών λύσεων
  - ❖ Την προετοιμασία του εδάφους για ένα νέο οικοσύστημα που θα εισάγει νέες εφαρμογές, υπηρεσίες και διαδικασίες χρησιμοποιώντας ευρυζωνικές δυνατότητες για τη δημόσια ασφάλεια

- ❖ Την αξιοποίηση της δύναμης της κοινότητας των επαγγελματιών δημόσιας ασφάλειας της τεχνογνωσίας και των σχέσεών τους, με στόχο την επίτευξη διαλειτουργικότητας σε όλη την Ευρώπη. Αφορά σε ένα ενδιαφέρον μίγμα πολιτισμικών, πολιτιστικών και γεωγραφικών διαφορών, που λειτουργούν εντός διαφορετικών νομικών πλαισίων.

Το πέρας του έργου ακολούθησε μια μεταβατική περίοδος, απαιτούμενη για την προετοιμασία της ομαλής μετάβασης στο δεύτερο σκέλος, το BroadWay (8ος 2017 – 1ος 2018, που αναλώθηκε στο σχεδιασμό της υποβληθείσας πρότασης για την έγκριση του έργου.

- Το *BroadWay*, διάρκειας τριών ετών (από 1/5/2018 έως 30/4/2021), είχε ως στόχο να υλοποιήσει τα πρώτα συντονισμένα ευρωπαϊκά βήματα προς τη μελλοντική προμήθεια επόμενης γενιάς ευρυζωνικών συστημάτων ραδιοεπικοινωνίας για τη βελτίωση των υπηρεσιών δημόσιας ασφάλειας στους πολίτες της Ευρώπης και την ενίσχυση της διασυνοριακής διαλειτουργικότητας. Μάλιστα, στο πλαίσιο του έργου υλοποιήθηκε μια εμπορική προμήθεια (Pre-Commercial Procurement), που είχε ως σκοπό καινοτόμες λύσεις για την υλοποίηση της αρχιτεκτονικής «SpiceNet Reference» όπως είχε ορισθεί με το έργο BroadMap. Συγκεκριμένα, ένα πανευρωπαϊκό πιλοτικό σύστημα αναπτύχθηκε εντός του 2021, επικυρωμένο από δοκιμές, ώστε να αποδειχθούν οι βιώσιμες δυνατότητές του προς ικανοποίηση μιας πανευρωπαϊκής ομάδας επαγγελματιών δημόσιας ασφάλειας. Το έργο υποστηρίζεται συνολικά από 23 ευρωπαϊκές χώρες, από 49 οργανώσεις επαγγελματιών και περίπου από 1,4 εκατομμύρια επαγγελματίες της δημόσιας ασφάλειας. Στα τρία αυτά χρόνια έγιναν σημαντικότατα βήματα και ειδικότερα ολοκληρώθηκε η επίσημη διαδικασία δημοσίων συμβάσεων μέσα από τις ακόλουθες φάσεις:

  Φάση 1. Τέσσερις εταιρίες (4 Designs) υπέγραψαν σύμβαση για την παροχή σχεδίων που παρέχουν λύση. Συγκεκριμένα η Airbus Defence and Space [323], η Frequentis [324], η Leonardo [325] και η Rohill Technologies [326]. Η φάση αυτή διήρκησε μέχρι τον Μάρτιο του 2020.

  Φάση 2. Τρεις από τις τέσσερις εταιρίες που αρχικά κατέθεσαν προτάσεις, προκρίθηκαν στη φάση αυτή και συγκεκριμένα οι Airbus DS, Frequentis AG και Leonardo S.p.A. (3Prototypes). Η φάση αυτή διήρκησε μέχρι τον Ιούνιο του 2021.

  Φάση 3. Οι δύο πρώτες σε σειρά κατάταξης εταιρίες και συγκεκριμένα οι Airbus DS και Frequentis AG (2 Pilots) προκρίθηκαν στην πιλοτική φάση, η οποία ξεκίνησε τον Οκτώβριο του 2021 και ολοκληρώθηκε το Σεπτέμβριο του 2022. Πρωταρχικός στόχος για τη Φάση 3 ήταν και τα δύο πιλοτικά συστήματα να διασυνδεθούν και να

παρέχονται ως υπηρεσία, ώστε να αξιολογηθούν καλύτερα από τους επαγγελματίες. Στο πλαίσιο της φάσης αυτής έλαβαν χώρα τρεις δοκιμές – ασκήσεις:

- 8 Ιουνίου 2022[29], Λουμπλιάνα Σλοβενίας [327]. Το πρώτο πιλοτικό σενάριο αφορούσε σε δασική πυρκαγιά στην οποία επιχείρησαν περισσότεροι από 45 επαγγελματίες της δημόσιας ασφάλειας από Ιταλία, Ολλανδία, Λετονία, Γαλλία και Νορβηγία και οι εμπλεκόμενοι δοκίμασαν τη λύση της Airbus DS για ένα πανευρωπαϊκό δίκτυο κινητής τηλεφωνίας για υπηρεσίες δημόσιας ασφάλειας.
- 28/30 Ιουνίου 2022[30], Kerkrade Ολλανδίας, στα σύνορα με Βέλγιο και Γερμανία [328]. Το δεύτερο πιλοτικό σενάριο αφορούσε σε μια διασυνοριακή προσομοίωση καταδίωξης λαθρεμπόρων ναρκωτικών μέσω των συνόρων της Ολλανδίας, του Βελγίου και της Γερμανίας και οι περίπου 50 επαγγελματίες της δημόσιας ασφάλειας δοκίμασαν την προτεινόμενη λύση τόσο από την Airbus DS όσο και από την Frequentis AG.
- 18/21 Ιουλίου 2022[31], Μάλαγα Ισπανίας [329]. Το τρίτο και τελευταίο πιλοτικό σενάριο αφορούσε σε πυρκαγιά σε πλοίο, όπου έλαβαν μέρος συνολικά περισσότεροι από 100 επαγγελματίες από όλη την Ευρώπη που δοκίμασαν τη λύση της κοινοπραξίας Frequentis AG.

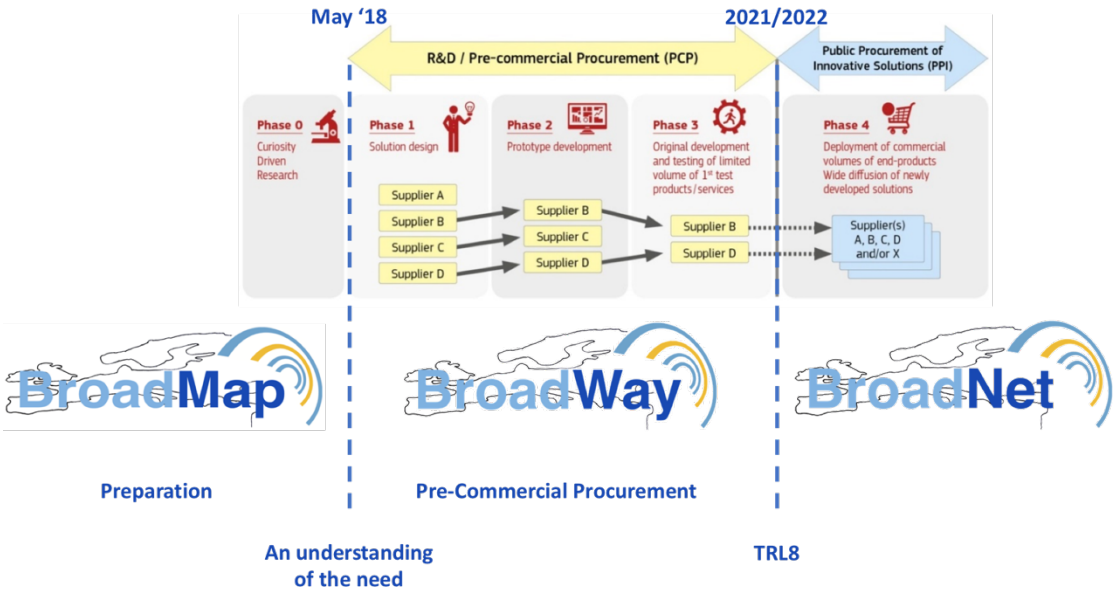
- Το *BroadNet* είναι η φυσική συνέχεια του BroadWay, που φιλοδοξεί να μετουσιώσει τις δύο πιλοτικές λύσεις, που δοκιμάστηκαν σε σχετικές ασκήσεις, σε υλοποιήσεις που θα βγουν στο πεδίο. Η πορεία έως το BroadNet συνοψίζεται στην Εικόνα 116. Ο στόχος εξακολουθεί να είναι η διασύνδεση εθνικών κρίσιμων κινητών ευρυζωνικών δικτύων, επιτρέποντας στους ανταποκριτές να λειτουργούν όπου κι αν βρίσκονται στην Ευρώπη, όποτε χρειάζεται και με όποιον τους ανατίθεται να συνεργαστούν. Οι επιμέρους στόχοι του έργου είναι:
  - Προετοιμασία για νομικά ζητήματα
  - Μοντέλο χρηματοδότησης του έργου
  - Έναρξη της οργάνωσης
  - Καθορισμός λειτουργικών προτύπων, πολιτικών και κανόνων
  - Ρύθμιση ζητημάτων πολιτικής και επικοινωνίας

Ο χρονικός ορίζοντας του έργου προκύπτει από την Εικόνα 117. Το παρόν και το μέλλον του έργου αφορά πλέον συνολικά στο BroadNet. Η αρχιτεκτονική που χρησιμοποιείται είναι το SpiceNet και βασίζεται σε πρότυπα και τυποποιήσεις της 3GPP.

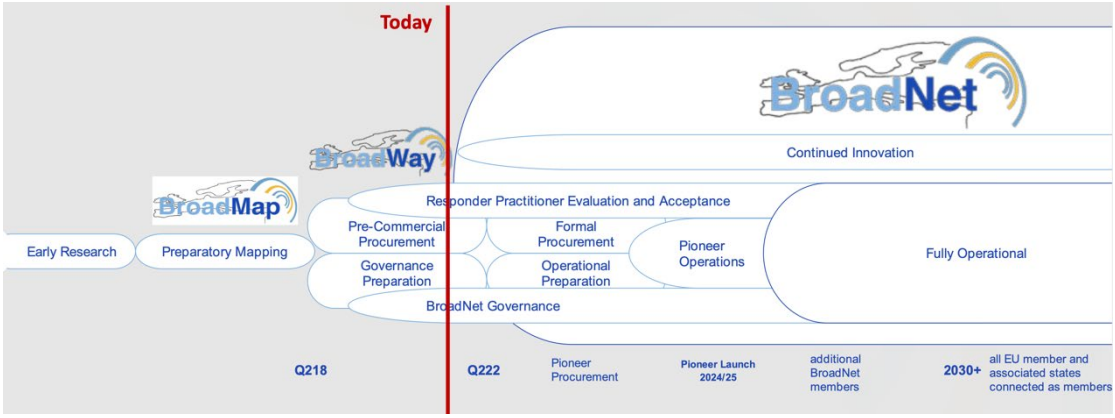
[29] https://youtu.be/g4oUO-axekM

[30] https://youtu.be/3ib49aNYQrk

[31] https://youtu.be/R21ULgDyKAs



Εικόνα 116. Από το BroadMap, στο BroadWay, στο BroadNet [322]

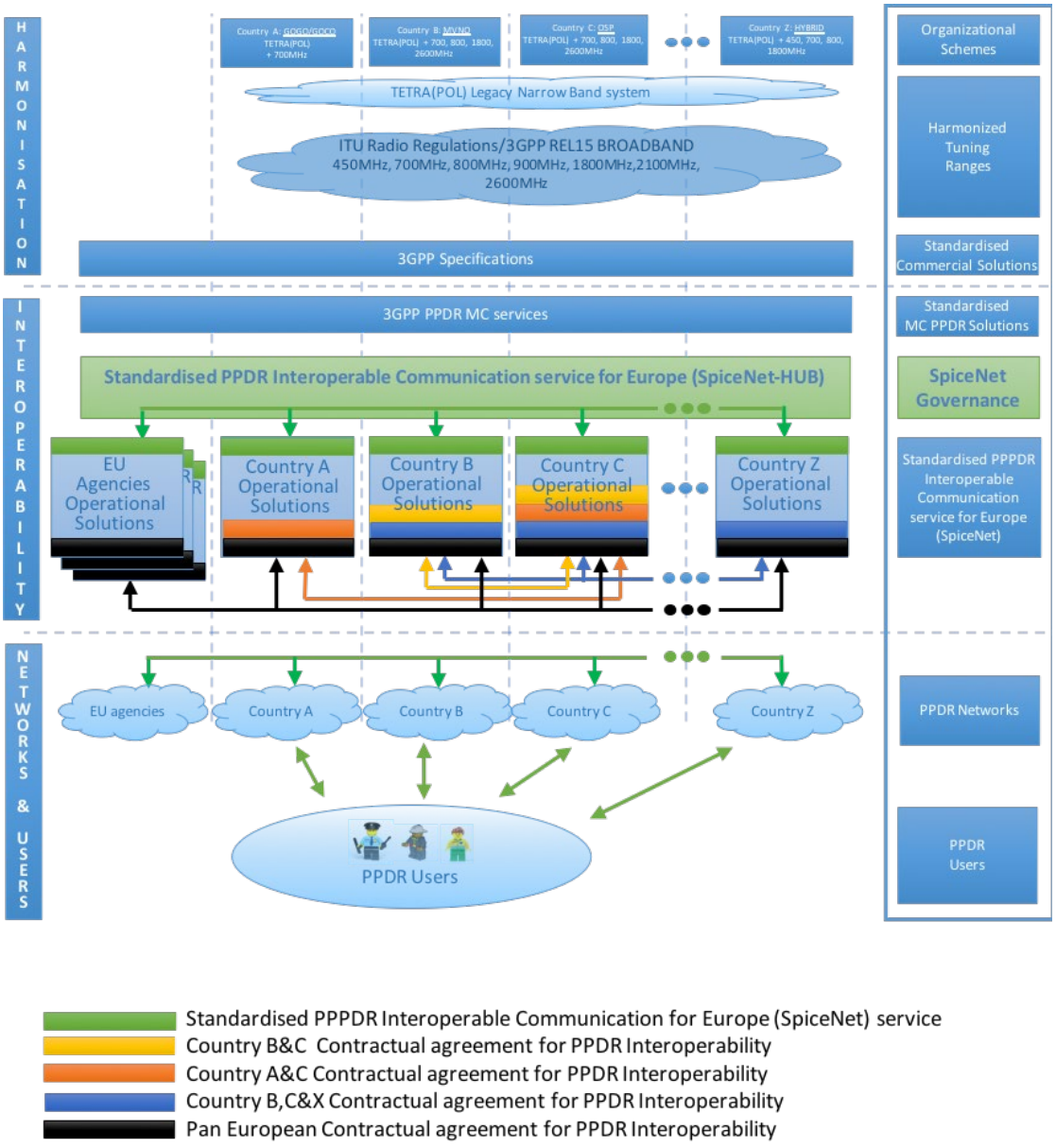


Εικόνα 117. Επιχειρησιακή κινητικότητα του έργου, από το BroadWay στο BroadNet [330]

Η αρχιτεκτονική του SpiceNet έχει σχεδιαστεί ώστε να μπορεί να παρέχει υπηρεσίες Mission Critical, MC όπως για παράδειγμα MC PTT, MC Data, MC Video, μηνύματα κατάστασης, επείγουσα ειδοποίηση, μηνύματα SDS. Οι υπηρεσίες SpiceNet βασίζονται σε ένα κατανεμημένο μοντέλο όπου κάθε χώρα έχει το δικό της HUB υπηρεσιών (SpiceNet HUB), το οποίο περιλαμβάνει επιχειρηματική λογική για όλες τις συμφωνίες διαλειτουργικότητας που σχετίζονται με κάθε χώρα. Το SpiceNet (Εικόνα 118) επιτρέπει στους χρήστες δημόσιας ασφάλειας διαλειτουργικότητα μεταξύ χωρών, αλλά και διυπηρεσιακή διαλειτουργικότητα.

Η διακρατική, πανευρωπαϊκή διαλειτουργικότητα μπορεί να υλοποιηθεί με αμοιβαίες διμερείς και πολυμερείς συμφωνίες μεταξύ χωρών κρατών μελών, οργανισμών PPDR και πανευρωπαϊκών οργανισμών (π.χ. Frontex, Europol, κ.λπ.). Οι βασικοί τομείς – επίπεδα της αρχιτεκτονικής του μοντέλου SpiceNet αφορούν:

i. Επίπεδο εναρμόνισης με τα υφιστάμενα πρότυπα και σχήματα οργανισμών
ii. Επίπεδο διαλειτουργικότητας
iii. Επίπεδο δικτύων και χρηστών



Εικόνα 118. Αρχιτεκτονική SpiceNet [331]

Το έργο φαίνεται ότι έχει ήδη επιτύχει σημαντική πρόοδο και μάλιστα τη σημαντικότερη έναντι οποιουδήποτε άλλου ανάλογου προγράμματος. Ωστόσο, βασικά «αγκάθια» σε μια τελική και υλοποιήσιμη λύση φαίνεται ν` αποτελούν ακόμη το ζήτημα της συνολικής χρηματοδότησης, αλλά και της πολιτικής συναίνεσης, που περιλαμβάνει την αποδεδειγμένη πρόθεση των Χωρών Μελών να εντάξουν την ενδεχόμενη λύση στην καθημερινή λειτουργία των υπηρεσιών δημόσιας ασφάλειας και ν` αποδώσουν σ` αυτήν πρωταγωνιστικό ρόλο, προβαίνοντας σε ανάλογες νομοθετικές και κανονιστικές ρυθμίσεις του ισχύοντος πλαισίου που τις διέπει.

b. Respond-A

Ένα ακόμη ευρωπαϊκό έργο ενταγμένο στο πρόγραμμα HORIZON2020, που ξεκίνησε τον Ιούνιο του 2020 και έχει διάρκεια τρία χρόνια (Ιούνιο 2023), έχει ως κύριους στόχους την

τεχνολογική αξιοποίηση και ένταξη των δυνατοτήτων του 5G για τους πρώτους ανταποκριτές και τον σχεδιασμό εξοπλισμού που θα φέρεται από τους επαγγελματίες, οι οποίοι θα χρησιμοποιούν τρία σετ αισθητήρων: υγείας, περιβαλλοντικούς, ενεργοποίησης έκτακτης ανάγκης για περίπτωση ατυχήματος. Για την υλοποίηση του έργου ακολουθείται συγκεκριμένη μεθοδολογία, που περιλαμβάνει πέντε διακριτά επίπεδα:

(α)Αντίληψης, η οποία επιτυγχάνεται με διαφόρων ειδών αισθητήρων, με κάμερες, με εντοπισμό τοποθεσίας ή ακόμη και με UAVs.

(β)Δικτύου, που αφορά στο δίκτυο επικοινωνίας και την τεχνολογία που χρησιμοποιείται (4G/5G, TETRA, TETRAPOL, Δορυφόροι, κ.λπ.)

(γ)Επεξεργασίας, που επιτυγχάνεται με την εφαρμογή τεχνολογίας MEC που φέρνει τους τεχνολογικούς πόρους πιο κοντά στον τελικό χρήστη, συγχώνευση δεδομένων για την παραγωγή πληροφοριών που διακρίνονται από συνέπεια, ακρίβεια και ευχρηστία.

(δ)Κατανόησης, που περιλαμβάνει έλεγχο, επίγνωση της κατάστασης, επαυξημένη πραγματικότητα και έγκαιρη προειδοποίηση.

(ε)Διεπαφής Χρήστη, που περιλαμβάνει τις εφαρμογές κινητών συσκευών, τις φιλικές προς τον χρήστη εφαρμογές και τις εφαρμογές επαυξημένης πραγματικότητας για τα κέντρα ελέγχου και τους πρώτους ανταποκριτές.

Το έργο Respond-A στοχεύει στην αξιοποίηση της ασφάλειας και της αποτελεσματικότητας των πρώτων ανταποκριτών μεγιστοποιώντας την επίγνωση της κατάστασης και ενισχύοντας τις επιχειρησιακές τους ικανότητες. Συνδυάζοντας μια ποικιλία καινοτόμων τεχνολογιών, ενισχύει την έγκαιρη και ασφαλή αξιολόγηση, τον μετριασμό του κινδύνου, ενώ διασφαλίζει σαφή κοινή λειτουργική εικόνα και βέλτιστη διαχείριση λειτουργιών, ακόμη και μεταξύ διαφορετικών μονάδων έκτακτης ανάγκης. Η αρχιτεκτονική του συστήματος και οι προδιαγραφές των εργαλείων είναι τα βασικά στοιχεία του συστήματος Respond-A, προς ένα ενιαίο και ευέλικτο πλαίσιο [332].

Η αρχιτεκτονική του συστήματος συνοψίζεται στην Εικόνα 120 και αποδεικνύει ότι η κύρια πρόκληση που κλήθηκε να αντιμετωπίσει ήταν η ενσωμάτωση όλων των διαφορετικών τεχνολογιών, με στόχο την παραγωγή ενός ενοποιημένου συστήματος, ικανού να υποστηρίξει επιχειρήσεις διάσωσης σε περιβαλλοντική ποικιλία και καταστάσεις. Τα βασικά δομικά στοιχεία της αρχιτεκτονικής είναι:

- Εφαρμόσιμη πλατφόρμα (deployable platform): Είναι το στοιχείο που προσφέρει υπηρεσίες επικοινωνίας και κέντρου ελέγχου και διοίκησης στους πρώτους ανταποκριτές. Η πλατφόρμα περιλαμβάνει δύο διακριτά πεδία που αλληλοεπιδρούν μεταξύ τους:

- ❖ Υποδομή επικοινωνίας (communication Infrastructure), που προσφέρει τοπική συνδεσιμότητα στην ευρύτερη περιοχή συμβάντων για τις διαφορετικές μονάδες πρώτων ανταποκριτών ώστε να μπορούν να επικοινωνούν όχι μόνο μεταξύ τους, αλλά και με το κέντρο ελέγχου και διοίκησης. Επιπλέον, επιτυγχάνει συνδεσιμότητα με τα απομακρυσμένα κέντρα ελέγχου, αλλά και το διαδίκτυο.
- ❖ Κινητό κέντρο ελέγχου και διοίκησης (mobile command and control center): όπου γίνεται επεξεργασία όλων των εισερχομένων δεδομένων και η υποστήριξη, ο συντονισμός και η οργάνωση όλων των διαφορετικών μονάδων των πρώτων ανταποκριτών.

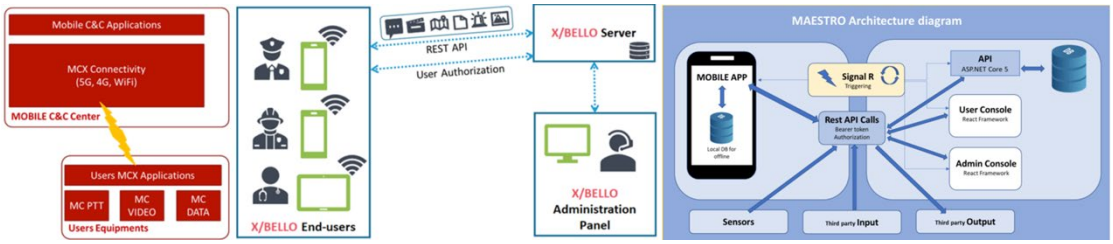
- Εργαλεία πεδίου (field tools), όπου εντάσσονται οι τεχνολογίες που υποστηρίζουν τους πρώτους ανταποκριτές και είναι ενσωματωμένες στον εξοπλισμό τους (π.χ. μπουφάν, κράνη, έξυπνα κινητά τηλέφωνα κ.λπ.), ή υπάρχουν επί των αυτόνομων μη επανδρωμένων οχημάτων που χρησιμοποιούν (π.χ.. UAV, UGV).
- Οι επικοινωνίες που εμπλέκονται στην αρχιτεκτονική μπορούν να είναι επίγειες, μεταξύ των πρώτων ανταποκριτών για αποστολή και λήψη δεδομένων, μέσω τοπικού δικτύου που δημιουργείται από ένα όχημα (Emergency Van), ή το δημόσιο δίκτυο εφόσον υφίσταται, καθώς επίσης και δορυφορικές (Iridium Satellite) φτάνοντας στο διαδίκτυο, καθώς και στο απομακρυσμένο κέντρο ελέγχου και διοίκησης.

Η ροή της πληροφορίας είναι η ακόλουθη: Τα δεδομένα που παράγονται από τις τεχνολογίες που εφαρμόζονται στην περιοχή που λαμβάνει χώρα το συμβάν, όπου επιχειρούν οι πρώτοι ανταποκριτές, μεταδίδονται στο κινητό κέντρο ελέγχου και διοίκησης, όπου αποθηκεύονται, αναλύονται, υποβάλλονται σε επεξεργασία και διατίθενται στους αρμόδιους χειριστές (εξειδικευμένο προς τούτο προσωπικό), παρέχοντας έτσι επίγνωση της κατάστασης και ενισχύοντας την αποτελεσματικότητα των πρώτων ανταποκριτών στη διαχείριση της συνολικής αποστολής. Οι λειτουργίες αυτές πραγματοποιούνται όσο το δυνατόν πιο κοντά στους πρώτους ανταποκριτές ώστε να παρέχεται ευελιξία, ευρωστία και αποτελεσματικότητα.

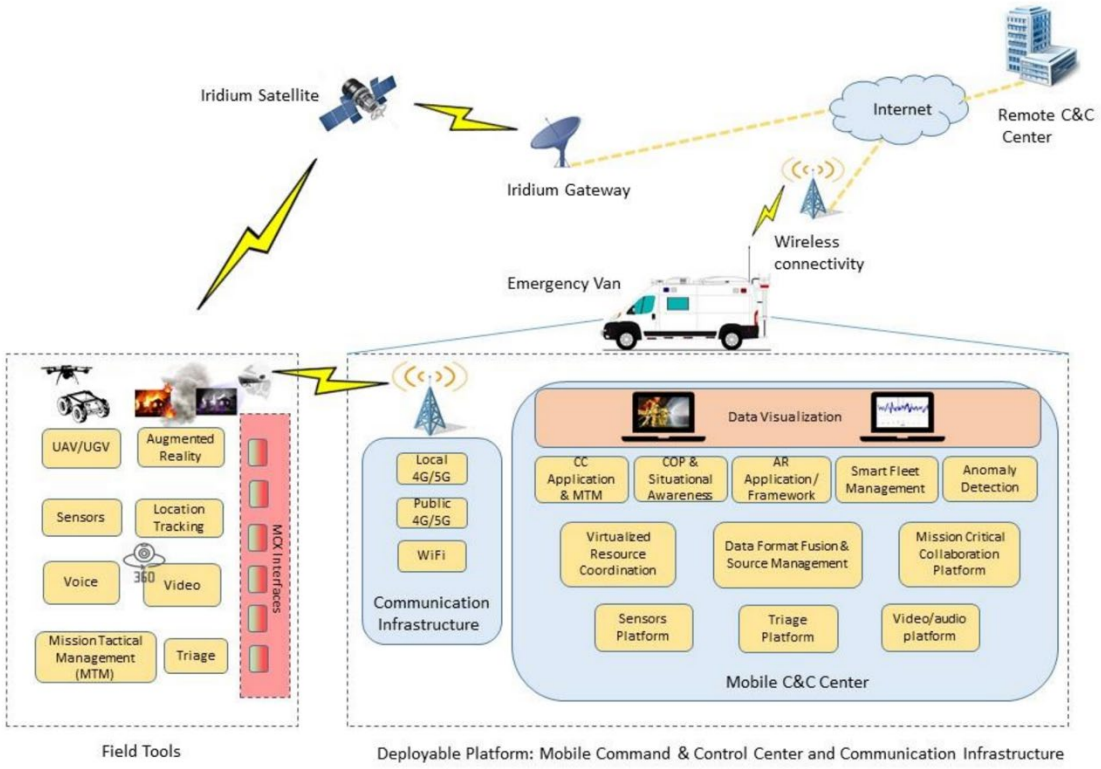
Οι βασικές τεχνολογίες που υποστηρίζουν τη συνολική λειτουργία είναι οι ακόλουθες και κάθε μία εξ αυτών βασίζεται σε δική της αρχιτεκτονική λειτουργίας, η οποία περιγράφεται αναλυτικά στο [332] και εποπτικά στην Εικόνα 119:

- MCX, επιτρέπει τη δημιουργία ομάδων, με διακριτούς προδιαγεγραμμένους ρόλους και καθήκοντα, με δυνατότητες δυναμικής τροποποίησης της σύνθεσης αυτών κατά τις ανάγκες της επιχείρησης και παροχή στις συσκευές των χρηστών υπηρεσιών MCPTT (φωνής), MCVideo (βίντεο) και MCData (δεδομένων) (Εικόνα 119.a).

- XBELLO, προσφέρει στους πρώτους ανταποκριτές δύο είδη εφαρμογών, την εφαρμογή διαδικτύου (Web Desktop) και την εφαρμογή για έξυπνα κινητά τηλέφωνα, μέσω σύνδεσης με τον server, όπου φυλάσσονται όλες οι πληροφορίες (Εικόνα 119.b).
- MAESTRO, ως ολοκληρωμένο σύστημα διαχείρισης πληροφοριών (IMS) επιτρέπει στους πρώτους ανταποκριτές από διαφορετικά οντότητες (Αστυνομία, Πυροσβεστική, Λιμενικό, ΕΚΑΒ, κ.λπ.) να επικοινωνούν και ανταλλάσσουν πληροφορίες από το πεδίο, σε άμεση και διαρκή επικοινωνία με το κέντρο ελέγχου και διοίκησης, ώστε να λαμβάνουν ανατροφοδότηση στην κινητή συσκευή τους την ενιαία επιχειρησιακή εικόνα και κατάσταση (Εικόνα 119.c).



Εικόνα 119. Αρχιτεκτονική (a)MCX, (b)X/BELLO, (c)MAESTRO



Εικόνα 120. Αρχιτεκτονική του συστήματος RESPOND-A [332]

Στο έργο συμμετέχουν συνολικά δεκατρείς (13) χώρες της Ευρωπαϊκής Ένωσης (Εικόνα 121), ανάμεσα στις οποίες και η χώρα μας. Στο πλαίσιο δοκιμών των προτεινόμενων λύσεων έχουν υλοποιηθεί ήδη τρία σενάρια (Περιπτώσεις Χρήσης) τα οποία αποτυπώνονται στη συνέχεια συνοπτικά και τα αποτελέσματα των οποίων καταγράφηκαν αναλυτικά στο [333]:

- 19 Οκτωβρίου 2022, Λεμεσός και Λάρνακα Κύπρου[32]. Την πρώτη εβδομάδα του Ιουλίου του 2021 τεράστια πυρκαγιά έκαψε 55Km^2 και προκάλεσε τον θάνατο τεσσάρων ανθρώπων. Οι Κύπριοι πυροσβέστες έσβησαν την φωτιά με τη συνδρομή πυροσβεστών από την Ελλάδα, το Ισραήλ, την Ιταλία και το Ηνωμένο Βασίλειο. Με αφορμή την καταστροφική αυτή πυρκαγιά, το διάστημα 28/30-9-2021 η Respond-A διοργάνωσε στην Κύπρο τη δεύτερη εκπαιδευτική συνεδρίαση, στο πλαίσιο της οποίας παρουσίασε τις νέες τεχνολογικές λύσης. Ακολούθως, την 19-10-2021 στη Λάρνακα, σε σενάριο εκτεταμένης έκτασης πυρκαγιάς σε δασική περιοχή δοκιμάστηκαν καινοτόμες τεχνολογίες και εξοπλισμός που ενισχύουν την ασφάλεια και τις επιχειρησιακές δυνατότητες των πρώτων ανταποκριτών, σε. Τα πεπραγμένα του σεναρίου είναι διαθέσιμα στο [334].
- 22 Σεπτεμβρίου 2022, Αιγάλεω Αττικής[33]. Το διάστημα 2/3-3-2022 στο Αιγάλεω Αττικής έλαβε χώρα η δεύτερη εκπαιδευτική συνάντηση της Respond-A, το πλαίσιο της οποίας παρουσιάστηκαν - προτάθηκαν καινοτόμες λύσεις στο πλαίσιο του έργου, οι οποίες φιλοδοξούν να υλοποιήσουν τους σκοπούς του και οι οποίες δοκιμάστηκαν αργότερα σε άσκηση – σενάριο σεισμού και διαχείρισης καταστροφικών συνεπειών του, που έλαβε χώρα στον ίδιο ελληνικό δήμο την 22-9-2022. Στην άσκηση συμμετείχαν 43 επαγγελματίες της δημόσιας ασφάλειας από το σύνολο των Χωρών που συμμετέχουν στο έργο. Τα πεπραγμένα του σεναρίου είναι διαθέσιμα στο [335].
- Φεβρουάριος 2023, Βαλένθια Ισπανίας. Στις 8/9-6-2022 η Respond-A διοργάνωσε την τέταρτη εκπαιδευτική συνάντηση στη Φιλιππούπολη, όπου συμμετείχαν 50 επαγγελματίες προερχόμενοι από το σύνολο των χωρών που συμμετέχουν στο έργο. Παρουσιάστηκαν τεχνολογικές λύσεις οι οποίες θα δοκιμαστούν στη συνέχεια σε σενάριο εκτεταμένης μόλυνσης από εκτεταμένη διαρροή πετρελαίου που θα λάβει χώρα στη Βαλένθια της Ισπανίας τον Φεβρουάριο του 2023.

Εικόνα 121. Χώρες της ΕΕ που συμμετέχουν στο Respond-A Project

[32] https://youtu.be/yF18j6B2c2g

[33] https://youtu.be/g4bAzVHt2H0

Το έργο βρίσκεται ακόμη σε εξέλιξη για να εκτιμηθεί με ασφάλεια εάν θα οδηγήσει σε κάποια ρεαλιστική λύση και αν θα επιτύχει τον αρχικό του στόχο. Σαφέστατα, όπως αποτυπώθηκε ήδη έχουν γίνει σημαντικά βήματα με αξιόλογες προτάσεις – υλοποιήσεις, ειδικότερα στο τομέα των συσκευών που χρησιμοποιούν οι πρώτοι ανταποκριτές, οι οποίες παρουσιάζονται διεξοδικά στο ανάλογο κεφάλαιο, πλην όμως από τη μέχρι τώρα πορεία δεν φαίνεται να είναι ικανό να οδηγήσει σε μια πλήρως ικανοποιητική λύση που θα αποτελέσει οδηγό για την επίτευξη της πλήρους διαλειτουργικότητας. Ωστόσο, για τα τελικά συμπεράσματα απομένει να ολοκληρωθεί η προσπάθεια ώστε αποτιμηθεί αναλόγως.

c. Άλλες υλοποιήσεις - προγράμματα

Έχουν γίνει αρκετές ανάλογες προσπάθειες και αυτό που έχει ήδη καταγραφεί είναι ότι κάθε μια εξ αυτών συνεισφέρει είτε λιγότερο, είτε περισσότερο στην καταγεγραμμένη και δρομολογημένη πλέον πορεία προς τη διαλειτουργικότητα, τη συνεργασία και την επιχειρησιακή συνέχεια, πέρα και πάνω από γεωγραφικά σύνορα. Χαρακτηριστικά παραδείγματα, τμηματικές υλοποιήσεις και συσκευές των οποίων θα δούμε σε επόμενα κεφάλαια, αποτελούν:

- INGENIOUS[34], που αποτελεί ένα πρόγραμμα που στοχεύει να βοηθήσει τους πρώτους ανταποκριτές να είναι πιο αποτελεσματικοί κατά τη διάρκεια φυσικών και ανθρωπογενών καταστροφών και κρίσεων, αξιοποιώντας νέες τεχνολογίες υπό τη γενική ονομασία Ενσωματωμένη Εργαλειοθήκη Επόμενης Γενιάς (Next Generation Integrated Toolkit – NGIT).
- FASTER[35], που αποτελεί ένα πρόγραμμα για την προστασία των πρώτων ανταποκριτών σε επικίνδυνα περιβάλλοντα και την ενίσχυση των δυνατοτήτων τους όσον αφορά την επίγνωση της κατάστασης και την επικοινωνία. Χρησιμοποιεί ένα σύνολο σημαντικών τεχνολογιών υποστήριξης που θα αναπτυχθούν για την παράκαμψη ειδικών συνθηκών που εκδηλώνονται κατά τη διάρκεια καταστροφών και εμποδίζουν την ανάπτυξη και την αποτελεσματικότητα των παραδοσιακών συστημάτων αντιμετώπισης καταστροφών.
- Search And Rescue[36], που αποτελεί ένα πρόγραμμα που παρέχει τεχνολογικές λύσεις για τον γρήγορο εντοπισμό εγκλωβισμένων θυμάτων με τη χρήση προηγμένων ένδυτων μέσων για την αξιολόγηση του κινδύνου και την ασφάλεια των πρώτων ανταποκριτών.

[34] https://ingenious-first-responders.eu

[35] https://www.faster-project.eu

[36] https://search-and-rescue.eu

- SIXTHSENSE[37], που αποτελεί μια διεπιστημονική δράση καινοτομίας και έρευνας με γενικό στόχο την ανάπτυξη ενός φορητού συστήματος παρακολούθησης της υγείας με απτική βιοανάδραση κλειστού βρόχου, που επιτρέπει στους πρώτους ανταποκρινόμενους σε επικίνδυνες καταστάσεις να αντιληφθούν την τρέχουσα κατάσταση της υγείας τους.

Θα ήταν ουτοπικό βέβαια να θεωρήσουμε ότι ο κατάλογος εξαντλείται μ' αυτά, καθώς έγινε όλως ενδεικτική αποτύπωση των χαρακτηριστικότερων. Παράλληλα, σε βιβλιογραφικό επίπεδο είναι άξια αναφοράς η προσπάθεια που έκαναν οι [52], οι οποίοι συγκέντρωσαν, ενέταξαν σε τρεις μεγάλες κατηγορίες και συνέκριναν με βάση θεμελιώδη χαρακτηριστικά έναν αριθμό από ασύρματα δίκτυα και συστήματα άμεσης ανταπόκρισης, τα οποία κατά κύριο λόγο επιχείρησαν να δώσουν τεχνολογικές απαντήσεις στην αντιμετώπιση των περιπτώσεων έκτακτης ανάγκης και αντιμετώπισης των συνεπειών καταστροφικών γεγονότων (ανθρωπογενών ή μη). Η κατηγοριοποίηση αφορά σε:

(1)Δίκτυα και συστήματα με δυνατότητα μετάδοσης πολυμέσων

(2)Δίκτυα και συστήματα ανάκαμψης και διαχείρισης καταστροφών

(3)Δίκτυα και συστήματα για την παρακολούθηση ασθενών σε πραγματικό χρόνο και από άκρο σε άκρο. Τα έργα που αναφέρονται και συγκρίνονται στην αναφερόμενη σχετική εργασία διαλαμβάνονται στον Πίνακα 24. Ανεξαρτήτως δε εάν οι επιστημονικές αυτές προτάσεις πήραν ή όχι την οδό της βιομηχανικής παραγωγής, το κυρίαρχο και ταυτοχρόνως πολύτιμο συμπέρασμα της συγκριτικής μελέτης όλων αυτών είναι ότι η επιλογή των κατάλληλων τεχνολογικών λύσεων είναι ένα ζήτημα πολυπαραγοντικό που εξαρτάται εκτός των άλλων μια σειρά κριτηρίων και χαρακτηριστικών, όπως:

[37] https://sixthsenseproject.eu

Α/Α	Συστήματα έκτακτης ανάγκης	Αναφορές	Πεδία εφαρμογής – Σκοπιμότητα των έργων
1	DUMBONET	[336]	Διεπιστημονική προσπάθεια για τη δημιουργία ενός πραγματικού, βιώσιμου συστήματος που μπορεί να χρησιμοποιηθεί σε καταστάσεις έκτακτης ανάγκης που σχετίζονται με καταστροφές, όπου η παραδοσιακή επικοινωνιακή υποδομή δεν είναι λειτουργική.
2	DistressNet	[337], [338]	Ένα ad hoc δίκτυο που υποστηρίζει τις επικοινωνίες σε κατατάσσεις έκτακτης ανάγκης με στόχο να παρέχει καλύτερη δυνατή επίγνωση κατάστασης και έγκαιρη παράδοση υψηλών όγκων δεδομένα. Η αρχιτεκτονική προσφέρει ενεργειακή απόδοση και μεγιστοποιεί την κάλυψη.
3	SALICE	[115]	Επικεντρώνεται αφενός στην προσπάθεια επίτευξης παγκόσμιας κάλυψης της περιοχής έκτακτης ανάγκης με την κατάλληλη συνεργατική χρήση δορυφορικών συστημάτων, και αφετέρου στην ανάπτυξη ενός αναδιαμορφώσιμου συνεταιριστικού συστήματος NAV/COM, για την υλοποίηση του οποίου προτείνεται μια τεχνική υποβοηθούμενου εντοπισμού. Αναλύονται πτυχές αναδιαμόρφωσης, διασύνδεσης και διαλειτουργικότητας και μελετήθηκαν στρατηγικές συνεργασίας μεταξύ πλατφορμών μεγάλου υψομέτρου (HAPs) και ad hoc αναπτυγμένων δικτύων (π.χ. MANET). Η τεχνική υποβοηθούμενου εντοπισμού που προτείνεται βασίζεται σε κατάλληλη αλγοριθμική εκμετάλλευση της μετάδοσης βοηθητικών πληροφοριών των συστημάτων γεωοεντοπισμού (GNSS).
4	MIKoBOS	[339]	Προτείνεται ένα σύστημα με συνδυασμό επίγειων και δορυφορικών δικτύων που επιτρέπουν την αξιόπιστη επικοινωνία δεδομένων εντός της κρίσιμης περιοχής, καθώς και με το κέντρο ελέγχου (έδρα), η οποία παρέχει διαφορετικά επίπεδα πρόσβασης στους εμπλεκομένους, συνεισφέροντας στην αποτελεσματικότερη επικοινωνία και επιχειρησιακή ανταπόκριση
5	SAFIRE	[340]	Μια αρχιτεκτονική που βασίζεται (1)στο Main Command Center για την υποστήριξη της άμεσης επικοινωνίας μεταξύ των πρώτων ανταποκριτών, (2)σε έναν μηχανισμό δημοσίευσης-εγγραφής για την ανταλλαγή πληροφοριών μεταξύ των πρώτων ανταποκριτών και (3) σε ένα ευέλικτο πλαίσιο πολλαπλών επιπέδων για τη βέλτιστη διαμόρφωση του συστήματος
6	Hybrid System	[341]	Προτείνεται ένα υβριδικό μοντέλο δορυφορικού και επίγειου συστήματος για κινητές επικοινωνίες έκτακτης ανάγκης, που μπορεί να αναπτυχθεί γρήγορα και να προσαρμόζεται δυναμικά σε καταστροφές οποιασδήποτε φύσης και τοποθεσίας. Η συνολική αρχιτεκτονική βασίζεται σε IPv6 και σε VCG, τα οποία μπορούν να δημιουργήσουν ένα δίκτυο ad-hoc μεταξύ οχημάτων που ενεργούν στο πεδίο και να παρέχουν συνδεσιμότητα σε απομονωμένες κυψέλες IPv6. Συγκεκριμένα, προτείνονται δύο τύποι VCG για τη δορυφορική επαφή, για τους οποίους θα αναφέρουμε περαιτέρω αναλυτικά στοιχεία στη συνέχεια του κεφαλαίου (οχήματα S-UMTS στη ζώνη L ή S και οχήματα DVB-RCS στη ζώνη Ku ή Ka).
7	IoT-based System	[342]	Μια πρόταση που δεν αφορά στην επικοινωνία, αλλά στην εμπλοκή της τεχνολογίας στη λήψη κρίσιμων αποφάσεων σε καταστάσεις έκτακτης ανάγκης. Προτείνεται μια νέα μεθοδολογία για την επίτευξη μεγιστοποίησης συναίνεσης στη λήψη αποφάσεων, όπου εφαρμόζονται τα ανάλογα σχέδια απόκρισης της κοινότητας. Η μοντελοποίηση που προτάθηκε ενσωματώθηκε σε υπολογιστικά προγράμματα σε πανεπιστημιακό επίπεδο (Ιντιάνα, Η.Π.Α.) και η μεθοδολογία της περιλαμβάνει ενίσχυση της γνώσης από την ομάδα, κατάλληλη αλγοριθμική ομαδοποίηση και ένταξη των απόψεων των ειδικών χωρίς να επηρεάζεται η λήψη της απόφασης.
8	WiMesh	[343]	Προτείνεται ένα ανθεκτικό ασύρματο δίκτυο επικοινωνίας για καταστάσεις έκτακτης ανάγκης (WMN) για αγροτικές περιοχές, ή περιοχές – χώρες με πολύ περιορισμένους πόρους. Το δίκτυο αυτό εστιάζει σε σχεδιαστικές παραμέτρους και στα κύρια χαρακτηριστικά των απαιτήσεων (ασφάλεια, χαμηλό κόστος, χαμηλή ισχύ, μέγεθος, διαθεσιμότητα, προσαρμογή, φορητότητα, ευκολία εγκατάστασης και ανάπτυξης και περιοχή κάλυψης). Δοκιμάστηκε η επικοινωνία μεταξύ χρηστών ευρισκομένων σε ένα ορεινό χωριό του Πακιστάν, σε μεγάλη γεωγραφική περιοχή, με έλλειψη κυψελοειδούς κάλυψης ή άλλης επικοινωνιακής υποδομής. Για τον σκοπό αυτό αξιοποιήθηκε η δικτύωση hop mesh και φορητές συσκευές εξοπλισμένες με Wi-Fi.
9	MyDisasterDroid	[344]	Σε περιοχή που ταλανίζεται από καταστροφικά φυσικά φαινόμενα, αλλά και έλλειψη αποτελεσματικού συστήματος διαχείρισης αυτών, όπως οι Φιλιππίνες, προτείνεται ένα σύστημα επικοινωνίας που βασίστηκε στα ούτως ή άλλως ελκυστικά έξυπνα κινητά τηλέφωνα και στο λειτουργικό σύστημα Android της Google (MyDisasterDroid). Η εφαμρογή καθορίζει τη βέλτιστη διαδρομή κατά μήκος διαφορετικών γεωγραφικών τοποθεσιών που πρέπει να ακολουθήσουν οι εθελοντές και οι διασώστες για να εξυπηρετήσουν τον μεγαλύτερο αριθμό ατόμων και να παρέχουν τη μέγιστη κάλυψη της περιοχής στο συντομότερο δυνατό χρόνο.
10	WISARD	[345]	Το σύστημα που προτείνεται διερευνά τη χρήση επεκτάσιμων ασύρματων δικτύων για τη διευκόλυνση της ιατρικής περίθαλψης στον τόπο μιας καταστροφής και ειδικότερα βιομηχανικών ατυχημάτων ή τρομοκρατικών επιθέσεων με τραυματίες ή πληγέντες από χημική, βιολογική ή ραδιενεργή μόλυνση. Εμπλέκονται δίκτυα πλέγματος και τεχνολογικές λύσεις που βασίσθηκαν σε τηλεμετρία και RFID. Έγινε δοκιμαστική εφαρμογή σε ασκήσεις στο Σαν Ντιέγκο, Η.Π.Α..
11	ARTEMIS	[346]	Το όνομα του έργου προέρχεται από το Automated Remote Triage and Emergency Management Information System (ARTEMIS) και επιδιώκει να παρέχει επίγνωση της κατάστασης σε όλα τα επίπεδα εντολών, προκειμένου να αυξηθεί το ποσοστό επιβίωσης των ασθενών σε καταστάσεις έκτακτης ανάγκης. Για τον σκοπό αυτό χρησιμοποιεί ένα δίκτυο ενσωματωμένων αισθητήρων σε ανταποκριτές και θύματα για τη συλλογή των δεδομένων που απαιτούνται για μεγαλύτερη επίγνωση της κατάστασης και αναμετάδοση αυτών σε κατάλληλα επίπεδα εντολών τόσο στο πεδίο όσο και σε απομακρυσμένες τοποθεσίες

Α/Α	Συστήματα έκτακτης ανάγκης	Αναφορές	Πεδία εφαρμογής – Σκοπιμότητα των έργων (**συνέχεια πίνακα**)
12	MEDiSN	[347]	Το έργο αφορά σε ένα ασύρματο δίκτυο αισθητήρων (Physiological Monitors) για την παρακολούθηση των ιατρικών δεδομένων των ασθενών στα νοσοκομεία και κατά τη διάρκεια καταστροφών. Αφορά σε αρχιτεκτονική δύο επιπέδων που παρέχει αξιόπιστη επεξεργασία δεδομένων μεγάλου όγκου και εκπλήρωση απαιτήσεων QoS. Για την αξιολόγηση, πραγματοποιήθηκαν πιλοτικές δοκιμές και προσομοιώσεις σε κλίνες νοσοκομείων και τα αποτελέσματα κρίθηκαν ενθαρρυντικά.
13	HYGEIAnet	[348]	Μια επισκόπηση της κατάστασης των κινητών συστημάτων υγειονομικής περίθαλψης και των εφαρμογών τους που εστιάζουν στην παρεχόμενη υποστήριξη για καταστάσεις έκτακτης ανάγκης. Η τεχνολογική αξιοποίηση ασύρματων επικοινωνιών και εφαρμογών, ειδικότερα στη μετάδοση ζωτικής σημασίας δεδομένων που αφορούν στην καρδιακή λειτουργία, αλλά και σε εξειδικευμένα σενάρια αυξημένων ιατρικών απαιτήσεων (αντιμετώπιση εγκεφαλικού, διενέργεια υπερήχου, κ.λπ.).
14	AID-N	[349]	Άλλη μια περίπτωση αξιοποίησης της τεχνολογίας για την απομακρυσμένη παρακολούθηση ιατρικών δεδομένων ασθενών. Ειδικότερα σε περιπτώσεις αντιμετώπισης μαζικών καταστροφών, όπου οι ανάγκες ταυτόχρονης παρακολούθησης ασθενών εκτοξεύονται, η τεχνολογική αρωγή καθίσταται επιβεβλημένη. Στο πλαίσιο αυτό παρουσιάζεται ο σχεδιασμός ηλεκτρονικών ετικετών με περιορισμένη μνήμη και υπολογιστική ισχύ, που χρησιμοποιούν βιοϊατρικούς αισθητήρες (παλμογράφο, οξύμετρο, ηλεκτροκαρδιογράφο) για τη συνεχή παρακολούθηση ασθενών – τραυματισμένων και των παροχή χρήσιμων πληροφοριών στους πρώτους ανταποκριτές. Έγινε δοκιμαστική εφαρμογή σε άσκηση και αποδείχθηκε ότι με τη χρήση του συστήματος επιτεύχθηκε η επιτυχημένη διαλογή στοιχείων ασθενών – τραυματιών από τριπλάσιο αριθμό ατόμων, σε σχέση με την παραδοσιακή μέθοδο.
15	MiTag	[350]	Ένα παρεμφερές σύστημα, τουλάχιστον ως προς τη χρησιμότητα, με το προηγούμενο. Συγκεκριμένα, μια πλατφόρμα παρακολούθησης ασθενών που αναπτύχθηκε σε συνεργασία με το EMS και το Νοσοκομείο της Βαλτιμόρης, Η.Π.Α., η οποία περιλαμβάνει ένα οικονομικά αποδοτικό δίκτυο αισθητήρων, ένα ασύρματο δίκτυο με δυνατότητα αυτό-οργάνωσης και ένα επεκτάσιμο λογισμικό που παρέχει ανάλυση δεδομένων αισθητήρων και ενημερώσεις σε πραγματικό χρόνο. Το σύστημα αξιολογήθηκε μέσω δοκιμών με ενθαρρυντικά αποτελέσματα.
16	Integrated System	[351]	Ίδιας φιλοσοφίας προσέγγιση και σ' αυτή την περίπτωση, η οποία αναφέρει ότι οι τεχνολογικές εξελίξεις μπορούν να έχουν εφαρμογή στη βελτίωση της επιτόπιας φροντίδας ασθενών – θυμάτων καταστροφών και τη διαχείριση πόρων (πρώτοι ανταποκριτές - διασώστες, ιατρικό προσωπικό πεδίου, τμήματα έκτακτης ανάγκης και νοσοκομεία)
17	Patient Monitoring	[352], [353]	Ένα ακόμη σύστημα παρακολούθησης ασθενών σε πραγματικό χρόνο που ενσωματώνει αισθητήρες ζωτικών σημείων, αισθητήρες τοποθεσίας, ad-hoc δικτύωση, ηλεκτρονικά αρχεία ασθενών και τεχνολογία διαδικτυακής πύλης για να επιτρέπει την απομακρυσμένη παρακολούθηση της κατάστασής τους και παρέχει σημαντικότατες υπηρεσίες στους επαγγελματίες της αντιμετώπισης καταστροφών [352]. Η «κινητή υγεία» όπως χαρακτηρίζεται ξεπερνά τα γεωγραφικά, χρονικά και οργανωτικά εμπόδια και διευκολύνει την απομακρυσμένη διάγνωση, παρακολούθηση και μεταφορά ιατρικών δεδομένων και αρχείων. Γίνεται αναφορά σε τεχνολογικά πρότυπα και συγκεκριμένα στα IEEE 802.16/WiMAX και IEEE 802.11/WLAN και παρατίθενται συγκριτικά στοιχεία αυτών [353].
18	MASCAL	[354]	Ένα ακόμη ολοκληρωμένο σύστημα απομακρυσμένης ιατρικής παρακολούθησης για τη βέλτιστη αξιοποίηση των πόρων σε ένα νοσοκομείο κατά τη διάρκεια μιας κατάστασης μαζικών καταστροφών ή ατυχημάτων. Το συγκεκριμένο χρησιμοποιεί ετικέτες που επικοινωνούν με χρήση πρωτοκόλλου 802.11b για την παρακολούθηση ασθενών, εξοπλισμού και προσωπικού κατά τη διάρκεια της απόκρισης σε μια καταστροφή, ενσωματώνοντας πληροφορίες θέσης με δεδομένα από διάφορες βάσεις δεδομένων και συστημάτων. Μάλιστα, περιλαμβάνει ένα σύνολο επαρκών διεπαφών για την κάλυψη των αναγκών λειτουργίας του. Υποβλήθηκε σε λειτουργική αξιολόγηση στο Naval Medical Center, San Diego, USA
19	AMON	[355]	Ένα σύστημα παρακολούθησης που φοριέται στον καρπό και απαλλάσσει τον ασθενή υψηλού κινδύνου από τους περιορισμούς του σταθερού εξοπλισμού παρακολούθησης. Συνδυάζει πολύπλοκη ιατρική παρακολούθηση, ανάλυση δεδομένων και δυνατότητες επικοινωνίας σε μορφή ρολογιού. Η εργασία αναφέρεται στη λειτουργικότητα, στην αρχιτεκτονική και στα ζητήματα υλοποίησης του συστήματος
20	AMBULANCE	[356]	Ανάπτυξη μιας φορητής ιατρικής συσκευής που επιτρέπει την τηλεδιάγνωση και την απομακρυσμένη υποστήριξη του ασθενούς στο στάδιο προνοσοκομειακής διαχείρισης από ειδικούς γιατρούς, η οποία έχει αποδειχθεί ότι βελτιώνει σημαντικά τα ποσοστά επιβίωσης. Η συσκευή μεταδίδει ζωτικής σημασίας πληροφορίες χρησιμοποιώντας το δίκτυο κινητής τηλεφωνίας GSM. Η απόδοση του συστήματος έχει υποβληθεί σε έλεγχο με πραγματικούς ασθενείς.
21	Serval BatPhone	[357]	Προτείνεται μια πλατφόρμα κινητής τηλεφωνίας serval mesh και γίνεται ανάλυση της αναγκαιότητας και περιγραφή της λειτουργικότητάς της, χωρίς να αναφέρονται ιδιαίτερα τεχνολογικά στοιχεία υλοποίησης ή αρχιτεκτονικής.

Πίνακας 24. Αξιολόγηση ασύρματων συστημάτων έκτακτης ανάγκης (Πεδία εφραρμογής και πηγές των έργων).

- Την περιοχή κάλυψης, επειδή είναι σημαντικά διαφορετικό να υπάρχει ανάγκη κάλυψης χιλιομέτρων για μια εκτεταμένη φυσική καταστροφή, συγκριτικά με την παρακολούθηση για μόνο κάποια μέτρα (π.χ. αισθητήρων που φέρουν οι πρωτοι ανταποκριτές που επιχειρούν εντός ενός κτηρίου)
- Το κόστος, σε σχέση πάντοτε και με το αποτέλεσμα και την αποτελεσματικότητα του συστήματος του οποίου επίκειται η προμήθεια. Συνήθως αφορούν κυβερνητικές αποφάσεις, σε περιόδους που λόγω της καταστροφής η οικονομία είναι ήδη επιβαρυμένη.
- Τη διαθεσιμότητα εξοπλισμού που σε κάθε περίπτωση συναρτάται άμεσα από τις εταιρείες που κατασκευάζουν αυτόν. Εξυπακούεται ότι ο μεγαλύτερος ανταγωνισμός, επιδρά θετικά στον δυνητικό αγοραστή.
- Την ευχρηστία εγκατάστασης που περιλαμβάνει την ευκολία εγκατάστασης, χειρισμού και συντήρησης του εξοπλισμού.
- Την τεκμηρίωση, η οποία είναι άμεσα συνδεδεμένη με την ευκολία στη χρήση και την εν γένει ευχρηστία του εξοπλισμού

Για κάθε ένα από αυτά τα χαρακτηριστικά, προκύπτει η συγκριτική παράθεση των έργων στον Πίνακας 25.

Emergency Response System	Wireless Coverage	Cost Effectiveness	Equipment Avialability	Portability & Installation	Documentation
DUMBONET [9]	Several hundred kilometers	Low due to satellite subscription	COTS	Portable & high installation time	Good
DistressNet [10]	Few hundred kilometers	High	Inexpensive COTS	Portable & average installation time	Good
SALICE [11]	Several hundred kilometers	Low due to satellite & aerial platforms	Combination of COTS & proprietery	Portable & high installation time	Not available
MIKoBOS [56]	Several hundred kilometers	Low due to satellite & PSO-proprietary TETRA	Combination of COTS & proprietary	Portable & high installation time	Not available
SAFIRE [62]	Tens of kilometers	No information given	No information given	Portable & low installation time	Not available
Hybrid System [58]	Several hundred kilometers	Low due to satellite subscription	COTS	Portable & average installation time	Not available
IoT-based System [29]	Hundreds of kilometers	No information given	No information given	Portable & low installation time	Not available
WiMesh [76]	Tens of kilometers	High due to cheap equipment	COTS	Portable and very low installation time	Average
MyDisasterDroid [77]	Few hundred meters	High	COTS	Highly portable & very low installation time	Average
WIISARD [71]	Tens of kilometers	Average	Combination of COTS & proprietary	Portable & low installation time	Average
ARTEMIS [20]	Several hundred kilometers	Low due to satellite subscription	COTS	Highly portable & low installation time	Poor
MEDiSN [17]	Few kilometers	Average	Combination of COTS & proprietery	Portable & average installation time	Average
HYGEIAnet [13]	Thousands of kilometers	Not enough information	No information given	Not enough information	Not available
AID-N [14]	Few hundred kilometers	Average	Mostly Proprietery	Portable & low installation time	Good
MiTag [12]	Few hundred meters	High	COTS	Portable & low installation time	Not available
Integrated System [16]	Several hundred kilometers	Low due to satellite subscription	No information given	No information given	Not available
Patient Monitoring [8], [15]	Tens of kilometers	High	COTS	Portable & low installation time	Not available
MASCAL [70]	Few hundred kilometers	Average	Proprietery geolocation system	Portable & low installation time	Not available
AMON [84]	Tens of kilometers	High	COTS	Highly portable & very low installation time	Average
AMBULANCE [18]	Tens of kilometers	Average	COTS	Highly portable & very low installation time	Not available
Serval BatPhone [63]	Few Kilometers	Low	High if using Mobilephones Low if using Batphone	Highly portable & low installation time	Good

Πίνακας 25. Χαρακτηριστικά ασύρματων συστημάτων έκτακτης ανάγκης [52]

5.2.2 Μη επίγεια δίκτυα

5.2.2.1 Δορυφορικά δίκτυα

Από την πρώτη εκτόξευση δορυφόρου το 1957 έως σήμερα η δορυφορική τεχνολογία έχει εξελιχθεί και έχει επιτύχει σημαντικές καινοτομίες οι οποίες βρίσκουν σήμερα εφαρμογή σε διάφορους τομείς όπως οι τηλεπικοινωνίες, οι στρατιωτικές εφαρμογές, η πρόγνωση του καιρού, η πλοήγηση κ.α. [358]. Ο τομέας της δημόσιας ασφάλειας απαιτεί την απρόσκοπτη επικοινωνία των πρώτων ανταποκριτών ιδιαίτερα σε κρίσιμες καταστάσεις εκτάκτων αναγκών που προκύπτουν από φυσικές ή ανθρωπογενείς καταστροφές. Η δυνατότητα άμεσης χρήσης δορυφορικών επικοινωνιών από το πρώτα κρίσιμα λεπτά καθώς και η αποδοτική λειτουργία των συστημάτων αυτών σε περιοχές όπου είτε δεν καλύπτονται από κάποιο επίγειο δίκτυο είτε έχει καταστραφεί από φυσικές ή άλλες αιτίες τις καθιστούν ως ένα από τα σημαντικότερα και πλέον αξιόπιστα συστήματα υποστήριξης των επικοινωνιών. Τα δορυφορικά συστήματα αποτελούνται από δύο τμήματα, το τμήμα του διαστήματος που περιλαμβάνει τους τεχνητούς δορυφόρους (Satellites) και το επίγειο τμήμα που περιλαμβάνει τους σταθμούς εδάφους (Ground Stations).

5.2.2.1.1 Τμήμα διαστήματος

Στο πλαίσιο της παρούσας εργασίας θα ασχοληθούμε με τρείς κατηγορίες δορυφόρων που παρουσιάζουν ενδιαφέρον ως προς την παροχή κρίσιμων επικοινωνιών. Τους γεωστατικούς δορυφόρους (GEO), τους δορυφόρους ενδιάμεσης τροχιάς (MEO) και τους δορυφόρους χαμηλής τροχιάς (LEO).

i. Οι Γεωστατικοί δορυφόροι (Geostationary Equatorial Orbit- GEO).

Βρίσκονται σε απόσταση 35.786 km από την επιφάνεια της γης και είναι τοποθετημένοι πάνω από τον ισημερινό. Η ταχύτητα τους είναι ίση με την ταχύτητα της γης, γεγονός που εξασφαλίζει τη συνεχή κάλυψη της ίδιας γεωγραφικής περιοχής και την συνεχή ορατότητα στο ίδιο σημείο από το έδαφος. Η διάρκεια ζωής αυτών των δορυφόρων ανέρχεται στα 15 έτη. Τα σημαντικότερα πλεονεκτήματα των γεωστατικών δορυφόρων είναι :

- Παγκόσμια κάλυψη με χρήση μικρού αριθμού δορυφόρων.
- Σταθερή θέση πάνω από συγκεκριμένη γεωγραφική περιοχή (για όλο το 24ωρο), που συνεπάγεται τη διασφάλιση της αδιάλειπτης επικοινωνίας με τον σταθμό εδάφους.
- Δεν απαιτείται η ύπαρξη κινούμενης κεραίας στον σταθμό εδάφους.
- Δεν απαιτεί επιπρόσθετους πολύπλοκους μηχανισμούς για τη διαχείριση των μεταπομπών (handoff) που χρειάζονται οι δορυφόροι ενδιάμεσης και χαμηλής κυκλικής τροχιάς.

Αντίστοιχα, τα μειονεκτήματα που εμφανίζουν είναι:

- Υψηλό κόστος κατασκευής και λειτουργίας λόγω μεγαλύτερου μεγέθους.
- Η λειτουργία σε υψηλότερη τροχιά απαιτεί την χρήση ισχυρότερων πομποδεκτών.
- Απαιτεί πιο προηγμένο τεχνολογικά εξοπλισμό για την διαδικασία της εκτόξευσης.
- Σχετικά μεγάλη καθυστέρηση (latency) από 240 ms έως και 2s που οφείλεται στην απόστασης(δορυφόρου - Γης). Για την αντιμετώπιση του φαινομένου η επιστημονική κοινότητα σχεδίασε νέα πρωτόκολλα μετάδοσης [359].
- Ανάγκη για μεγαλύτερη ισχύ εκπομπής από τους επίγειους σταθμούς (σταθερούς, κινητούς, φορητούς).
- Αυξημένο κόστος των παρεχόμενων υπηρεσιών.

ii. Οι Δορυφόροι Ενδιάμεσης τροχιάς (Medium Earth Orbit-MEO)

Οι μη γεωστατικοί δορυφόροι ενδιάμεσης τροχιάς βρίσκονται σε υψόμετρο 8.000 km έως 20.000 km [358] και χρησιμοποιούνται συνήθως σε συστήματα πλοήγησης όπως το Παγκόσμιο σύστημα εντοπισμού θέσης (GPS). Τα πλεονεκτήματα που εμφανίζουν είναι:

- Για την κάλυψη της γης το σύστημα απαιτεί μόνο δώδεκα δορυφόρους, σε τροχιά ύψους 10.000 km. Ενώ συγκριτικά με τους δορυφόρους χαμηλής τροχιάς, απαιτούνται λιγότεροι για την κάλυψη της ίδιας έκτασης,
- Η ταχύτητα κίνησης τους είναι μικρότερη από αυτή της γης γεγονός που οδηγεί σε πιο απλό σχεδιασμό του συστήματος . (οι δορυφορικές περίοδοι είναι περίπου έξι ώρες).
- Ανάλογα με την κλίση, ένας δορυφόρος ενδιάμεσης τροχιάς (MEO) μπορεί να καλύψει μεγαλύτερους πληθυσμούς, οπότε απαιτούνται λιγότερες μεταπομπές.

Ενώ τα μειονεκτήματά τους:

- Οι δορυφόροι αυτοί λόγω της μεγαλύτερης απόστασης από τους αντίστοιχους της χαμηλής τροχιάς παρουσιάζουν καθυστέρηση (latency) της τάξης των 70–80 ms.
- Οι δορυφόροι χρειάζονται μεγαλύτερη ισχύ εκπομπής και ειδικές κεραίες για μικρότερα αποτυπώματα.

iii. Δορυφόροι χαμηλής τροχιάς (Low Earth Orbit- LEO).

Οι δορυφόροι που βρίσκονται σε απόσταση μικρότερης των 2000 km ανήκουν σε αυτή την κατηγορία. Η τροχιά ενός LEO δορυφόρου είναι συνήθως κυκλική και το ύψος της κυμαίνεται από τα 400km, έως τα 2000 km. Σε αυτές τις τροχιές ο δορυφόρος πραγματοποιεί μια πλήρη περιστροφή γύρω από τη γη κάθε 95min-120min ανάλογα με το ύψος της τροχιάς. Τα σημαντικότερα πλεονεκτήματα τους είναι:

- Μικρότερο κόστος εκτόξευσης για κάθε δορυφόρο

- Μικρή καθυστέρηση (latency) λόγω χαμηλής τροχιάς (50-100 ms, σε υψόμετρο 1200 km)
- Ικανοποιητική λειτουργία με πομποδέκτες μικρότερης ισχύος από τους σταθμούς εδάφους.
- Δεν απαιτεί μεγάλη ισχύ εκπομπής στο τμήμα του δορυφόρου.
- Μικρότερο κόστος παρεχόμενων υπηρεσιών.

Ενώ τα μειονεκτήματα είναι:

- Απαιτεί αρκετά μεγάλο αριθμό δορυφόρων (40-80) για την εξασφάλιση αδιάλειπτης επικοινωνίας σε έξη ή επτά επίπεδα ώστε να υπάρχει παγκόσμια κάλυψη.
- Απαιτεί πιο συχνές μεταπομπές (διαχείριση handoff)
- Η διάρκεια κατά την οποία είναι ορατοί είναι 10-20min ανάλογα με το ύψος της τροχιάς.
- Μικρή διάρκεια ζωής (5-7 έτη) λόγω του ότι 1/3 του χρόνου ζωής του ο δορυφόρος δεν βλέπει τον ήλιο και δεν μπορεί να εκμεταλλευτεί πλήρως την ηλιακή ενέργεια.

Τα δορυφορικά συστήματα Iridium (66 δορυφόροι σε έξι επίπεδα σε υψόμετρο780 km) [359] και Globalstar (48 δορυφόροι σε οκτώ επίπεδα σε υψόμετρο 1414 km) [360] χρησιμοποιούν δορυφόρους χαμηλής τροχιάς για παροχή υπηρεσιών IP τηλεφωνίας και Δεδομένων.

Στους δορυφόρους χαμηλής τροχιάς συναντούμε δυο τύπους ανάλογα με τις υπηρεσίες που προσφέρουν, τους Big και mega-LEOs. Οι πρώτοι λειτουργούν πάνω από τη ζώνη των 2GHz ενώ οι δεύτεροι λειτουργούν στη ζώνη συχνοτήτων από 20-30Ghz. Έτσι οι mega-LEOs διαθέτουν μεγαλύτερη χωρητικότητα γεγονός που τους καθιστά κατάλληλους για μεταδόσεις βίντεο με μικρή καθυστέρηση, κριτήριο που καλύπτει τις σύγχρονες απαιτήσεις των πρώτων ανταποκριτών και συμβαδίζει με τις προδιαγραφές της 3GPP για MC Video μεταδόσεις.

5.2.2.1.2 Επίγειο τμήμα

Τα επίγεια[38] τμήματα ενός δορυφορικού συστήματος επικοινωνιών αποτελούνται από τους:

i. σταθερούς (στη τοποθεσία) τερματικούς σταθμούς.
ii. μεταφερόμενους σταθμούς.
iii. κινητούς-φορητούς σταθμούς.

Οι σταθεροί τερματικοί σταθμοί εγκαθίστανται κοντά στην περιοχή που δραστηριοποιούνται οι πρώτοι ανταποκριτές και είναι σχεδιασμένοι ώστε κατά τη διάρκεια της λειτουργίας τους να παραμένουν ακίνητοι. Χαρακτηριστικό παράδειγμα αυτών των σταθμών αποτελούν οι μικροί τερματικοί σταθμοί που χρησιμοποιούνται σε δίκτυα VSAT (Very Small Aperture

[38] Οι σταθμοί εδάφους υπεύθυνοι για την ανίχνευση, τηλεμετρία, έλεγχο και επιτήρηση των δορυφόρων δεν θεωρούνται ότι ανήκουν στο επίγειο τμήμα [470]

Terminal). Τα VSAT είναι σταθμοί εδάφους με μικρές διαστάσεις κεραιών (από 75cm μέχρι 3m) που μπορούν να μεταφέρουν δεδομένα από και προς τον δορυφόρο με ταχύτητα από 56Kb/s μέχρι και 4Mbit/s. Αρχικά σχεδιάστηκαν για λειτουργία στη ζώνη C (4 & 6 GHz) και αργότερα για τη ζώνη Ku (12 & 14 GHz). Σήμερα έχει επεκταθεί η λειτουργία τους και στη ζώνη Ka. (20 και 31 GHz). [361] Χρησιμοποιούνται για την παροχή πρόσβασης στο διαδίκτυο σε περιοχές που είτε δεν υπάρχει δίκτυο είτε έχει καταστραφεί. Τα VSAT μπορούν επίσης να παρέχουν υπηρεσίες μετάδοσης βίντεο και τηλεφωνίας.

Οι μεταφερόμενοι σταθμοί είναι σχεδιασμένοι ώστε να μπορούν εύκολα να μετακινηθούν σε περιοχές που έχουν πληγεί για την κάλυψη των αναγκών των πρώτων ανταποκριτών. Κατά τη διάρκεια της δορυφορικής επικοινωνίας και αυτοί όπως οι σταθεροί σταθμοί παραμένουν ακίνητοι. [362]. Παραδείγματα του μεταφερόμενου τερματικού είναι δορυφορικά φορτηγά συλλογής ειδήσεων (SGN), τα οποία μετακινούνται σε τοποθεσίες, σταματούν στη θέση τους και στη συνέχεια αναπτύσσουν μια κεραία για να δημιουργήσουν συνδέσμους με τον δορυφόρο.

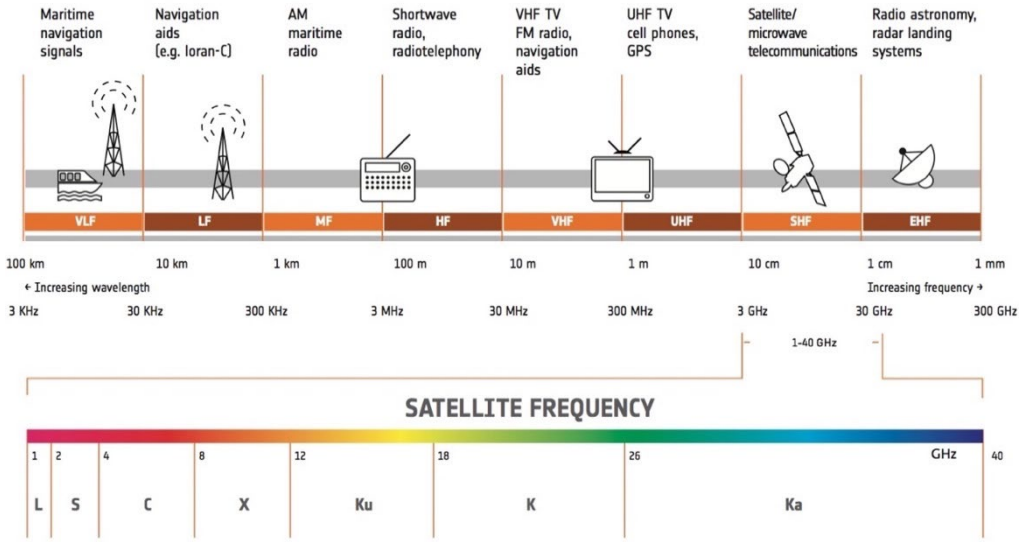
Οι κινητοί σταθμοί έχουν σχεδιαστεί για να επικοινωνούν με τον δορυφόρο ενώ βρίσκονται σε κίνηση. Κατηγοριοποιούνται περαιτέρω ως επίγειοι, αεροναυτικοί ή θαλάσσιοι, ανάλογα με τη θέση τους πάνω ή κοντά στην επιφάνεια της γης. Παραδείγματα αυτών των σταθμών συναντάμε στο ευρυζωνικό παγκόσμιο δίκτυο περιοχής (BGAN) της Inmarsat. Το Ευρυζωνικό Παγκόσμιο Δίκτυο Περιοχής (Broadband Global Area Network - BGAN) προσφέρει σύνδεση φωνής και δεδομένων υψηλής ταχύτητας, μέσω τερματικών που έχουν το μέγεθος ενός φορητού υπολογιστή. Παρέχει ευρυζωνική μετάδοση δεδομένων με ταυτόχρονη μετάδοση φωνής και λειτουργεί στη ζώνη L-(L-band). Στη συγκεκριμένη ζώνη οι επικοινωνίες είναι πιο ανθεκτικές από μεταβολές στις καιρικές συνθήκες. Το BGAN προσφέρει σύνδεση με σταθερή IPστα 490 kbps μέγιστη ταχύτητα και υπηρεσίες με δυνατότητα επιλογής από 32kbps έως 384kbps.

Άλλα σημαντικά του χαρακτηριστικά είναι ότι χρησιμοποιεί κεραίες που αυτόματα εντοπίζουν το δορυφόρο κατά τη διάρκεια κίνησης του οχήματος στο οποίο έχει τοποθετηθεί το τερματικό και ότι λειτουργεί με επαναφορτιζόμενες μπαταρίες. Μάλιστα, αυτά του τα χαρακτηριστικά το κάνουν κατάλληλο για ατομική χρήση, ή για μικρές ομάδες καλύπτοντας τις βασικές ανάγκες επικοινωνίας.

5.2.2.1.3 Ζώνες δορυφορικών συχνοτήτων

Η εξέλιξη της διαστημικής τεχνολογίας και της αεροναυπηγικής οδήγησε στην ανάπτυξη νέων δορυφορικών δικτύων τόσο από κρατικούς οργανισμούς όσο και από ιδιωτικές επιχειρήσεις όπως η SpaceX που ήδη έχει αναπτύξει 1300 δορυφόρους και σχεδιάζει να φτάσει τους 4400 δορυφόρους στα επόμενα χρόνια [363]. Το γεγονός αυτό οδήγησε σε

κορεσμό στη χρήση συχνοτήτων που βρίσκονται στις χαμηλότερες ζώνες τους φάσματος και πλέον με την αξιοποίηση νέων λύσεων αρχίζει σταδιακά να επιτυγχάνεται η αξιοποίηση συχνοτήτων στις υψηλότερες ζώνες του φάσματος.



Εικόνα 122. Οι Ζώνες δορυφορικών συχνοτήτων (πηγή: European Space Agency – ESA)

Στις παρακάτω ζώνες συχνοτήτων περιγράφονται οι υπηρεσίες που χρησιμοποιούνται από κυβερνητικούς και άλλους οργανισμούς δημόσιας ασφάλειας (Εικόνα 122):

i. L-band (1–2 GHz)

Η ζώνη αυτή χρησιμοποιείται από το Παγκόσμιο σύστημα εντοπισμού θέσης, καθώς και για υπηρεσίες δορυφορικής τηλεφωνίας από τις εταιρείες, Iridium και Inmarsat.

ii. S-band (2–4 GHz)

Χρήση σε Ραντάρ καιρού, ραντάρ επιφανείας πλοίων καθώς και από ορισμένους δορυφόρους επικοινωνίας (συγκεκριμένα της NASA για επικοινωνία με τον ISS και το Διαστημικό Λεωφορείο).

iii. C-band (4–8 GHz)

Χρησιμοποιείται και για δορυφορικές επικοινωνίες σε περιοχές που δέχονται τροπικές καταιγίδες διότι αυτή η ζώνη συχνοτήτων επηρεάζεται λιγότερο από την Ku.

iv. X-band (8–12 GHz)

Χρησιμοποιείται κυρίως για στρατιωτικές εφαρμογές όπως διαφόρων τύπου ραντάρ (συνεχών κυμάτων, παλμικών, μονής / διπλής πόλωσης κ.α.). Οι υπό-ζώνες συχνοτήτων χρησιμοποιούνται από πολιτικά, στρατιωτικά και κυβερνητικά ιδρύματα για παρακολούθηση καιρού, έλεγχο εναέριας κυκλοφορίας, έλεγχο κυκλοφορίας θαλάσσιων σκαφών, παρακολούθηση άμυνας και ανίχνευση ταχύτητας οχημάτων για την επιβολή του νόμου.

v. Ku-band (12–18 GHz)

Χρησιμοποιείται για δορυφορικές επικοινωνίες. Στην Ευρώπη, η κάτω ζεύξη(downlink) για την Ku-band πραγματοποιείται στις συχνότητες από 10,7 GHz έως 12,75 GHz για δορυφορικές υπηρεσίες απευθείας μετάδοσης, όπως οι δορυφόροι Astra.

vi. Ka-band (26–40 GHz)

Χρησιμοποιείται από δορυφόρους επικοινωνιών με ανερχόμενη ζεύξη είτε στις ζώνη συχνοτήτων 27.5GHz είτε στη 31GHz καθώς και από υψηλής ανάλυσης ραντάρ μικρής ακτίνας σε στρατιωτικά αεροσκάφη.

5.2.2.1.4 Δορυφορικά Δίκτυα και υπηρεσίες

Σήμερα η ανάπτυξη του 5G και η διασύνδεση του με τα δορυφορικά δίκτυα αποτελεί στόχο της 3GPP η οποία με την πρόσφατη ολοκλήρωση του Release 17 ουσιαστικά έθεσε τις προϋποθέσεις προτυποποίησης ώστε σύντομα επιχειρήσεις και οργανισμοί να σχεδιάσουν αρχιτεκτονικές, υπηρεσίες και συσκευές ώστε να υλοποιηθεί αυτός ο στόχος. Στα τέλη Αυγούστου του 2022 η T-Mobile και η SpaceX ανακοίνωσαν το πρόγραμμα «Coverage Above and Beyond» το οποίο θα παρέχει κάλυψη σε περιοχές χωρίς επίγειο δίκτυο αξιοποιώντας το δορυφορικό δίκτυο της SpaceX. Η υπηρεσία ανακοινώθηκε πως θα τεθεί σε λειτουργία μέσα στο 2023. [364] Λίγες ημέρες αργότερα (Σεπτέμβριος 2022) η Apple με το iPhone14 σε συνεργασία με την GlobalStar εγκαινίασε την υπηρεσία «Emergency SOS» για την αποστολή μηνυμάτων εκτάκτου ανάγκης μέσω δορυφόρων. Η υπηρεσία αυτή αρχικά θα είναι δωρεάν για τα δυο πρώτα χρόνια και θα καλύπτει συνδρομητές σε συγκεκριμένες χώρες [365].

5.2.2.1.5 Τι παρέχει η υπηρεσία «Emergency SOS»

Η ανάπτυξη της υπηρεσίας αυτής από την Apple ουσιαστικά ανοίγει το δρόμο για να αξιοποιηθούν τα δορυφορικά δίκτυα για την αποστολή μηνυμάτων ανάγκης από τους πολίτες όταν βρεθούν σε καταστάσεις ή περιοχές χωρίς επίγεια κάλυψη Εικόνα 123. Μέσω της εφαρμογής, παρέχονται οι παρακάτω δυνατότητες:

- αποστολή μηνύματος εκτάκτου ανάγκης μέσω δορυφόρου
- αποστολής απαντήσεων σε τυπικές ερωτήσεις για την πλήρη αποτύπωση της κατάστασης
- αποστολή του ιατρικού φακέλου του χρήστη (εφόσον διατηρεί ενημερωμένο το medical ID στη συσκευή του)
- Κοινοποίηση της γεωγραφικής θέσης και του υψομέτρου του χρήστη
- την κατάσταση της μπαταρίας του κινητού

- την αποστολή στοιχείων σε τρίτο άτομο από τις επαφές που έχει οριστεί στην εφαρμογή Health
- Κρυπτογράφηση από άκρο σε άκρο

Αυτές οι εμπορικές συνεργασίες από εταιρίες που ηγούνται στον τομέα τους δείχνουν ότι τα επόμενα χρόνια θα υπάρξουν εξελίξεις και στον τομέα της δημόσιας ασφάλειας με δεδομένο ότι τόσο η τεχνολογία, όσο και η τεχνογνωσία υπάρχει. Η εμπορική διάδοση αυτών των υπηρεσιών θα οδηγήσει σταδιακά σε μείωση του κόστους γεγονός από το οποίο οι οργανισμοί δημόσιας ασφάλειας με περιορισμένους συνήθως προϋπολογισμούς θα είναι εφικτό να αξιοποιήσουν.

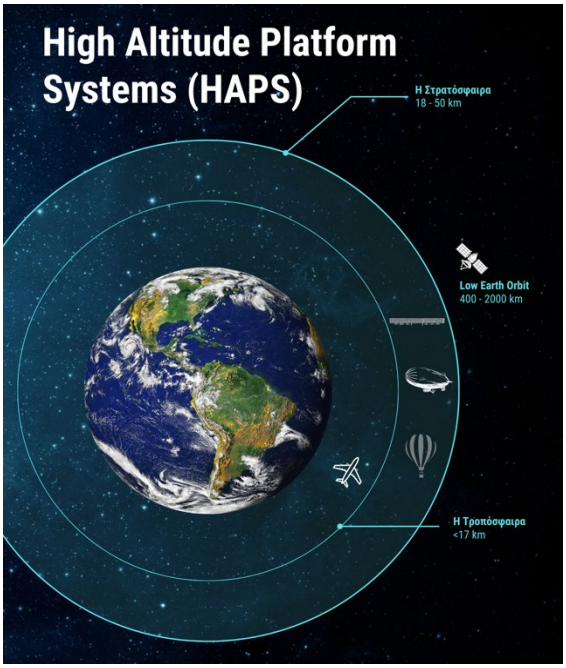
Εικόνα 123. Σύνδεση με το Δορυφόρο και αποστολή μηνύματος (πληροφορίες)

5.2.2.2 Συστήματα Πλατφόρμας Μεγάλου Υψομέτρου

a. Ιστορικό

Η ιδέα της κατασκευής Συστημάτων Πλατφόρμας Μεγάλου Υψομέτρου (High Altitude Platform Stations - HAPS) για χρήση στις τηλεπικοινωνίες γνώρισε μεγάλη απήχηση στη δεκαετία του 1990. Στο Παγκόσμιο Συνέδριο Ραδιοεπικοινωνιών που διοργάνωσε η Διεθνής Τηλεπικοινωνιακή Ένωση (ITU) το 1997, ορίστηκε για πρώτη φορά ο HAPS ως ένα τηλεπικοινωνιακός σταθμός που βρίσκεται σε ένα σταθερό σημείο ως προς τη γη σε απόσταση 20 έως 50 km [366]. Και μπορεί τα τεχνολογικά μέσα στις δεκαετίες 1990 και 2000 να μην οδήγησαν στην ανάπτυξη αυτών των σταθμών παρά τις σημαντικές προσπάθειες αρκετών οργανισμών και επιχειρήσεων, αυτό όμως άλλαξε προσωρινά, όταν το 2014 δυο από τις μεγαλύτερες επιχειρήσεις του διαδικτύου (η Google και η Facebook) ανακοίνωσαν επενδύσεις σε HAPS με στόχο την παροχή πρόσβασης στο διαδίκτυο σε περιοχές που δεν υπήρχε επίγεια υποδομή, γεγονός που αναζωπύρωσε, έστω και προσωρινά[39], το ενδιαφέρον για αυτές τις πλατφόρμες [366].

[39] Η Alphabet (Google) ανακοίνωσε τον τερματισμό του προγράμματος Loon τον Ιανουάριο του 2021 [375]



Εικόνα 124. HAPS στη στρατόσφαιρα

Σήμερα οι τεχνολογικές καινοτομίες στους τομείς των αυτόνομων εναέριων συστημάτων, των κεραιών συστοιχίας (array antennas), σε συνδυασμό με την αύξηση τόσο των επιπέδων απόδοσης των ηλιακών πάνελ όσο και της πυκνότητας ενέργειας των μπαταριών δείχνουν πως οι HAPS θα διαδραματίσουν κύριο ρόλο στα ασύρματα δίκτυα των επόμενων γενεών [367].

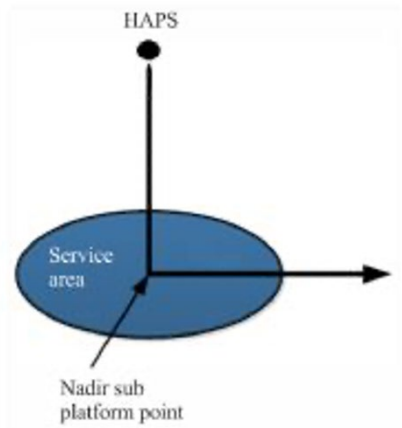
b. Σήμερα

Κύριος στόχος των HAPS, ως προς τις τηλεπικοινωνίες, αποτελεί η λειτουργία τους ως οπισθοζεύκτες (backhaul) των επίγειων δικτύων (για την επέκταση της κάλυψης) σε περιοχές όπου η εγκατάσταση δικτύων οπτικών ινών δεν είναι δυνατή (π.χ. ωκεανοί) [368], ή είναι ασύμφορη οικονομικά. Οι HAPS παρουσιάζουν ιδιαίτερο ενδιαφέρον διότι προσφέρουν μικρότερη καθυστέρηση σήματος (latency), μικρότερη απώλεια ενέργειας (path loss) συγκριτικά με τους δορυφόρους χαμηλής τροχιάς (LEO) [369] και μεγαλύτερη κάλυψη ως προς τους σταθμούς βάσης των επίγειων ασύρματων δικτύων με δυνατότητα απευθείας παροχής υπηρεσιών στους επίγειους χρήστες [370].


Εικόνα 125. Airbus HAPS Zephyr, 2022

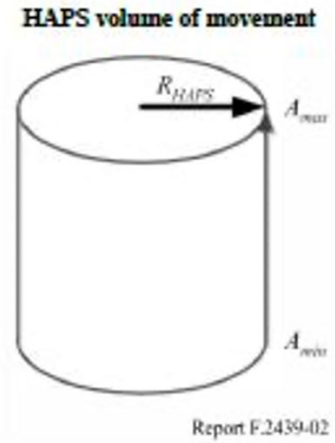
c. Λειτουργία

Οι HAPS αποτελούνται από μια εναέρια πλατφόρμα η οποία ίπταται πάνω από ένα προκαθορισμένο σημείο της γης με σκοπό την παροχή τηλεπικοινωνιακών υπηρεσιών σε χρήστες οι οποίοι βρίσκονται σε μια συγκεκριμένη γεωγραφική περιοχή, η οποία αποτελεί και το αποτύπωμα (footprint) της κάλυψης της πλατφόρμας στο έδαφος (Εικόνα 124, Εικόνα 126).



Εικόνα 126. HAPS. Περιοχή παροχής υπηρεσίων. Πηγή: ITU Report F.2439-01

Οι HAPS επικοινωνούν με τις μόνιμες εγκαταστάσεις του πελάτη (CPE-Customer Premises Equipment) ή με τους σταθμούς - πύλες εισόδου στο έδαφος εντός της περιοχής κάλυψης. Ο HAPS χρησιμοποιεί μία ή περισσότερες συνδέσεις πύλης (feeder links) από διάφορες τοποθεσίες εντός της περιοχής εξυπηρέτησης της πλατφόρμας. Κάθε πλατφόρμα έχει τη δυνατότητα να παρέχει κάλυψη εντός μιας ακτίνας R_{user} από το σημείο ναδίρ (Nadir sub) της υπό-πλατφόρμας όπως απεικονίζεται στο Εικόνα 126. Αυτή η υπό-πλατφόρμα παρέχει συνήθως κάλυψη σε μια μεγάλη περιοχή. Για παράδειγμα, σε υψόμετρο 20 km, μια πλατφόρμα μπορεί να καλύψει ακτίνα έως και 50 km, για γωνίες ανύψωσης (τερματικού σταθμού) μεγαλύτερη των 20 μοιρών στην περιοχή κάλυψης και υπό ορισμένες συνθήκες ακτίνα έως 200 km για γωνίες ανύψωσης (τερματικού σταθμού) μεγαλύτερες των 5 μοιρών.



Εικόνα 127. Υψομετρικά όρια ενός HAPS

Όταν η πλατφόρμα φτάσει στο συγκεκριμένο σημείο της στρατόσφαιρας ,θα παραμείνει για το διάστημα λειτουργίας της εντός των ορίων ενός κυλινδρικού όγκου. Με την πάροδο του χρόνου μπορεί να αλλάξει υψόμετρο, πάντα όμως μέσα σε καθορισμένα όρια, σύμφωνα με την οδηγία RR No. 1.66A. Αυτή η διαδρομή πτήσης μπορεί να αναπαρασταθεί χρησιμοποιώντας έναν κύλινδρο όπως απεικονίζεται στην Εικόνα 127. Η ακτίνα του κυλίνδρου, R_{HAP} είναι η μέγιστη απόσταση από το ονομαστικό κέντρο που θα πετάξει η πλατφόρμα κατά την διάρκεια της παροχής υπηρεσίας. Το A_{min} είναι το ελάχιστο υψόμετρο ενώ το A_{max} είναι το μέγιστο υψόμετρο στο οποίο μπορεί να κινηθεί η πλατφόρμα. Η σχεδίαση του κυλίνδρου μαζί με τις καθορισμένες θέσεις του τερματικού (Fixed Services) στην περιοχή κάλυψης καθορίζουν τη διακύμανση των γεωμετρικών χαρακτηριστικών των Links FS. Ένα γενικό παράδειγμα αυτών των χαρακτηριστικών παρέχεται στον Πίνακας 26.

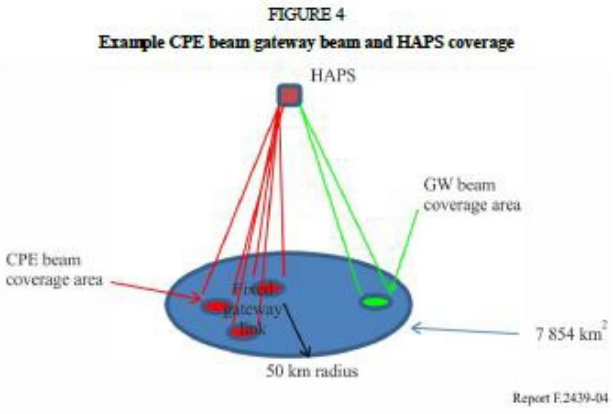
Παράμετροι	Τιμές
R_{user} Ακτίνα εξυπηρέτησης της πλατφόρμας	20 km έως 50 km
A_{min} Ελάχιστο υψόμετρο της πλατφόρμας	20 km
A_{max} Μέγιστο υψόμετρο της πλατφόρμας	26 km
R_{HAPS} Μέγιστη ακτίνα πτήσης της πλατφόρμας	1 έως 5 km

Πίνακας 26. Παράδειγμα γεωμετρικών χαρακτηριστικών της πλατφόρμας

Με τις δυνατότητες των σημερινών τύπων κεραιών όπως adaptive antenna array-AAA και active electronically scanned array-AESA οι HAPS έχουν τη δυνατότητα να σχηματίζουν δυναμικά ακτίνες επικοινωνίας με τους τερματικούς σταθμού των πελατών (CPE) όπως φαίνεται στην Εικόνα 128.

d. Απαιτήσεις

Ο σχεδιασμός των HAPS θα πρέπει να καλύπτει τη δυνατότητα να επιχειρούν από μερικές εβδομάδες έως μήνες φέροντας ταυτόχρονα φορτίο της τάξης των δεκάδων κιλών (kg) στο ιδιαίτερο περιβάλλον της στρατόσφαιρας.



Εικόνα 128. Σενάριο Κάλυψης HAPS - Δυναμικός σχηματισμός ακτίνων εκπομπής

e. Προκλήσεις

Για να επιτευχθούν οι παραπάνω απαιτήσεις θα πρέπει να συντρέχουν κάποιες προϋποθέσεις που λογίζονται ως ανοιχτές προκλήσεις:

i. Να γίνεται αποδοτική χρήση της ηλιακή ενέργειας, λαμβάνοντας υπόψη συγκεκριμένους περιορισμούς:
   - Δυνατότητα αποθήκευσης της, στη διάρκεια της ημέρας σε μπαταρίες ώστε να εξασφαλίζεται η νυχτερινή λειτουργία
   - Σε περιοχές πάνω από τον 35^{o} Βόρειο και κάτω από τον 35^{o} Νότιο μεσημβρινό η ηλιοφάνεια έχει μικρότερη χρονική διάρκεια (γεγονός που θα πρέπει να ληφθεί υπόψη εφόσον ο στόχος είναι η επιχειρησιακή λειτουργία της πλατφόρμας σε όλη τη διάρκεια του έτους σε αυτές τις περιοχές).

ii. Να χρησιμοποιηθούν μπαταρίες υψηλής πυκνότητας, μικρού βάρους, μεγάλης διάρκειας, λαμβάνοντας υπόψη και τις χαμηλές θερμοκρασίες (-60^{o} C) λειτουργίας.

iii. Ιδιαίτερη προσοχή στο σχεδιασμό που θα εξασφαλίζει την μακρόχρονη παραμονή τους στις ατμοσφαιρικές συνθήκες της στρατόσφαιρας. (χαμηλή πυκνότητα του αέρα).

f. Τύποι

Τρείς είναι οι βασικές κατηγορίες των HAPS, τα αεροσκάφη, τα αερόπλοια και τα αερόστατα (Εικόνα 129) [366]. Κάθε μια κατηγορία διαθέτει διαφορετικά χαρακτηριστικά και αντιμετωπίζει διαφορετικές προκλήσεις. Τα αεροπλάνα δαπανούν σημαντική ενέργεια για τη λειτουργία των μηχανών τους. Ενώ τα αερόστατα και τα αερόπλοια είναι ελαφρύτερα από τον αέρα και δεν απαιτείται ενέργεια για την παραμονή τους σε πτήση. Ειδικότερα, τα αερόπλοια διαθέτουν μηχανές γεγονός που τα επιτρέπει να οδηγούνται με ακρίβεια στο επιθυμητό σημείο ώστε να ξεκινήσουν την επιχειρησιακή τους δράση. Αντίθετα τα αερόστατα κινούνται αξιοποιώντας τα ρεύματα του αέρα γεγονός που περιορίζει τις δυνατότητες ελιγμών ακριβείας (π.χ. δυνατότητα για στροφή). Κοινό χαρακτηριστικών και των τριών αυτών κατηγοριών αποτελεί ότι είναι μη επανδρωμένα και πλήρες αυτοματοποιημένα, το οποίο αποτελεί προϋπόθεση για οικονομική λειτουργία και παραμονή στο σημείο της στρατόσφαιρας από όπου επιχειρούν για εβδομάδες ή ακόμη και μήνες [371].

Η επιλογή του συγκεκριμένου υψομέτρου λειτουργίας (~ 17 km) έγινε, λόγω των ευνοϊκών ατμοσφαιρικών συνθηκών που επικρατούν στη στρατόσφαιρα. Σχεδόν όλα τα καιρικά φαινόμενα είναι πιο ήπια αλλά το σημαντικότερο είναι οι χαμηλές ταχύτητες των ανέμων που είναι συγκρίσιμες με αυτές στην επιφάνεια της γης. Μια συγκεντρωτική αποτύπωση των τύπων HAPS και των προκλήσεων που αντιμετωπίζουν παρουσιάζεται στον Πίνακα 27.

Εικόνα 129. Οι τρεις τύποι των HAPS (Αερόστατο, Αερόπλοιο και Αεροσκάφος)

	Αεροσκάφος	Αερόστατο	Αερόπλοιο
Βαρύτερη / Ελαφρύτερη από τον αέρα	Βαρύτερο από τον αέρα	Ελαφρύτερο από τον αέρα	Ελαφρύτερο από τον αέρα
Ικανότητα να στρίβει	Πλήρης	Καθόλου η περιορισμένη	Πλήρης
Πηγή ενέργειας	Ηλιακή Ενέργεια		
Επιχειρησιακό Υψόμετρο	20 km		
Τεχνικές Προκλήσεις	Απαιτείται μεγάλο άνοιγμα φτερών, ευαίσθητη κατασκευή	Περιορισμένη ικανότητα για στροφές, δυσκολία να κατευθυνθεί στην περιοχή από όπου θα επιχειρεί	Μεγάλη υποδομή εδάφους, διαχείριση της θερμότητας

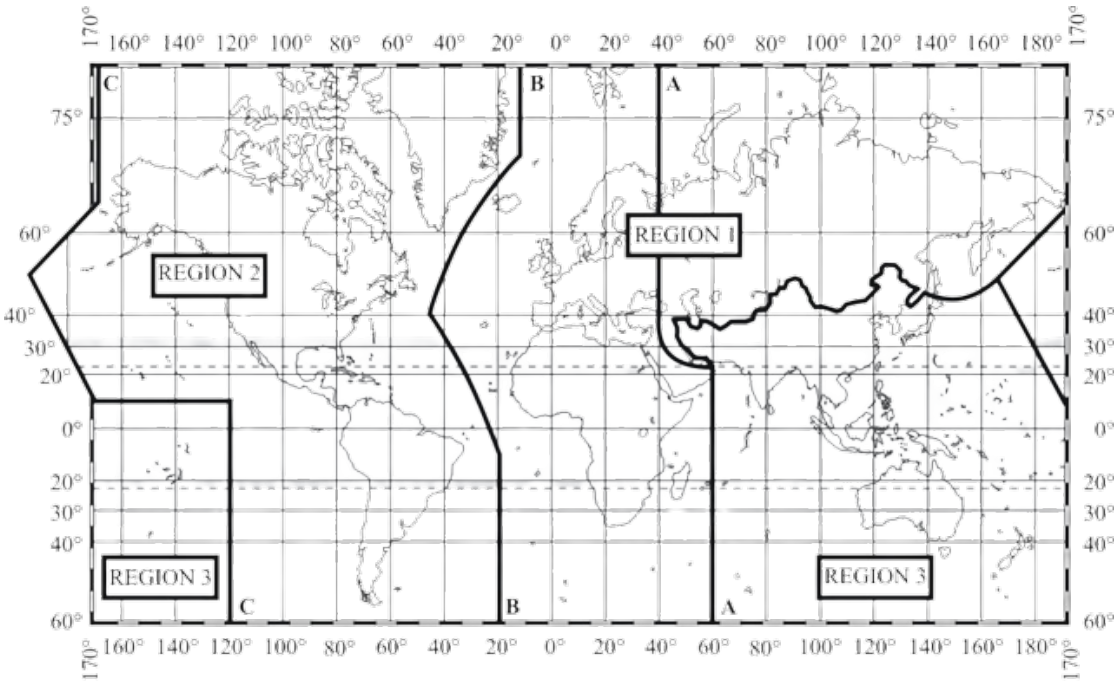
Πίνακας 27. HAPS τύποι και τεχνικές προκλήσεις [371]

g. Οι ζώνες συχνοτήτων

Το φάσμα συχνοτήτων ανά περιοχή (ITU Region) στις οποίες οι HAPS έχουν ήδη καθοριστεί από την ITU καθώς επίσης και αυτές που βρίσκονται στην ατζέντα για συζήτηση στο συνέδριο της ITU του 2023 (WRC-23) παρουσιάζονται συνοπτικά στον Πίνακας 28.

	ITU Region 1	ITU Region 2	ITU Region 3
HIBS Ζώνες συχνοτήτων (RR Res.221)	1885 – 1980 MHz		
	2010 – 2025 MHz		2010 – 2025 MHz
	2110 – 2170 MHz	2110 – 2160 MHz	2110 – 2170 MHz
Ζώνες συχνοτήτων υπό συζήτηση (AI 1.4 στο WRC-23 Res. 247)	694-960 MHz		
	1710-1885 MHz		
	2500 – 2690 MHz		2500 – 2655 MHz

Πίνακας 28. HAPS ζώνες συχνοτήτων



Εικόνα 130. ITU Περιοχές χάρτη 1,2,3 [372]

h. Προτυποποίηση

Οι τεχνολογικές εξελίξεις σε μια σειρά από σημαντικούς για την ανάπτυξη των HAPS τομείς [367] οδήγησαν τόσο την ITU όσο και τον 3GPP στο να επικαιροποιήσουν ή και να καθορίσουν (όπου αυτό δεν είχε συμβεί στο παρελθόν) τα πρότυπα, με στόχο την διασύνδεση τους με τα επίγεια δίκτυα. Συγκεκριμένα, η ITU [372] με τη σύσταση Rec. ITU-R F.2438-0 του 2018 προέβλεψε τη χρήση τους για παροχή ευρυζωνικών υπηρεσιών και παρουσίασε αναλυτικά και τις εκτιμήσεις της για πιθανές εφαρμογές στους τομείς της πολιτικής προστασίας και της δημόσιας ασφάλειας. Επίσης στο Παγκόσμιο συνέδριο του 2023 (WRC-23) της ITU η χρήση των HAPS ως International Mobile Telecommunications (IMT) σταθμών βάσης κινητής τηλεφωνίας γνωστών και ως HIBS (High Altitude platform station as IMT) βρίσκεται ψηλά στα θέματα της ατζέντας. Αντίστοιχα και ο 3GPP με την ολοκλήρωση του Rel. 17 ενσωμάτωσε την υποστήριξη των μη επίγειων δικτύων (NTN) για το 5G στα οποία περιλαμβάνονται και οι HAPS [373].

i. Πλεονεκτήματα των HAPS για τις εφαρμογές Πολιτικής Προστασίας και Δημόσιας Ασφάλειας

Οι εφαρμογές που συναντάμε να υλοποιούν οι πλατφόρμες HAPS έχουν σαφή πλεονεκτήματα και συγκεκριμένα:

- Υποστηρίζουν επιτυχημένα και αποδοτικά έκτακτες καταστάσεις που απαιτούνται ασφαλείς και αδιάλειπτες επικοινωνίες .
- Προσφέρουν μια πλατφόρμα επικοινωνίας για έρευνα και διάσωση, βοηθώντας στην καλύτερη αντίληψη της κατάστασης (Situational awareness) με ενδιάμεσο στόχο την

απόκτηση κοινής επιχειρησιακής εικόνας (Common Operation picture) με τελικό σκοπό τον καλύτερο συντονισμό των ομάδων των πρώτων ανταποκριτών διαφορετικών οργανισμών.

- Παρέχουν δυνατότητα άμεσης αποκατάστασης της διασύνδεσης με το διαδίκτυο κρίσιμων εγκαταστάσεων όπως υδραγωγεία, υποσταθμοί της ΔΕΗ, σιδηροδρομικό δίκτυο βοηθούν στην ταχύτερη επιστροφή στην ομαλότητα εξοικονομώντας παράλληλα σημαντικούς κρατικούς πόρους.
- Αποτελούν έναν εξαιρετικό υποψήφιο για την υποστήριξη αποστολών ανθρωπιστικής βοήθειας γιατί παρέχουν ευρεία κάλυψη περιοχής, από 30 έως 200 km.
- Σε περίπτωση καταστροφής του επίγειου τηλεπικοινωνιακού δικτύου έχουν τη δυνατότητα να παράσχουν υπηρεσίες τηλεφωνίας και πρόσβαση στο διαδίκτυο για πολλές ημέρες σε μεγάλο μέρος του πληθυσμού.
- Όλοι οι πολίτες που βρίσκονται σε κατάσταση ανάγκης μπορούν να αποκτήσουν πρόσβαση στις παραπάνω υπηρεσίες από το κινητό τηλέφωνο που ήδη διαθέτουν, χωρίς να απαιτούνται επιπρόσθετες ρυθμίσεις.
- Η πλατφόρμα μπορεί να βρίσκεται σε ετοιμότητα σε ένα αεροδρόμιο και σε περίπτωση ανάγκης να απογειωθεί άμεσα και τοποθετηθεί πάνω από την πληγείσα περιοχή προσφέροντας ασφαλείς και αξιόπιστες επικοινωνίες. (LTE 4G ή και 5G)
- Προσφέρουν πολύ μεγαλύτερη κάλυψη από τα οχήματα που διαθέτουν σταθμούς βάσης και μπορούν να καλύψουν δύσβατες περιοχές ή όπου έχει υποστεί καταστροφές το οδικό δίκτυο.
- Έχει επίσης τη δυνατότητα να λειτουργήσει ως σύστημα έγκαιρης προειδοποίησης , αποστέλλοντας μαζικά SMS σε πολίτες που βρίσκονται στις πληγείσες περιοχές και τα δίκτυα κινητής τηλεφωνίας έχουν καταστραφεί.
- Μπορεί να χρησιμοποιηθεί σε αποστολές επιτήρησης και έγκαιρης ανίχνευσης πυρκαγιών με χρήση αισθητήρων (θερμικές κάμερες κλπ.)
- Μπορεί επίσης να χρησιμοποιηθεί συμπληρωματικά της υπάρχουσας αρχιτεκτονικής διαχείρισης επικοινωνιών ανάγκης ώστε να τη βελτιώσει, αυξάνοντας τις επιχειρησιακές της δυνατότητες.
- Εξασφαλίζουν την ανθεκτικότητα του δικτύου παρέχοντας υπηρεσίες από την στρατόσφαιρα χωρίς να διατρέχουν κίνδυνο καταστροφής από φυσικές καταστροφές όπως σεισμοί, πλημμύρες και πυρκαγιές.
- Παρέχουν τρισδιάστατη κάλυψη μιας μεγάλης γεωγραφικής περιοχής με δυνατότητες απομακρυσμένης διαχείρισης σμήνους εναέριων μη επανδρωμένων συστημάτων (UAVs) [371]
- Έχουν χαμηλότερο κατασκευαστικό και λειτουργικό κόστος συγκριτικά με τους δορυφόρους.

- Έχουν αποδεδειγμένες επιχειρησιακές δυνατότητες στο πεδίο. Χρησιμοποιήθηκαν με επιτυχία στις καταστροφές που πραγματοποιήθηκαν στο Πουέρτο Ρίκο το 2017 και στο Περού το 2019 [374].

j. Τα μειονεκτήματα των HAPS

Η αποτυχημένη έως σήμερα πορεία μεγάλων project στον τομέα των HAPS όπως το Loon της Alphabet (Google) το οποίο τερματίστηκε το 2021 έδειξε πως δεν είναι δυνατή η οικονομική βιωσιμότητα τους [375]. Όμως η επιστήμη και η τεχνολογία προχωρούν με γρήγορους ρυθμούς και το έντονο ενδιαφέρον από οργανισμούς όπως η ITU, ο 3GPP, η GSMA η οποία μάλιστα προτείνει [376] στα μέλη της (Τηλεπικοινωνιακοί πάροχοι) να στηρίξουν τα projects της HAPS Alliance δείχνουν πως όχι μόνο δεν έκλεισε ο κύκλος αλλά μάλλον τώρα ανοίγει. Ο Πίνακας 29 παρουσιάζει τα συγκριτικά πλεονεκτήματα των HAPS έναντι των δορυφόρων οι οποίοι βρίσκονται και αυτοί σε ανοδική τροχιά, τόσο από επιστημονικό όσο και τεχνολογικό (επενδυτικό) ενδιαφέρον.

		Αριθμός Δορυφόρων για παγκόσμια κάλυψη	Χρονική διάρκεια μια πλήρους τροχιάς (Ώρες)	Χρόνος παραμονής σε ορατότητα από το ίδιο επίγειο σημείο	Καθυστέρηση: RTT (ms)	Βάρος (Kg)	Διάρκεια ζωής (έτη)
Παγκόσμια κάλυψη	**GEO**	**3**	**24**	**Πάντα**	**600-700**	**~3500**	**15**
	MEO	**10-30**	**5-12**	**2-4 Ώρες**	**<150**	**~700**	**12**
	LEO	**100+**	**1.5**	**15 λεπτά**	**<50**	**5 – 1000**	**<5-7**
Στοχευμένη / Τοπική Κάλυψη	**HAPS**	**1 αεροσκάφος ~ 12 731 Km² (70 km ακτίνα)**		**Πάντα**	**<10**	**<320 (Αερόστατο) <100 (Αεροσκάφος)**	**>5 (Αερόστατο) >8 (Αεροσκάφος)**

Πίνακας 29. Συγκριτικά χαρακτηριστικά των Non Terrestrial Networks (Δορυφόροι και HAPS)

k. Σημαντικές εταιρείες

Οι παρακάτω εταιρείες δραστηριοποιούνται στον τομέα ανάπτυξης και λειτουργίας των HAPS σήμερα με συγκεκριμένες πλατφόρμες, εξυπηρετώντας ανάγκες τηλεπικοινωνιών αλλά και στρατιωτικών εφαρμογών.

- Airbus (Zephyr, 5G υποστήριξη ιδιωτικών τηλεπικοινωνιακών δικτύων) [377]
- Lockheed Martin (Martin Stalker VXE UAS) [378]
- Tao Group (SkyDragon) [379]
- RosAeroSystems (Berkut) [380]
- Thales (Stratobus) [381]

l. Αρχιτεκτονική επέκτασης ενός δικτύου PPDR σε καταστάσεις εκτάκτων αναγκών

Η παρακάτω αρχιτεκτονική αξιοποιεί τις πλατφόρμες HAPS οι οποίες φέρουν τηλεπικοινωνιακό εξοπλισμό σύμφωνα με τα πρότυπα του 3GPP LTE 4G/5G παρέχοντας αξιόπιστες ευρυζωνικές επικοινωνίες στους πρώτους ανταποκριτές. Το δίκτυο αποτελείται:

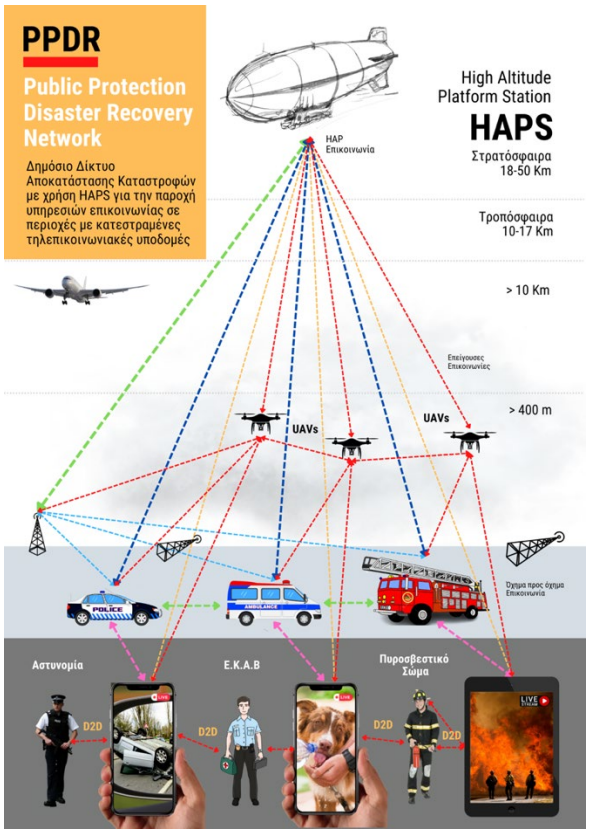
i. Από την πλατφόρμα (HAPS) που παρέχει ευρυζωνικές επικοινωνίες (LTE 4G/5G/6G) τόσο ως σταθμός βάσης για οπισθοζεύξη (σύνδεση με επίγειο σταθμό του πάροχου) όσο και ως πύλη με απευθείας σύνδεση με τη συσκευή του πρώτου ανταποκριτή.

ii. Τα UAVs τα οποία μπορούν να επιχειρούν ως:
   - Relay, λειτουργία αναμεταδότη σήματος στον εξοπλισμό του χρήστη (UEs)
   - να τηλεχειρίζονται απομακρυσμένα από την πλατφόρμα

iii. Τους τερματικούς σταθμούς στα οχήματα με δυνατότητες
   - ProSe επικοινωνία συσκευή προς συσκευή χωρίς να απαιτείται base station (BS)
   - Relay, λειτουργία αναμεταδότη σήματος στον εξοπλισμό του χρήστη

iv. Τον εξοπλισμό του χρήστη (UE)
   - Έξυπνα κινητά τηλέφωνα
   - Tablet
   - Ένδυτα μέσα

Τα σημαντικότερα πλεονεκτήματα της συγκεκριμένης αρχιτεκτονικής αποτελούν η άμεση κάλυψη περιοχών στις οποίες έχει υποστεί βλάβες το επίγειο δίκτυο καθώς επίσης η δυνατότητα παροχής ευρυζωνικών υπηρεσιών στους πρώτους ανταποκριτές οι οποίοι μπορούν να επικοινωνούν μεταξύ τους ανεξάρτητα από την υπηρεσία στην οποία υπηρετούν.



Εικόνα 131. Χρήση HAPS σε περιοχή με μερικώς κατεστραμμένη επικοινωνιακή υποδομή. LTE, 5G, NR, 3GPP, Rel,17 (NTN)

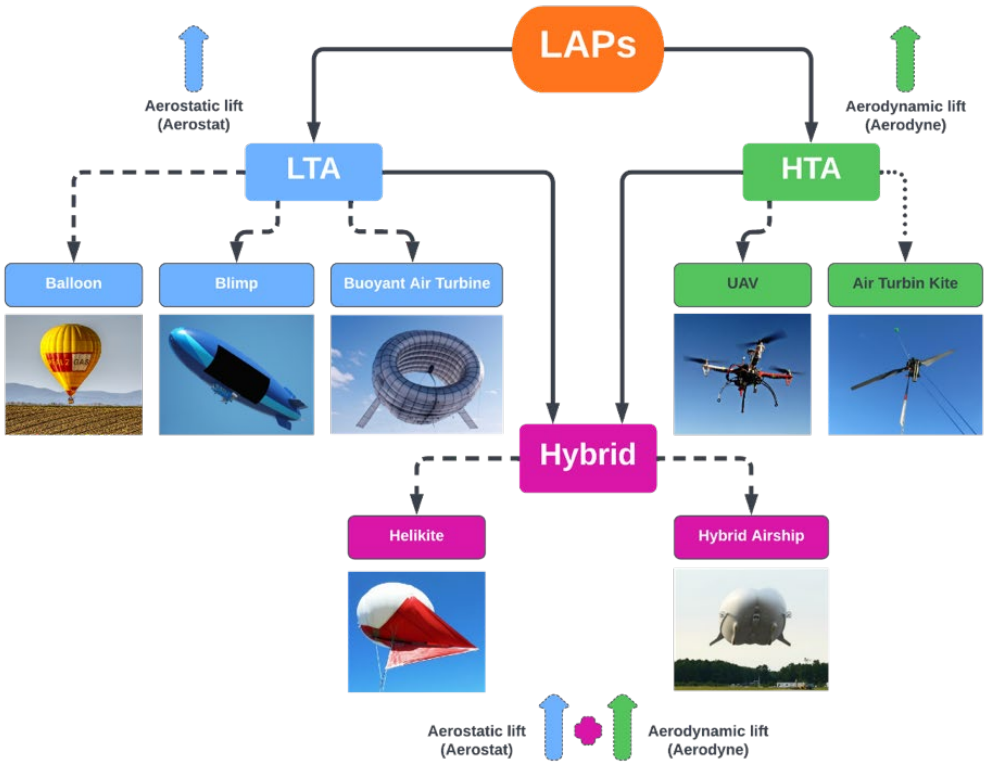
5.2.2.3 Συστήματα Πλατφόρμας Χαμηλού Υψομέτρου

Οι πλατφόρμες χαμηλού υψομέτρου (Low Altitude Platform Systems - LAPs) είναι εναέρια συστήματα τα οποία επιχειρούν σε υψόμετρο 100m έως 6km [382], [383], παρέχοντας ποικίλες υπηρεσίες με διαφορετικές εφαρμογές σε καταστάσεις έκτακτης ανάγκης.

5.2.2.3.1 Κύριοι τύποι

Οι κύριοι τύποι αυτών των συστημάτων κατηγοριοποιούνται ως εξής [383] (Εικόνα 132):

- Ελαφρύτερα του αέρα (Lighter Than Air-LTA) όπως τα
  - ❖ Αερόστατα
  - ❖ Αερόπλοια (Blimp)
  - ❖ Πνευστοί Αεροστρόβιλοι (Buoyant Air Turbine)
- Βαρύτερα του αέρα (Heavier Than Air -HTA) όπως τα
  - ❖ Μη επανδρωμένα UAVs
  - ❖ Air Turbine Kite
- Υβριδικά τα οποία συνδυάζουν χαρακτηριστικά από τις παραπάνω κατηγορίες και είναι τα:
  - ❖ Helikite
  - ❖ Hybrid Airship



Εικόνα 132. Διαφορετικοί τύποι LAPs [383]

Τα χαρακτηριστικά αυτών είναι:

a. LAPS – LTA

Οι πλατφόρμες αυτές γεμίζουν το φάκελο τους με αέριο (π.χ. ήλιο) μικρότερης πυκνότητας από την ατμοσφαιρική. Η διαφορά μεταξύ της πυκνότητας του αέρα έξω από το περίβλημα του αερόστατου και της πυκνότητας του αερίου στο εσωτερικό του, παράγει την άνωση σύμφωνα με την αρχή του Αρχιμήδη. Τα πιο δημοφιλή αυτής της κατηγορίας είναι τα αερόστατα και τα αερόπλοια.

b. Τα αερόστατα (balloons)

Αποτελούν τον ποιο συνηθισμένο τύπο που χρησιμοποιείται ως πλατφόρμα χαμηλού υψομέτρου λόγου του ότι είναι εύκολα στο να κατασκευαστούν και το κόστος τους παραμένει χαμηλό συγκριτικά με άλλα προσδεδεμένα αερόστατα. Επίσης είναι εύκολη και η ανάπτυξη τους στο πεδίο. Το επιχειρησιακό τους ύψος βρίσκεται στα 600-700m ενώ το μέγιστο ωφέλιμο φορτίο τους ανέρχεται περίπου στα 50kg. Ωστόσο ο συγκεκριμένος τύπος δεν είναι σχεδιασμένος για αντοχή σε ισχυρούς ανέμους. Αερόστατα τα οποία είναι προσδεδεμένα μπορούν να λειτουργήσουν με ανέμους των 20km/h έως 40km/h μέγιστης ταχύτητας (Εικόνα 133.1).

c. Τα αερόπλοια (blimps)

Αντίθετα, τα αερόπλοια (Εικόνα 133.2) έχουν σχεδιαστεί ώστε να μπορούν να επιχειρούν με υψηλές ταχύτητες αέρα μεταφέροντας μεγαλύτερο ωφέλιμο φορτίο, παραμένοντας σταθερά πάνω από την επιθυμητό σημείο και σε μεγαλύτερο υψόμετρο. Μια από τις πρωτοπόρες εταιρείες κατασκευής αερόπλοιων η TCOM τα ταξινομεί σε τρείς ακόμη επιμέρους κατηγορίες με βάση συγκεκριμένα χαρακτηριστικά. Οι διάφορες κατηγορίες είναι:

- Τακτική (Tactical): τα συγκεκριμένα αερόπλοια είναι μικρά και μπορούν να αναπτυχθούν σε πολύ μικρό χρονικό διάστημα. Το περίβλημα τους έχει διαστάσεις από 12 έως 17m και είναι κατάλληλα για επιχειρήσεις επιτήρησης περιοχής. Μπορούν να επιχειρούν σε υψόμετρο 300m με ωφέλιμο φορτίο 27kg και ταχύτητα ανέμου έως 100km/h. Η μέγιστη διάρκεια παραμονής τους στον αέρα είναι επτά ημέρες.
- Λειτουργική (Operational): η συγκεκριμένη κατηγορία διαθέτει περίβλημα μεσαίων διαστάσεων που κυμαίνονται από 22 έως 28m.Συνδυάζουν φορητότητα και ευελιξία για γρήγορη ανάπτυξη στο πεδίο και γρήγορη επανατοποθέτηση για μεταφορά. Κατάλληλα για επιτήρηση επιχειρήσεων τόσο σε στεριά όσο και θάλασσα καθώς επίσης και για την επιτήρηση των συνόρων. Μπορούν να αιωρούνται έως δυο εβδομάδες και με ταχύτητες ανέμων έως 130km/h.

- Στρατηγική (Strategic): Σε αυτή την κατηγορία τα αερόστατα διαθέτουν περίβλημα από 71 έως 78m με δυνατότητα ανύψωσης ωφέλιμου φορτίου 2300kg. Ιδανικά για παρακολούθηση και επιτήρηση επιχειρήσεων με δυνατότητα παραμονής στον αέρα για 30 ημέρες και αντοχής σε ανέμους ταχύτητας έως 166km. Επιχειρούν ακόμη και από ύψος 4.6km επιτρέποντας την κάλυψη μιας πολύ μεγάλης περιοχής.

Διάρκεια Πτήσης		**7 ημέρες**	**14 ημέρες**	**30 ημέρες**
Υψόμετρο	**Κατηγορία**	-	-	71m -74m
5km	Στρατηγική			
1km	Λειτουργική	-	22m-28m	-
300m	Τακτική	12m-17m	-	-
Φορτίο		27kg	200kg	2300kg
Ταχύτητες Ανέμου		74km/h -100km/h	92km/h – 130km/h	130km/h – 166km/h

Πίνακας 30. Κατηγορίες (TCOM) αερόπλοιων

d. Πνευστοί αεροστρόβιλοι (Buoyant Airborne Turbines – BATs)

Είναι τουρμπίνες αέρος κατασκευασμένες από την εταιρεία Altaeros [384] οι οποίες μπορούν να επιχειρούν σε υψόμετρο 600m παράγοντας διπλάσια ποσότητα ενέργειας σε σύγκριση με τις ανεμογεννήτριες που είναι εγκατεστημένες στο έδαφος. Το εσωτερικό τους αέριο είναι το ήλιο και είναι προσδεμένες στο έδαφος κατά τη διάρκεια μεταφοράς της ενέργειας στο σταθμό εδάφους (Εικόνα 133.3).

e. Οι πλατφόρμες HTA

Χρησιμοποιούν τη δύναμη της ώθησης για να ξεπεράσουν τη δύναμη της αντίστασης του αέρα και μόλις η δύναμη της ανύψωσης ξεπεράσει τη δύναμη της βαρύτητας εξαιτίας της αεροδυναμικής κλίσης των πτερύγων (αρχή του Bernoulli) η πλατφόρμα αιωρείται. Οι πιο δημοφιλείς πλατφόρμες είναι τα προσδεδεμένα UAV (tUAV) και οι αερομεταφερόμενοι χαρταετοί τουρμπίνας.

f. Προσδεμένα UAVs (tethered UAVs - tUAVs)

Είναι μη επανδρωμένα εναέρια οχήματα τα οποία είναι προσδεμένα με το έδαφος ώστε να τροφοδοτούνται και να ανταλλάσσουν δεδομένα. Επιχειρούν σε ύψος έως 200mκαι μπορούν να μεταφέρουν ωφέλιμο φορτίο 15kg. Επίσης διαθέτουν μπαταρία σε περίπτωση που το καλώδιο διακοπεί ή καταστραφεί ώστε να μπορέσουν να προσγειωθούν με ασφάλεια. Θεωρητικά εφόσον υπάρχει αδιάλειπτη τροφοδοσία το UAV μπορεί να επιχειρεί για μέρες. Στη πράξη ωστόσο, υπάρχει ο περιορισμός της θερμοκρασίας των κινητήρων του που δεν μπορεί να ξεπεράσει τις δύο ή κατά μέγιστο τις τέσσερις ημέρες.

g. Airborne Turbine kite

Είναι ανεμογεννήτριες που τοποθετούνται σε μεγάλο υψόμετρο όπου η ταχύτητα του αέρα είναι μεγαλύτερη (Εικόνα 133.4). Με αυτό τον τρόπο επιτυγχάνουν καλύτερες αποδόσεις από τις επίγειες και το κόστος κατασκευής τους είναι χαμηλότερο. Ο ηλεκτρικός κινητήρας

μπορεί να είναι επίγειος (στο έδαφος) ή εναέριος (να ίπταται). Το καλώδιο μεταδίδει την ενέργεια που έχει συλλεχθεί στο έδαφος. Αυτές οι ανεμογεννήτριες μπορούν να αιωρούνται σε μικρό ή μεγάλο ύψος και έως 4600m. [385] [386]

h. Υβριδικές πλατφόρμες

Αυτές χρησιμοποιούν τόσο τη στατική όσο και τη δυναμική άνοδο βασισμένες στις αρχές του Αρχιμήδη και Bernoulli αντίστοιχα για την αιώρηση τους. Δύο είναι αυτές με τη συχνότερη χρήση, τα Helikites και τα υβριδικά αερόπλοια

i. Helikites

Αυτά είναι υβριδικά αερόστατα (Εικόνα 133.5) που χρησιμοποιούν τόσο τη στατική όσο και τη δυναμική άνοδο. Η λέξη Helikites προκύπτει από τη σύνθεση των λέξεων ήλιο και χαρταετός. Η κατοχύρωση της πατέντας τους πραγματοποιήθηκε το 1993 από την εταιρεία Sandy Allsopp40. Ένα Helikite αποτελείται από ένα σφαιροειδές μπαλόνι το οποίο περιέχει ήλιο ώστε να παρέχει την στατική άνοδο, και μια δομή χαρταετού ώστε να εξασφαλίσει την δυναμική άνοδο. Ο συνδυασμός αυτών των δυο μειώνει την απαιτούμενη ποσότητα ηλίου που απαιτείται σε σύγκριση με τα αντίστοιχου μεγέθους αερόστατα, εξασφαλίζοντας στο Helikite τη δυνατότητα να πετά σε μεγαλύτερα υψόμετρα από αντίστοιχα άλλα αερόστατα του ίδιου μεγέθους. Επίσης διαθέτουν συγκριτικά πλεονεκτήματα και από τις άλλες πλατφόρμες όπως:

- Συμπαγείς σχεδιασμός που τα επιτρέπει να αναπτυχθούν με μικρότερο προσωπικό.
- Δεν υπάρχει κίνδυνος πτώσης από ισχυρούς ανέμους διότι με το σχεδιασμό που διαθέτει οι άνεμοι το βοηθούν να παραμείνει στον αέρα.
- Διαθέτουν μικρότερο μέγεθος με λιγότερες πιθανότητες διαρροής ήλιου και χρησιμοποιούν μικρότερη ποσότητα ήλιο χάρη στον αεροδυναμικό τους σχεδιασμό.

Επίσης μπορούν να παραμείνουν στον αέρα για δυο εβδομάδες σε υψόμετρο 1.5km μεταφέροντας βάρος 23kg. Σύμφωνα με τα δημοσιευμένα στοιχεία της εταιρίας η σειρά Desert Star Helikites μπορεί να φέρει φορτίο 220kg σε υψόμετρο 3.4km. [387]

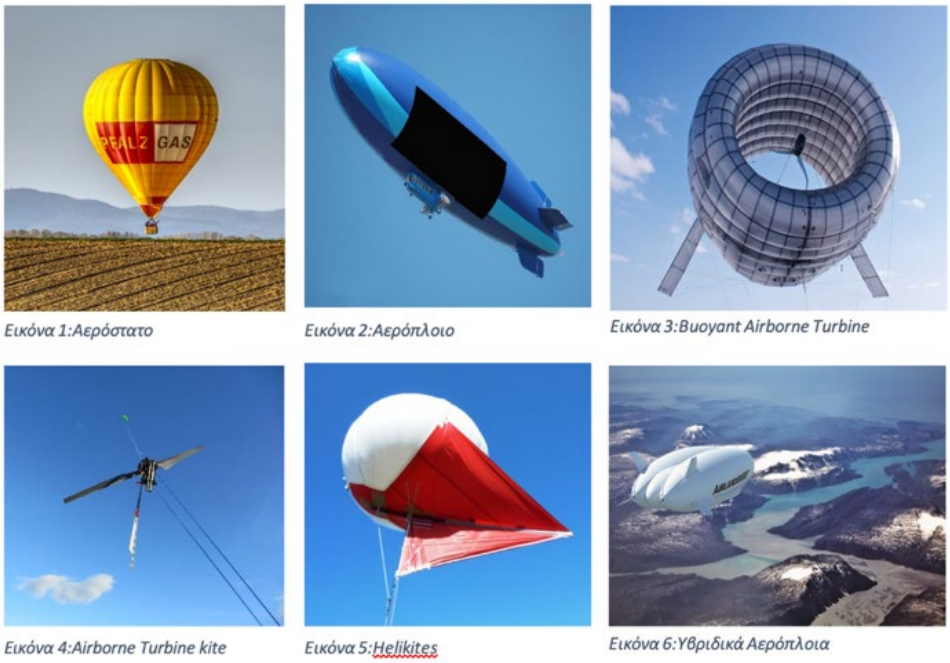
j. Υβριδικά Αερόπλοια

Είναι υβριδικά αεροσκάφη (Εικόνα 133.6) που το 60% της ανύψωσης τους προέρχεται με στατικό και το υπόλοιπο 40% από δυναμικό τρόπο. Τα υβριδικά αερόπλοια δεν χρειάζονται αεροδρόμια και μπορούν να απογειωθούν και να προσγειωθούν από οποιαδήποτε ανοιχτή τοποθεσία. Μπορούν να επιχειρήσουν από μέγιστο υψόμετρο τα 6km φέροντας φορτίο 50.000kg. Αν και η κύρια χρήση τους είναι η μεταφορά επιβατών και βαρειών εμπορευμάτων οι πλατφόρμες αυτές μπορούν χρησιμοποιηθούν και για άλλες εφαρμογές ακόμη και ως προσδεμένες σε συγκεκριμένο σημείο. Η λειτουργία τους εκτιμάται ότι θα ξεκινήσει το 2026. [388]

[40] Allsopps UK Patent No.2280381 and US Patent No.6016998A

Ιδιότητες	UAVs	Balloons	Helikite	Blimps	BATs
Φορτίο	1-15kg	5-50kg	2-25 kg	16-2600kg	Μ/Δ
Υψόμετρο	150-200m	150-700m	100m-1.5km	100m-5km	150-600m
Ταχύτητα Ανέμου	40-55km/h	20-40km/h	90km/h	75-165km/h	160km/h
Διάρκεια πτήσης	2-4 ημέρες	1-7 ημέρες	2-4 ημέρες	1-30 ημέρες	Μ/Δ
Χρόνος Ανάπτυξης	Γρήγορος	Μέτριος	Γρήγορος	Αργός	Γρήγορος
Κόστος	Χαμηλό/Μεσαίο	Χαμηλό/Μεσαίο	Χαμηλό/Μεσαίο	Μεσαίο/Υψηλό	Μ/Δ

Πίνακας 31. Συγκριτικά χαρακτηριστικά LAPs



Εικόνα 1:Αερόστατο
Εικόνα 2:Αερόπλοιο
Εικόνα 3:Buoyant Airborne Turbine
Εικόνα 4:Airborne Turbine kite
Εικόνα 5:Helikites
Εικόνα 6:Υβριδικά Αερόπλοια

Εικόνα 133. Διάφορα είδη LAPs

5.2.2.3.2 Εφαρμογές των LAPs στη δημόσια ασφάλεια και στην αποκατάσταση καταστροφών.

Οι εφαρμογές των LAPs στη δημόσια ασφάλεια και στην αποκατάσταση καταστροφών είναι:

- Αποστολές Έρευνας και Διάσωσης
- Αποστολές Δασοπυρόσβεσης και επιτήρησης δασικών εκτάσεων
- Επείγουσες Επικοινωνίες
- Διαχείριση και έλεγχος πλήθους
- Εναέριες Επιτηρήσεις
- Κυκλοφοριακή διαχείριση, Διαχείριση ατυχημάτων, Παρακολούθηση οχημάτων.

Αναλυτικά οι LAPs μπορούν να υποστηρίξουν τις παραπάνω αποστολές.

- Έρευνα και διάσωση: Η υπηρεσίες που μπορούν να προσφέρουν είναι εναέρια επιτήρηση με δυνατότητα κάλυψης μεγάλων περιοχών που δεν διαθέτουν επίγειο δίκτυο (μετάδοση βίντεο σε πραγματικό χρόνο στο κέντρο επιχειρήσεων),

τηλεπικοινωνιακή υποστήριξη τόσο στους πρώτους ανταποκριτές (επέκταση του σήματος) όσο και στους αγνοούμενους πολίτες. 76-79

- Δασοπυρόσβεση και επιτήρηση δασικών εκτάσεων: Οι LAPs παρέχουν όχι μόνο τηλεπικοινωνιακή κάλυψη στους δασοπυροσβέστες αλλά με τη χρήση υπέρυθρων καμερών δημιουργούν χάρτες θερμοκρασίας ώστε να εντοπιστούν και να αναγνωριστούν οι εστίες της πυρκαγιάς. Με αυτό τον τρόπο το κέντρο επιχειρήσεων μπορεί να πάρει κρίσιμες αποφάσεις για την έγκαιρη αντιμετώπιση της πυρκαγιάς δίνοντας τις κατάλληλες εντολές στο προσωπικό που βρίσκεται στο πεδίο.70-80.
- Επείγουσες επικοινωνίες: Σε μεγάλες φυσικές καταστροφές όπως τσουνάμι, σεισμοί, πλημμύρες ή τυφώνες που μπορούν να προκαλέσουν σημαντικές ζημιές στο επίγειο δίκτυο τηλεφωνίας καταστρέφοντας πυλώνες η δυνατότητα ταχείας αποκατάστασης των υπηρεσιών κινητής τηλεφωνίας και πρόσβασης στο διαδίκτυο είναι πρωτεύουσας σημασίας. Οι LAPs μπορούν να αναπτυχθούν σε σύντομο χρονικό διάστημα καλύπτοντας τις πληγείσες περιοχές ,εξασφαλίζοντας τις επικοινωνίες των διασωστικών συνεργείων συντελώντας στο να ληφθούν κρίσιμες αποφάσεις. Επίσης βοηθούν στην αναγνώριση και ιεράρχηση των περιοχών που έχουν επηρεαστεί από την καταστροφή.
- Διαχείριση και έλεγχο πλήθους: Ιδιαίτερα χρήσιμες σε αποστολές διαχείρισης πλήθους και διαδηλώσεων παρέχοντας σε πραγματικό χρόνο εικόνα από το πεδίο με στόχο να ληφθούν σημαντικές αποφάσεις για το συντονισμό των επίγειων δυνάμεων και την αποκατάσταση της τάξης.
- Εναέρια επιτήρηση: Λόγω του υψομέτρου από το οποίο επιχειρούν οι LAPs είναι κατάλληλες για αποστολές επιτήρησης συνόρων, παράνομης αλιείας, προστασίας του περιβάλλοντος.
- Κυκλοφοριακή διαχείριση, Διαχείριση ατυχημάτων, Παρακολούθηση οχημάτων: Με τη χρήση των LAPs οι αρμόδιες υπηρεσίες μπορούν να λαμβάνουν καλύτερες αποφάσεις για την διαχείριση του κυκλοφοριακού προβλήματος, ενημερώνοντας παράλληλα τους πολίτες για την κατάσταση της κυκλοφορίας στο οδικό δίκτυο ή για τυχόν ατυχήματα σε πραγματικό χρόνο ώστε να αποφευχθεί η υπερσυγκέντρωση των οχημάτων. Οι πλατφόρμες επίσης μπορούν να εντοπίσουν οχήματα που καταδιώκονται από τις αρχές και να παρέχουν στις αρμόδιες υπηρεσίες πληροφορίες για την ακριβή τους θέση.

5.2.2.3.3 Πλεονεκτήματα και μειονεκτήματα των LAPs

Στα πλεονεκτήματα των LAPs εντάσσονται:

- Αποδοτικά ως προς το κόστος

- Αντοχή και ανθεκτικότητα
- Φιλικές προς το περιβάλλον
- Ευρεία κάλυψη περιοχής
- Χωρητικότητα Οπισθοζεύξης (Backhaul)
- Ταχεία Ανάπτυξη
- Συνεχή Τροφοδοσία
- Ανεπηρέαστες από καιρικές συνθήκες
- Μεγάλο ωφέλιμο φορτίο

Ασφάλεια Εξειδικεύοντας κάθε ένα από τα πλεονεκτήματα παρατίθενται συνοπτικά τ' ακόλουθα:

- Αποδοτικά ως προς το κόστος: Οι LAPs είναι αποδοτικότερες ως προς το κόστος συγκρινόμενες με ελεύθερα κινούμενες ιπτάμενες πλατφόρμες (ΕΚΙΠ) ή με άλλες τηλεπικοινωνιακές υποδομές όπως επίγειοι πύργοι ή δορυφόροι. Επίσης διαθέτουν και χαμηλότερο λειτουργικό κόστος συγκριτικά με τις ΕΚΙΠ. Για παράδειγμα έχουν χαμηλότερο κόστος αγοράς, συντήρησης και υποστήριξης συγκριτικά με τις ελεύθερα ιπτάμενες πλατφόρμες. Επιπρόσθετα απαιτούν μικρότερο χρόνο εκπαίδευσης για την λειτουργία και μικρότερο αριθμό χειριστών. Συγκρινόμενες με τους πύργους το κόστος ανάπτυξης τους είναι δέκα φορές χαμηλότερο από την ανέγερση ενός τηλεπικοινωνιακού πύργου. Επίσης η τηλεπικοινωνιακή κάλυψη που παρέχουν οι LAPs σε υψόμετρο 250m είναι ίση με την κάλυψη που αντιστοιχεί από 14 πύργους ύψους 40-60m. Η ενεργειακή κατανάλωση των πύργων τόσο σε ρεύμα όσο και σε καύσιμο είναι πολύ μεγαλύτερη από τις LAPs η οποίες καταναλώνουν λιγότερη ενέργεια και δεν χρησιμοποιούν καύσιμα. Συγκριτικά με τους δορυφόρους τόσο το κόστος κατασκευής όσο και λειτουργίας είναι πολύ χαμηλότερο από το αντίστοιχο κόστος κατασκευής, και εκτόξευσης ενός τηλεπικοινωνιακού δορυφόρου στο διάστημα, ιδιαίτερα να λάβουμε υπόψη πως η διάρκεια ζωής των δορυφόρων είναι περίπου στα 10 χρόνια.
- Αντοχή και Ανθεκτικότητα: Συγκριτικά με τις ΕΚΙΠ οι LAPs προσφέρουν μεγαλύτερη ανθεκτικότητα και αντοχή. Ιδιαίτερα σε αποστολές παρακολούθησης και παροχής τηλεπικοινωνιακών υπηρεσιών όπου η πλατφόρμα θα πρέπει να παραμένει στατική πάνω από ένα σημείο για μεγάλο χρονικό διάστημα (π.χ. μέρες ή εβδομάδες) . Αντίθετα η διάρκεια των ελεύθερα ιπτάμενων πλατφορμών περιορίζεται μόνο σε μερικές ώρες με αδυναμία παραμονής πάνω από ένα συγκεκριμένο σημείο.
- Φιλικές προς το περιβάλλον: Η κατανάλωση ενέργειας και καυσίμου είναι πολύ χαμηλότερη σε σύγκριση με την αντίστοιχη ενέργεια που απαιτεί ένας τηλεπικοινωνιακός πύργος ή μια ελεύθερα ιπτάμενη πλατφόρμα. Για παράδειγμα η

Ινδία καταναλώνει 2 δις. λίτρα πετρελαίου κάθε έτος για την λειτουργία των τηλεπικοινωνιακών τις πύργων. Εκτιμάται πως αυτό το νούμερο θα αυξηθεί στα 15 δις λίτρα τα επόμενα χρόνια, με στόχο να καλυφθούν και οι αγροτικές περιοχές της Ινδίας γεγονός που θα οδηγήσει στην αύξηση τόσο του αποτυπώματος άνθρακα στην ατμόσφαιρα όσο και της μόλυνσης που αυτό θα προκαλέσει.

- Ευρεία Κάλυψη περιοχής: Οι LAPs λόγω του υψομέτρου από το οποίο επιχειρούν εξασφαλίζουν μεγαλύτερη κάλυψη από τους αντίστοιχους τηλεπικοινωνιακούς πύργους. Σε σύγκριση με τα δορυφορικά και επίγεια ασύρματα δίκτυα, προσφέρουν ισχυρότερο Light of Sight (LOS) σήμα και μικρότερο χρόνο καθυστέρησης της διάδοσης του σήματος. Επίσης παρέχουν ευρεία οπτική κάλυψη που τις καθιστούν ιδιαίτερα χρήσιμες σε αποστολές επιτήρησης.
- Χωρητικότητα Οπισθοζεύξης (Backhaul): Διαθέτουν μεγάλη χωρητικότητα οπισθοζεύξης και μυστικότητα συγκριτικά με τις ΕΚΠΙ των οποίων η ασύρματη οπισθοζεύξη είναι πιο επιρρεπείς σε παρεμβολές, υποκλοπές και με μεγαλύτερη καθυστέρηση σήματος. Σε μια προσδεμένη πλατφόρμα η ενσύρματη οπισθοζεύξη εξασφαλίζει ασφαλή, αξιόπιστη και με υψηλούς ρυθμούς μετάδοσης δεδομένων επικοινωνίες.
- Ταχεία Ανάπτυξη: Από τα σημαντικότερα πλεονεκτήματα των LAPs είναι η ταχεία ανάπτυξη τους στο πεδίο, κάνοντας τα κατάλληλα για αποστολές δημόσιας ασφάλειας και αποκατάστασης πληγέντων περιοχών. Επιπρόσθετα μπορούν εύκολα να μεταφερθούν και να επανατοποθετηθούν σε μικρό διάστημα σε διαφορετική περιοχή. Σε αντίθεση με τους τηλεπικοινωνιακούς πύργους που μετά την εγκατάσταση τους δεν μπορούν να μετεγκατασταθούν. Επίσης οι LAPs είναι ιδανικές για χρήση σε περιοχές που δεν είναι δυνατή η εγκατάσταση ενός τηλεπικοινωνιακού πύργου όπως για παράδειγμα σε περιοχές που το δίκτυο έχει υποστεί ολικές η μερικές ζημιές μετά από μια μεγάλη φυσική καταστροφή. Συνοπτικά τα πλεονεκτήματα των LAPs είναι ταχεία ανάπτυξη, εύκολη αποσυναρμολόγηση και γρήγορη μετεγκατάσταση .
- Ανεπηρέαστες από καιρικές συνθήκες: Οι LAPs που είναι προσδεμένες διαθέτουν περίβλημα που μπορεί να ανταπεξέλθει σε όλα τα καιρικά φαινόμενα, υψηλές αλλά και χαμηλές θερμοκρασίες, υγρασία, βροχή, χιόνι, κεραυνούς και άλλες δύσκολες καιρικές συνθήκες. Αυτά τα χαρακτηριστικά τους επιτρέπουν την απρόσκοπτη λειτουργία τους ανεξάρτητα από τα όποια δυσμενή καιρικά φαινόμενα.
- Μεγάλο Ωφέλιμο φορτίο: Η δυνατότητα ανύψωσης φορτίου έως και 2700kg εξασφαλίζει την εκπλήρωση κάθε αποστολής για την οποία καλείται να διεκπεραιώσει, φέροντας τον κατάλληλο εξοπλισμό και με χρήση μόνο μιας πλατφόρμας.

- Ασφάλεια: Με δεδομένο πως η πλατφόρμα είναι προσδεμένη στο έδαφος, η μεταφορά των δεδομένων πραγματοποιείται με καλώδιο, γεγονός που εξασφαλίζει την ασφάλεια της οπισθοζεύξης.

Στα μειονεκτήματα των LAPs εντάσσονται:

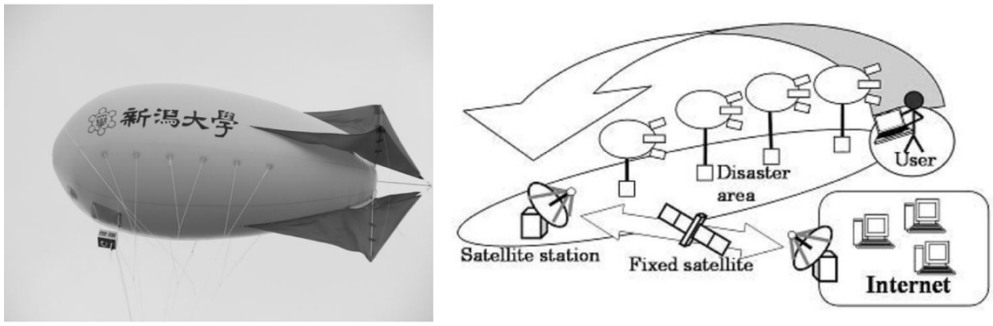
- Κινητικότητα. Παρά το γεγονός της ταχείας ανάπτυξης των LAPs και της καλύτερης κινητικότητας έναντι των τηλεπικοινωνιακών πύργων, οι κινήσεις είναι περιορισμένες λόγω του γεγονότος ότι είναι προσδεμένες στο έδαφος. Η πρόσδεση εξασφαλίζει αδιάλειπτη ισχύ και μεταφορά δεδομένων στη πλατφόρμα με κόστος την πολύ περιορισμένη κινητικότητα τους. Οι πλατφόρμες κινούνται στα όρια του μήκους του σχοινιού-καλωδίου με το οποίο η πλατφόρμες είναι προσδεμένες στο έδαφος.
- Περιορισμοί λόγω πρόσδεσης. Πέρα από το γεγονός της μειωμένης κινητικότητας που οφείλεται στην πρόσδεση της πλατφόρμας, ο κίνδυνος να υποστεί ζημιά το καλώδιο-σχοινί με το οποίο τροφοδοτείται και μεταφέρονται τα δεδομένα η πλατφόρμα είναι πιθανός. Κάτι τέτοιο θα μπορούσε να θέσει σε κίνδυνο τις αποστολές τις οποίες υποστηρίζει με καταστροφικές συνέπειες. Για αυτούς του λόγους η πρόσδεση πραγματοποιείται με πολλαπλά σημεία επαφής ώστε να μειωθεί το ρίσκο.
- Αδυναμία τοποθέτησης σε βέλτιστη θέση. Σε αντίθεση με τις ΕΚΙΠ οι προσδεμένες πλατφόρμες δεν μπορούν να μετακινηθούν σε θέσεις οι οποίες προσφέρουν βέλτιστη απόδοση για την αποστολή για την οποία προορίζονται διότι το μήκος της πρόσδεσης αποτελεί περιοριστικό παράγοντα.

5.2.2.3.4 Έργα και μελέτες εργασίας

Στη συγκεκριμένη ενότητα θα κάνουμε μια αναφορά στα σημαντικότερα projects που έχουν πραγματοποιηθεί από διάφορες ομάδες τα προηγούμενα έτη. Το πρόγραμμα Skymesh [389] του Πανεπιστημίου Niigata της Ιαπωνίας ήταν από τις πρώτες προσπάθειες για αξιοποίηση των LAPs σε καταστάσεις έκτακτης ανάγκης. Στις 23 Οκτωβρίου το 2004 ένας ισχυρός σεισμός συνέβη στην περιοχή Niigata της Ιαπωνίας. Μια σειρά από καταστροφές στις υποδομές αλλά και καταστάσεις που προέκυψαν οδήγησαν στο να απαιτηθεί περισσότερος χρόνος για την αποκατάσταση της περιοχής. Διαπιστώθηκε:

- Αποσύνδεση καλωδίων οπτικής ίνας στα επίγεια δίκτυα
- Καταστροφή σταθμών βάσης κινητής τηλεφωνίας
- Μη διαθεσιμότητα του δικτύου σταθερής τηλεφωνίας λόγω υπερφόρτωσης
- Το σύστημα επειγουσών κλήσεων δεν λειτουργούσε λόγω βλάβης σε υποσταθμούς παροχής ηλεκτρικής ενέργειας.

Όλα αυτά είχαν ως αποτέλεσμα το προσωπικό των αρχών να δαπανήσει πολύ χρόνο για να συλλέξει χρήσιμες πληροφορίες για την αποτύπωση της κατάστασης των ζημιών. Αυτές οι καταστάσεις δημιούργησαν την ανάγκη για την ανάπτυξη ενός συστήματος ταχείας ανάπτυξης στο πεδίο το οποίο θα μπορούσε να διατηρήσει τις απαιτούμενες επικοινωνίες και να υποστηρίξει όλες τις δράσεις για την ταχύτερη αποκατάσταση της πληγείσας περιοχής. Το Skymesh αναπτύχθηκε το 2005 [389] και βασίστηκε σε προσδεμένα αερόστατα τα οποία επιχειρούσαν από ύψος 100-500m παρέχοντας υπηρεσίες ασύρματης επικοινωνίας βασισμένες στο πρωτόκολλο 802.11g για διάστημα μιας περίπου εβδομάδας χωρίς να απαιτείται εξειδικευμένο προσωπικό για την ανάπτυξη και λειτουργία του (Εικόνα 134).

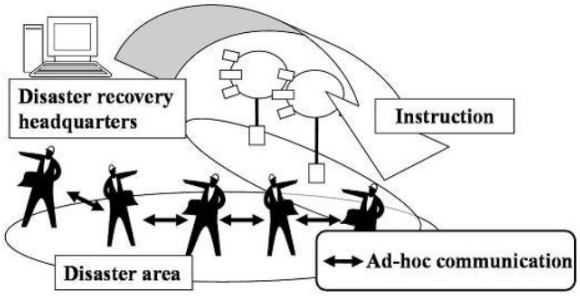


Εικόνα 134. Αερόστατο Skymesh- Χρήση και αρχιτεκτονική

Βασικοί στόχοι του ήταν:

- Να αποτελέσει ένα εφεδρικό δίκτυο κορμού σε καταστάσεις ανάγκης
- Να υποστηρίξει τις αποστολές έρευνας και διάσωσης
- Να προσφέρει εναέρια επιτήρηση της περιοχής

Η σύνδεση του αερόστατου με τον επίγειο δορυφορικό σταθμό βάσης (Εικόνα 134) εξασφάλιζε την παροχή υπηρεσιών διαδικτύου στις ομάδες (Εικόνα 135) που επιχειρούσαν στην περιοχή. Κόμβοι με αερόστατα μπορούσαν να καλύψουν μεγαλύτερες εκτάσεις και να παρέχουν ταυτόχρονα και εναέρια επιτήρηση της περιοχής. Το πρόγραμμα αυτό απέδειξε πως ήταν εύκολη η ανάπτυξη ενός εφεδρικού δικτύου σε μικρό χρονικό διάστημα και κατάλληλο για καταστάσεις έκτακτης ανάγκης. Επίσης το σύστημα μετέδιδε με επιτυχία και τέσσερις ροές βίντεο από την κάμερα που είχε τοποθετηθεί στο αερόστατο.

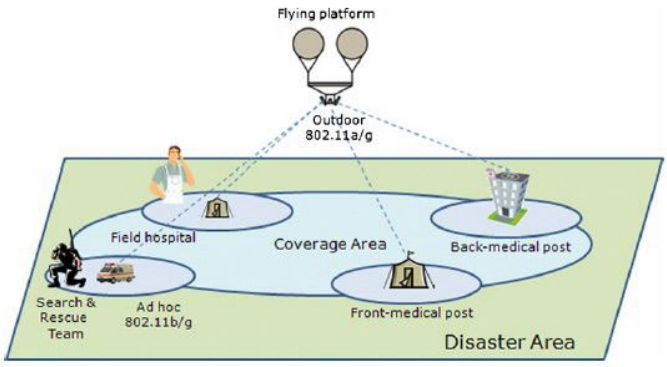


Εικόνα 135. Υποστήριξη επιχειρήσεων έρευνας και διάσωσης

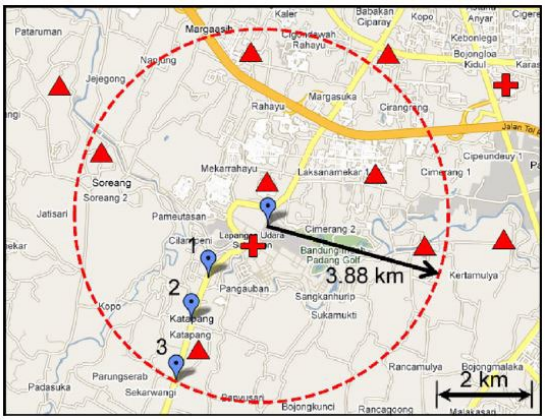
5.2.2.3.5 Σύστημα Επειγουσών Ιατρικών Επικοινωνιών

Το 2009 μια ομάδα επιστημόνων ανέπτυξε ένα σύστημα επειγουσών ιατρικών επικοινωνιών με χρήση LAP στην Ινδονησία [390]. Το 2004 η Ινδονησία βίωσε τις συνέπειες ενός θανατηφόρου τσουνάμι το οποίο χτύπησε την πόλη Aceh. Τα επίγεια δίκτυα δεν λειτουργούσαν λόγω σημαντικών καταστροφών, είτε στο δίκτυο κεραιών είτε στους σταθμούς ηλεκτροδότησης. Οι τηλεπικοινωνιακές εταιρείες για εβδομάδες δεν παρείχαν υπηρεσίες και χρειάστηκε περισσότερο από ένα μήνα για να επισκευαστούν οι εγκαταστάσεις του επίγειου ασύρματου δικτύου στην πόλη. Για το σύστημα αυτό χρησιμοποιήθηκε ένα προσδεμένο αερόστατο, ενώ η ασύρματη μετάδοση του σήματος πραγματοποιήθηκε με χρήση του πρωτοκόλλου Wi-Fi 802.11. Η μέγιστη απόσταση από την πλατφόρμα ήταν στα 3.88km και η ταχύτητα λήψης δεδομένων ήταν στα 54Mbps.

Η κάλυψη με μια πλατφόρμα έφτασε τα 47.39km ενώ ο απαιτούμενος χρόνος για να εγκατασταθεί μια πλατφόρμα σε υψόμετρο 440m ήταν 3-4h. Το σύστημα αξιολογήθηκε θετικά και αυτό διότι ο μικρός χρόνος ανάπτυξης , η κάλυψη που πρόσφερε, ο μεγάλος ρυθμός δεδομένων μετάδοσης αλλά και το χαμηλό κόστος σε συνδυασμό με το γεγονός ότι υπήρχε δυνατότητα γρήγορης μεταφοράς του, κατέστησε το σύστημα ιδιαίτερα αποδοτικό για καταστάσεις εκτάκτου ανάγκης

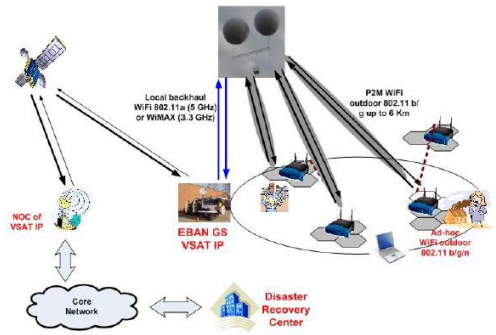


Εικόνα 136. Εγκατάσταση του συστήματος



Εικόνα 137. Προβλεπόμενες περιοχές κάλυψης για ύψος 440m [390]

Το Project EBAN [382] (Εικόνα 138) αναπτύχθηκε με αφορμή τις σοβαρές φυσικές καταστροφές που υπέστη η Ινδονησία την περίοδο 2004-2007. Για το Δίκτυο Ευρυζωνικής Πρόσβασης έκτακτης ανάγκης (EBAN) χρησιμοποιήθηκε αερόστατο που επιχειρούσε από υψόμετρο 100-500m, παρέχοντας ασύρματη ευρυζωνική πρόσβαση στις ομάδες διάσωσης καθώς και δυνατότητα χρήσης διάφορων εφαρμογών (applications) έκτακτης ανάγκης. Οι πρώτοι ανταποκριτές είχαν ασύρματη (WiFi) πρόσβαση στο διαδίκτυο, τηλεφωνία VoIP, δυνατότητα για βίντεο-διάσκεψη καθώς και δυνατότητα χρήσης εξειδικευμένων εφαρμογών έκτακτης ανάγκης όπως είναι το Σύστημα Πληροφοριών Επείγουσας Ιατρικής Φροντίδας (Emergency Medical Care Information System - EMCIS). Το σύστημα παρείχε κάλυψη σε ακτίνα 5.5km ή 72km^2 όταν η πλατφόρμα επιχειρούσε από υψόμετρο 440m. Η επιλογή ασύρματης μετάδοσης με χρήση του πρωτοκόλλου wifi επιλέχθηκε με κριτήριο πως είναι εξαιρετικά διαδεδομένο και οι χρήστες μπορούσαν να έχουν πρόσβαση από τα έξυπνα τηλέφωνα τους χωρίς να απαιτείται η χρήση επιπρόσθετου εξοπλισμού. Είναι επίσης σημαντικό να αναδειχθεί πως παρά το γεγονός πως η ποιότητα της υπηρεσίας (QoS) βασίζεται στην καλύτερη προσπάθεια (Best Effort), η απόδοση του συστήματος αξιολογήθηκε ως αποδεκτή για ασύρματη (Wi-Fi) πρόσβαση στο διαδίκτυο. Βασικός περιορισμός και αυτού του συστήματος αποτέλεσε η υποχρεωτική ύπαρξη οπτικής επαφής μεταξύ πομπού και δέκτη.



Εικόνα 138. Αρχιτεκτονική του συστήματος EBAN

5.2.2.3.6 Case Studies των LAPs για την επιτήρηση συνόρων

Οι LAPs έχουν συστηματικά χρησιμοποιηθεί για αποστολές φύλαξης συνόρων, ιδιαίτερα από το 2015 και μετά όπου διαπιστώθηκε σημαντική αύξηση των μεταναστευτικών ροών τόσο προς την Ευρώπη όσο και προς τις Η.Π.Α.

Νότιο Τέξας, Κοιλάδα Ρίο Γκράντε:- Οι αρμόδιες υπηρεσίες των Η.Π.Α. όπως το Τμήμα Εσωτερικής Ασφάλειας και η υπηρεσία φύλαξης συνόρων και τελωνείων είχαν μια σημαντική πρόκληση να αντιμετωπίσουν που ήταν η επιτήρηση μια τεράστιας συνοριακής έκτασης [383]. Αυτό δεν μπορούσε να αντιμετωπιστεί με επίγεια μέσα επιτήρησης από

πλευρά κόστους απόδοσης. Έτσι χρησιμοποίησαν μικρά προσδεδεμένα αερόστατα της εταιρείας TCOM. Τα σημαντικότερα πλεονεκτήματα αυτών των μικρών αερόστατων ήταν:

- η παραμονή τους για εβδομάδες στον αέρα
- η αξιοπιστία τους και η αντοχή τους σε καιρικές συνθήκες
- η δυνατότητα ταχείας μετακίνησης τους σε άλλο τομέα και
- το μικρό τους κόστος.

Με τη χρήση των μικρών αυτών προσδεμένων αερόστατων οι υπηρεσίες διαπίστωσαν μείωση στις παράνομες μεταναστευτικές ροές.

Ελλάδα, Αθήνα, Ολυμπιακοί Αγώνες 2004:- Στην περίοδο των Ολυμπιακών Αγώνων η χώρα μας χρησιμοποίησε LAP με δυνατότητες μετάδοσης εικόνων και δεδομένων. Επιχειρούσε σε υψόμετρο έως 3.3kmμε για 16 συνεχόμενες ώρες καθημερινά σε ημερήσιες και νυχτερινές αποστολές. Διέθετε τρείς κάμερες με δυνατότητα μετάδοσης βίντεο σε πραγματικό χρόνο στο Ολυμπιακό κέντρο ασφαλείας [391]. Η τελευταία του πτήση πραγματοποιήθηκε στις 5 Οκτωβρίου 2004.

Ελλάδα, Σάμος 2019 [392]:- Τον Ιούλιο του 2019 η χώρα μας στα πλαίσια της μικτής ευρωπαϊκής επιχείρησης «Ποσειδών», υπό την εποπτεία του Οργανισμού Ευρωπαϊκής Συνοριοφυλακής και Ακτοφυλακής - FRONTEX πραγματοποίησε την πρώτη δοκιμαστική πτήση του αερόπλοιου Ζέπελιν για την φύλαξη των συνόρων στη Σάμο Εικόνα 139. Το αερόπλοιο διαστάσεων 35m διέθετε ραντάρ, θερμική κάμερα, σύστημα αυτόματης αναγνώρισης (AIS) [393] και είχε δυνατότητα να επιχειρεί σε υψόμετρο έως 1000m. Στα πλαίσια αυτής της αποστολής, το Λιμενικό Σώμα έγινε η πρώτη ακτοφυλακή κράτους μέλους της Ευρωπαϊκής Ένωσης που χρησιμοποίησε προσδεμένο αερόπλοιο για την επιτήρηση του θαλασσίου πεδίου και την αντιμετώπιση του διασυνοριακού εγκλήματος καθώς και της παράνομης μετανάστευσης.

Εικόνα 139. Αερόπλοιο Ζέπελιν

Ελλάδα, Αλεξανδρούπολη και Λήμνος 2021 [394]:- Στα πλαίσια συνεργασίας των ελληνικών υπηρεσιών με τον FRONTEX δυο αερόπλοια ανέλαβαν την επιτήρηση των συνόρων σε Αλεξανδρούπολη και Λήμνο τον Ιούλιο και Αύγουστο του 2021.Τα προσδεδεμένα αυτά

αερόπλοια τοποθετήθηκαν στο Αεροδρόμιο της Αλεξανδρούπολης και στο χωριό Πλάκα της Λήμνου. Τα αερόπλοια είναι τύπου Eagle Owl της Γαλλικής εταιρείας CNIM (Εικόνα 140) και ο εξοπλισμός που φέρουν είναι της Γερμανικής εταιρεία GmbH. Κάθε σύστημα αποτελούταν από ένα αερόστατο 450 m³ Eagle Owl, εξοπλισμένο με οπτικό αντίζυγο Hensoldt ARGOS II HD EO/IR, ναυτικό ραντάρ Diades Marine και σύστημα αυτόματης αναγνώρισης (AIS) [395]. Επίσης διέθεταν επίγειο σταθμό εντολών και ελέγχου C2 (Command and Control) οι οποίοι αντλούσαν στοιχεία από τους αισθητήρες, ανέλυαν τα δεδομένα και μετέδιδαν τις απαραίτητες πληροφορίες στα επιχειρησιακά κέντρα του Frontex. Το σύστημα παρείχε τη δυνατότητα διαμοιρασμού της εικόνας θαλάσσιας επιτήρησης σε οποιονδήποτε απομακρυσμένο χρήστη μέσω της χρήσης διαδικτυακών ή φορητών εφαρμογών που ήταν συνδεδεμένες στο σύστημα C2. Κύρια πλεονεκτήματα του συστήματος:

- το χαμηλό κόστος πτήσης ανα ώρα λειτουργίας συγκριτικά με άλλες πλατφόρμες εναέριας επιτήρησης,
- η δυνατότητα να επιχειρεί 24/7 για συνεχόμενες ημέρες ακόμη και εβδομάδες
- η φορητότητα του συστήματος χωρίς να απαιτεί ειδική υποδομή για να αναπτυχθεί
- η ανθεκτικότητα του σε ανέμους ταχύτητας που φτάνουν τα 110km

Εικόνα 140. Αερόπλοιο τύπου Eagle Owl της Γαλλικής εταιρείας CNIM

5.2.2.3.7 Το μέλλον των LAPs

Στην ενότητα αυτή παρουσιάσαμε αναλυτικά τις πλατφόρμες που επιχειρούν από χαμηλό υψόμετρο παρέχοντας όχι μόνο υπηρεσίες επικοινωνίας αλλά και μετάδοσης εικόνας και δεδομένων στους πρώτους ανταποκριτές αλλά και στα κέντρα ελέγχου των αρμοδίων υπηρεσιών. Αναλύσαμε τα πλεονεκτήματα και μειονεκτήματα της κάθε πλατφόρμας, αναδείξαμε τις επιχειρησιακές τους δυνατότητες και καταγράψαμε ενδεικτικές μελέτες περίπτωσης των LAPs.

Με την εξέλιξη των τεχνολογιών επικοινωνίας και ιδιαίτερα του 5G αλλά και του 6G που θα ακολουθήσει από το 2030 και μετά, όλες οι πληροφορίες δείχνουν πως η χρήση των LAPs θα

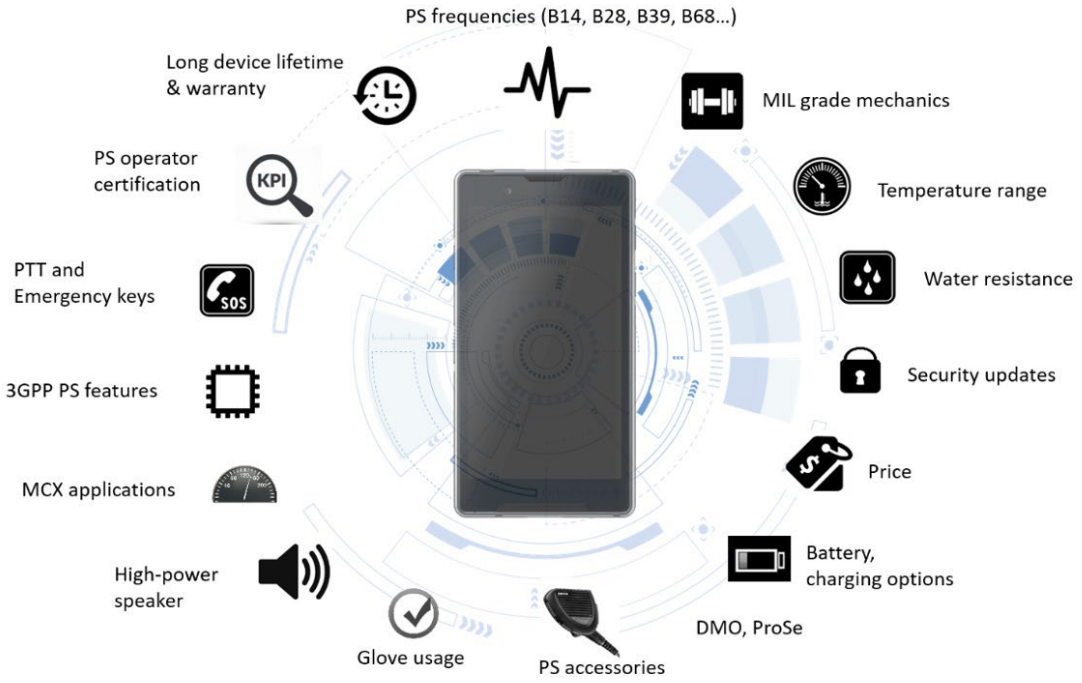
μεγαλώσει με στόχο την εξασφάλιση ευρυζωνικών επικοινωνιών, πολύ μικρής καθυστέρησης στο τελευταίο μίλι του δικτύου.

Η αξιοποίηση τους λόγω χαμηλού κόστους γρήγορης ανάπτυξης και μεγάλης γεωγραφικής κάλυψης καθώς και η δυνατότητα συνεργασίας τους, τόσο με HAPs όσο και με τα δορυφορικά δίκτυα δείχνουν πως η χρήση τους σε καταστάσεις έκτακτης ανάγκης θα μπορούσε να είναι καθοριστική στο άμεσο μέλλον.

5.3 Επίπεδο χρήστη

Στο επίπεδο αυτό επιχειρείται μια κοντινότερη ματιά στους πρώτους ανταποκριτές, που λειτουργούν ταυτόχρονα ως συλλέκτες και ως δέκτες της πληροφορίας. Δύο μεγάλες υποκατηγορίες εντάσσονται στο επίπεδο χρήστη. Το επίπεδο εξοπλισμού του χρήστη και οι υπηρεσίες που τίθενται στη διάθεσή του. Όλα αυτά αφενός συνθέτουν τα «όπλα» του πρώτου ανταποκριτή, αλλά σε κάθε περίπτωση και του επαγγελματία της δημόσιας ασφάλειας, από όποια θέση εμπλέκεται, αφετέρου καταγράφουν πρακτικά τις λύσεις στις ξεχωριστές τεχνολογικές απαιτήσεις.

Είναι βέβαιο ότι οι τεχνικές απαιτήσεις των συσκευών που μπορούν να υποστηρίξουν τους πρώτους ανταποκριτές στο πεδίο θα μπορούσαν έυκολα να αποτελέσουν μια ιδιατέρως εκτενή μελέτη. Στην ίδια λογική το [396] ανέδειξε τα βασικότερα σημεία των προδιαγραφών που πρέπει να έχουν οι ευρυζωνικές συσκευές των πρώτων ανταποκριτών. Θα πρέπει να επισημανθεί ότι απαιτήσεις που είναι υποχρεωτικές για ορισμένους οργανισμούς, μπορεί να είναι προαιρετικές ή ακόμη και να μην σχετίζονται με άλλους οργανισμούς. Σε κάθε περίπτωση στην Εικόνα 141 περιγράφονται σχηματικά οι τυπικές απαιτήσεις ευρυζωνικών συσκευών για κρίσιμες επικοινωνίες, τις οποίες θα αναλύσουμε εκτενώς στη συνέχεια.



Εικόνα 141. Τυπικές απαιτήσεις ευρυζωνικής συσκευής MC [396]

5.3.1 Εξοπλισμός

Σημαντικό ρόλο στο επίπεδο ανταπόκρισης των επαγγελματιών της δημόσιας ασφάλειας διαδραματίζει το υλικό και συγκεκριμένα ο κατεχόμενος εξοπλισμός. Ο εξοπλισμός μετουσιώνει τη δυνατότητα του χρήστη, που στην προκειμένη περίπτωση αφορά στους πρώτους ανταποκριτές, να αντιληφθεί, επεξεργαστεί στιγμιαία, διαβιβάσει και λάβει τις απαιτούμενες πληροφορίες στο πεδίο με τον καλύτερο δυνατό τρόπο για την εκπλήρωση της αποστολής του. Η ίδια δουλειά μπορεί να γίνει σαφώς πιο αποδοτικά και αποτελεσματικά έχοντας ως σύμμαχο ένα έξυπνο κράνος, ένα φορητό ρολόι με επαυξημένες δυνατότητες λήψης και μετάδοσης δεδομένων, ένα έξυπνο κινητό τηλέφωνο. Στο σημείο αυτό θα αναλύσουμε τους λόγους για τους οποίους ο εξοπλισμός αποτελεί έναν σημαντικό κρίκο στην αλυσίδα της απρόσκοπτης και ασφαλούς επικοινωνίας.

Βέβαια, δεν θα πρέπει να ξεχνάμε ότι ο εξοπλισμός δεν αφορά μόνο στα ευρυζωνικά δίκτυα, αλλά σχετίζεται σε μεγάλο βαθμό, ακόμη και στις μέρες μας, με τις επικοινωνίες στενής ζώνης και των προτύπων αυτής που εξακολουθούν, όντας πλήρως ανανεωμένα, να πρωταγωνιστούν στο πεδίο της δημόσιας ασφάλειας. Εντελώς ενδεικτικά παρατίθενται στη συνέχεια φορητοί ραδιοπομποδέκτες, σταθμοί βάσης αυτών και συστήματα υποστήριξης σε σταθερές ή κινητές υποδομές. Με την σύντομη παράθεσή τους καθίσταται αντιληπτό ότι, όπως ήδη έχει αναφερθεί και σε άλλα σημεία, η μετάβαση στην επόμενη ημέρα είναι μια διαδικασία χρονοβόρα, που απαιτεί αργά και σταθερά βήματα, με σεβασμό στο τεχνολογικό παρελθόν και σε δοκιμασμένες τεχνολογίες στις οποίες στηρίχθηκε επί πολλά χρόνια η

δημόσια ασφάλεια. Στις εικόνες που ακολουθούν, χωρίς να υφίσταται πρόθεση ανάδειξης εμπορικών προϊόντων κάποιων εταιριών, αλλά καθαρά από ενδεικτική σκοπιά, παρατίθεται εξοπλισμός που εξοπλίζει ακόμη και σήμερα, σε πολλές χώρες ανά τον κόσμο τους επαγγελματίες της δημόσιας ασφάλειας.

Λύσεις συμβατές με πρότυπα P25, TETRA, TETRAPOL, DMR, TEDS, κ.λπ. που αφορούν φορητούς και μη ραδιοπομποδέκτες και διασυνδέονται πλέον με προηγμένα στοιχεία της υποδομής ευρυζωνικών δικτύων, όπου υπάρχουν, όπως έξυπνα κινητά τηλέφωνα και tablets εμφανίζονται ενδεικτικά στην Εικόνα 142, Εικόνα 143 και Εικόνα 144.

Εικόνα 142. Διάφοροι τύποι ραδιοπομποδεκτών (α)P25 radiotης L3HARRIS[41], (β)TETRA radio της Hytera[42], (γ)TETRAPOL radio της Airbus[43] και (δ)NXDN radio/analog της KENWOOD[44]

Εικόνα 143. Πλήρες σύστημα P25 που παρέχει ραδιοπομποδέκτη, κονσόλα οχήματος και σύνδεσή του με tablet και smartphone από την L3HARRIS[45]

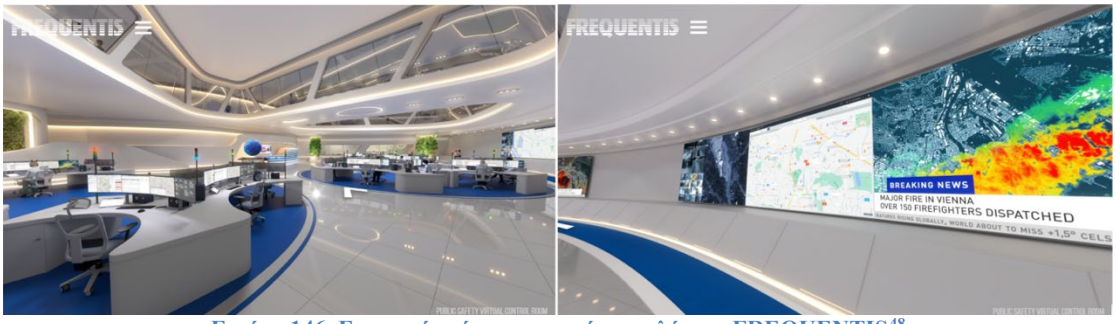
[41] https://www.l3harris.com/newsroom/trade-release/2022/12/l3harris-awarded-93-million-contract-improve-mbta-public-safety
[42] https://hytera-europe.com/products/pt350
[43] https://www.securelandcommunications.com/tph700-tetrapol-atex-radio
[44] https://kenwoodcommunications.co.uk/digital-pmr/digital-atex-safety/NX-330EXE/
[45] https://www.l3harris.com/newsroom/press-release/2020/10/l3harris-technologies-helps-public-safety-agencies-access-grants

Εικόνα 144. Πλήρες σύστημα NXDN και DMR της KENWOOD[46]

Ένα ακόμη αξιόλογο παράδειγμα που αποδεικνύει και την εξέλιξη των συστημάτων αυτών που πρωταγωνιστούν στο χώρο της δημόσιας ασφάλειας από τη δεκαετία του 1990 και αναμέναται να έχουν σημαντική παρουσία τουλάχιστον μέχρι το 2030 είναι το σύστημα TETRA SmartOne της Hytera, που υποστηρίζει λειτουργίες φωνητικών κλήσεων, υπηρεσίες τοποθεσίας GPS, λειτουργίες ανταλλαγής μηνυμάτων, εγγραφής φωνής. Η λειτουργικότητα του λογισμικού του μπορεί να επεκταθεί μέσω καμερών CCTV που συνδέονται με IP, ή να ενσωματώνει περιεχόμενο ιστού και να αντλεί δεδομένα από διάφορες βάσεις. Χαρακτηριστικό στιγμιότυπο από το κέντρο ελέγχου και διοίκησης του TETRA SmartOne παρουσιάζεται στην Εικόνα 145. Ανάλογο σύστημα υπάρχει και για το P25 και παρόμοιες υλοποιήσεις υπάρχουν και από άλλες εταιρίες του χώρου. Επιπλέον, στα δίκτυα 5G για υπηρεσίες δημόσιας ασφάλειας, παρουσιάζεται από την FREQUENTIS ένα πλήρως ψηφιακό και λειτουργικό Control Room στο οποίο υφίσταται η δυνατότητα εικονικής επίσκεψης και στιγμιότυπά της φαίνονται στην Εικόνα 146

Εικόνα 145. Σύστημα TETRA SmartOne της Hytera[47]

[46] https://kenwoodcommunications.co.uk/digital-pmr/
[47] https://hytera-europe.com/systems/tetra-smartone



Εικόνα 146. Εικονική επίσκεψη σε κέντρο ελέγχου FREQUENTIS[48]

Στη συνέχεια, θα γίνει μια εκτενής αναφορά σε εξοπλισμό που υποστηρίζει ευρυζωνική τεχνολογίας, με δεδομένο ότι αφορά στο τώρα, αλλά και στις μελλοντικές εξελίξεις στις κρίσιμες επικοινωνίες.

5.3.1.1 Έξυπνα κινητά τηλέφωνα (smartphones)

Στη βιβλιογραφία συνήθως τα έξυπνα τηλέφωνα για τη δημόσια ασφάλεια διαχωρίζονται σε διάφορες κατηγορίες, με συνηθέστερο διαχωρισμό αυτόν σε ανθεκτικά και μη (rugged smartphones / Non-rugged smartphones) [396]. Ουσιαστικά, τα smartphone που προορίζονται για τη δημόσια ασφάλεια θα πρέπει να καλύπτουν ένα ευρύ φάσμα δραστηριοτήτων, προκλήσεων και κινδύνων. Τα βασικά χαρακτηριστικά δημιουργούνται από ένα πλαίσιο στιβαρής συσκευής, που διαθέτει χαρακτηριστικά, εφαρμογές, αξεσουάρ και υποστήριξη υπηρεσιών που δύναται ν` ανταποκριθεί στις απαιτήσεις. Ειδικότερα και αναλυτικότερα [397]:

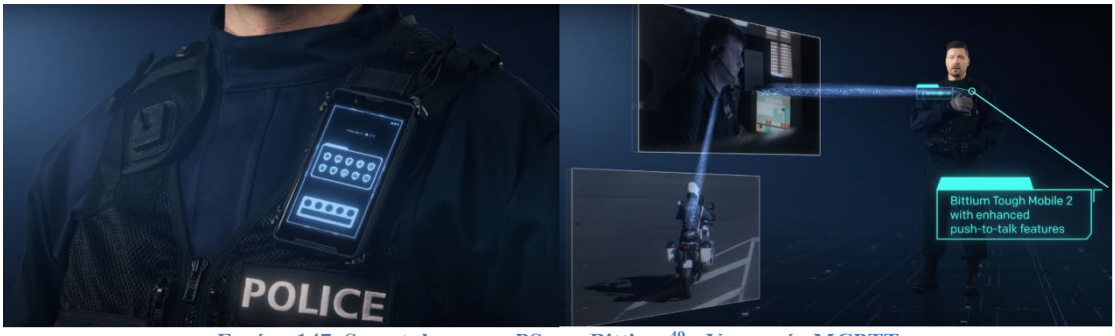
- Ανθεκτικότητα. Είναι διαφορετικό ένα τηλέφωνο να είναι ανθεκτικό και διαφορετικό να το προστατέψεις με μια ανθεκτική θήκη. Υπάρχουν τηλέφωνα που αντέχουν σε πτώσεις, βύθιση στο νερό, ακραίες θερμοκρασίες, μεγάλα υψόμετρα, βροχή και ψεκασμό αλατιού.
- Ποιότητα και μέγεθος οθόνης. Παρέχει τη δυνατότητα χρήσης σημαντικών εφαρμογών (π.χ. αποστολή μέσω Computer-Aided Dispatch - CAD), αναζήτηση αρχείων και επίγνωση της κατάστασης)
- PTT/MCPTT. Οι υπηρεσίες φωνής είναι πρωταρχικής σημασίας στη δημόσια ασφάλεια (Εικόνα 147).
- Διάρκεια ζωής μπαταρίας. Η διάρκεια ζωής της μπαταρίας είναι μια διαρκής ανησυχία των χρηστών και εξαιτίας αυτού θα ήταν ωφέλιμο να έχουμε συσκευές με μεγάλη χωρητικότητα (πάνω από 4.000mAh), οι οποίες παρέχουν τη δυνατότητα ταχείας φόρτισης.
- Απόδοση και αποθήκευση. Στοιχεία τα οποία σχετίζονται άμεσα με τον επεξεργαστή, καθώς ενδέχεται η χρήστες να εκτελούν εφαρμογές που ενεργούν ταυτόχορνα

[48] https://www.frequentis.com/en/public-safety/virtual-control-room/tour

πολλαπλές εργασίες και απαιτούν υψηλή απόδοση. Ταυτόχρονα, το ζήτημα της αποθήκευσης θεωρείται το ίδιο σημαντικό (περισσότερα από 64GB μνήμης και ιδανικά πλέον των 128GB)

- Λήψη φωτογραφιών και βίντεο. Θα πρέπει να υφίσταται δυνατότητα φωτογραφιών και βίντεο υψηλής ανάλυσης και ποιότητας σε διάφορα περιβάλλοντα φωτισμού και συνθηκών, που θα πρέπει να είναι εφάμιλλες αντίστοιχων ψηφιακών Εικόνα 148.
- Ασφάλεια. Με δεδομένο ότι γίνεται αποθήκευση δεδομένων, το υψηλό επίπεδο ασφάλειας των έξυπνων κινητών τηλεφώνων θεωρείται επιβεβλημένο, ώστε να παρέχεται προστασία από κακόβουλο λογισμικό, παραβιάσεις δεδομένων ή σε εξαιρετικές περιπτώσεις να παρέχεται προστασία συσκευών που έχουν κλαπεί ή απωλεσθεί.
- Αποτελεσματικό αναγνωριστικό δακτυλικών αποτυπωμάτων. Ώστε να παρέχει λειτουργικότητα ακόμη και στις περιπτώσεις που το δάχτυλο είναι υγρό ή λιπαρό. Ο χρόνος για τη συγκεκριμένη ταυτοποίηση θα πρέπει να είναι μιδαμηνός, ενώ σε καμία περίπτωση η κακή λειτουργικότητα δεν θα πρέπει ν` απασχολήσει ή καθυστερήσει τον πρώτο ανταποκριτή.
- Άμεση και χωρίς προβλήματα διασύνδεση του smartphone με laptop. Η αντιστοίχιση αυτή στο πεδίο κρίνεται παραίτηση, ιδιαίτερα σε περιπτώσεις που πραγματοποιείται σε laptop που είναι εγκατεστημένα σε οχήματα, καθώς αυξάνεται η λειτουργικότητα και αποτελεσματικότητα Εικόνα 149.

Η απαρίθμηση ή παρουσίαση συγκεκριμένων συσκευών διαφόρων κατασκευαστών δεν εξυπηρετεί τους σκοπούς αυτής της εργασίας. Ωστόσο, παρατίθενται στη συνέχεια χαρακτηριστικά στιγμιότυπα από τη λειτουργικότητα και χρηστικότητα ενός smartphone για τη δημόσια ασφάλεια, ώστε να προκύψει με τη δύναμη της εικόνας αυτά που ήδη περιγράφηκαν παραπάνω.



Εικόνα 147. Smartphone για PS της Bittium[49] - Υπηρεσία MCPTT

[49] https://toughmobile2.bittium.com

Εικόνα 148. Smartphone για PS της Bittium - Υπηρεσία MCVideo

Εικόνα 149. Smartphone για PS της Bittium - Διασύνδεση του smartphone με laptop

5.3.1.2 Φορητοί υπολογιστές – υπολογιστές ταμπλέτες (laptops - tablets)

Με πρωταρχικό στόχο οι επαγγελματίες της δημόσιας ασφάλειας να έχουν στο πεδίο όλη την τεχνολογία και την πληροφορία που χρειάζονται, ώστε να συνεργαστούν, διαλειτουργήσουν και διεκπεραιώσουν με τον καλύτερο δυνατό τρόπο την αποστολή τους, ένα ακόμη εργαλείο τίθεται στη διάθεσή τους. Οι φορητοί υπολογιστές, με αυξημένη επεξεργαστική ικανότητα που σε κάποιες περιπτώσεις δεν υστερεί σε τίποτα από τις υπολογιστικές μονάδες του Γραφείου, με πολύ σημαντικές δυνατότητες διασύνδεσης από το πεδίο με το κέντρο ελέγχου και διοίκησης, παρέχουν σημαντική βοήθεια και ευχρηστία στους πρώτους ανταποκριτές. Φορητοί υπολογιστές (laptop) ή tablet εγκατεστημένα σε οχήματα, η στα χέρια των ανθρώπων της δημόσιας ασφάλειας συνεισφέρουν αυτό ακριβώς που περιγράψαμε ήδη. Επεκτείνουν τις λειτουργικές τους δυνατότητες και τους παρέχουν πρόσβαση σε κρίσιμης σημασίας δεδομένα στο πεδίο. Οι προδιαγραφές και απαιτήσεις δεν διαφέρουν από αυτές του υπόλοιπου εξοπλισμού

5.3.1.3 Ενδυτά μέσα (wearables)

Οι φορητές συσκευές δίνουν μια νέα διάσταση στην τεχνολογία για τους πρώτους ανταποκριτές, παρέχοντας πρόσβαση ανά πάσα στιγμή και οπουδήποτε σε κρίσιμες πληροφορίες και βελτιώνοντας την επίγνωση της κατάστασης για τους χρήστες, ανεξαρτήτως αποστολής. Προς την κατεύθυνση αυτή έχουν γίνει σημαντικότατα βήματα, καθώς οι υπολογιστές που είναι εγκατεστημένοι στα οχήματα των υπηρεσιών της δημόσιας ασφάλειας

είναι από αρκετό καιρό μια πραγματικότητα, ακόμη και για τη χώρα μας. Ένας από τα βασικά χαρακτηριστικά των επαγγελματιών αυτών είναι η κινητικότητα. Επομένως, το να βασίζονται σε φορητούς υπολογιστές, έξυπνα κινητά τηλέφωνα ή υπολογιστές ταμπλέτες, δεν αποτελεί πάντοτε μια καλή λύση στο πεδίο, πολύ περισσότερο όταν οι συνθήκες που επιχειρούν είναι ακραίες και για τις ανάγκες της αποστολής φορούν προστατευτικά γάντια. Η λύση έρχεται από το οικοσύστημα IoLST που αναπτύσσει μια σειρά από φορητές συσκευές, με στόχο να προσφέρουν μοναδικές δυνατότητες, υψηλή κινητικότητα και σε πολλές περιπτώσεις αυτονομία εργασιών [398]. Η πράξη έχει δείξει όμως ότι η ανάγκη για πρόσβαση σε πληροφορίες δεν σταματά τη στιγμή που ο επαγγελματίας της δημόσιας ασφάλειας εγκαταλείπει το υπηρεσιακό του όχημα. Τουναντίον, σε κάποιες περιπτώσεις η γρήγορη και άμεση πρόσβαση σε κάποια δεδομένα κρίνεται ιδιαιτέρως σημαντική. Όπως είδαμε ήδη, σημαντικότατη συμβολή στην τεχνολογική συνέχεια παρέχουν τα έξυπνα κινητά τηλέφωνα, ωστόσο η εμπειρία από το πεδίο έχει αποδείξει ότι τα ένδυτα μέσα (whearables) είναι ικανά να ανεβάσουν το επίπεδο των παρεχόμενων υπηρεσιών που είναι διαθέσιμες στους πρώτους ανταποκριτές σε ένα εντελώς νέο επίπεδο. Παράλληλα, κάποια από τα ένδυτα μέσα συνεισφέρουν σημαντικότατα στην αύξηση του επιπέδου ασφάλειας και επίγνωσης της κατάστασης. Στα ένδυτα μέσα εντάσσονται κάμερες σώματος (body cameras), έξυπνα ρολόγια (smartwatches), έξυπνα κράνη (smart helmets), φορητοί κινητοί υπολογιστές (wearable mobile computers), κ.λπ. (Εικόνα 151, Εικόνα 152). Τα ένδυτα μέσα σε αναλογία με τα έξυπνα κινητά τηλέφωνα θα πρέπει να πληρούν κάποιες ελάχιστες λειτουργικές προδιαγραφές [399]:

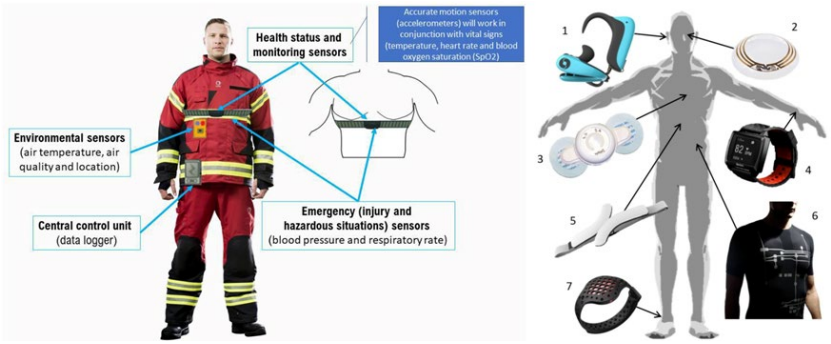
- Παρέχουν πρόσβαση σε (CAD) και σύνδεση με το όχημα, σε σημαντική απόσταση απ` αυτό, καθώς επίσης και τη δυνατότητα γρήγορης ανασκόπησης των εισερχόμενων πληροφοριών ακόμα και όταν ο χρήστης βρίσκεται σε κίνηση και επιτρέπει την ετοιμότητα σε περίπτωση που μια κατάσταση απαιτεί γρήγορη εμπλοκή, ή την ανάγκη πρόσβασης σε εξοπλισμό που είναι τοποθετημένος στη ζώνη.
- Ταχεία Επικοινωνία. Ένα έξυπνο ρολόι για παράδειγμα υποστηρίζει φωνητικές επικοινωνίες και ενημερώνει για σημαντικές πληροφορίες με απτική ανάδραση (δονήσεις), το οποίο συνιστά κρίσιμης σημασίας δυνατότητα και για λόγους ασφαλείας. Στο ίδιο παράδειγμα, το κέντρο διοίκησης και ελέγχου θα μπορούσε να ενημερώσει έναν αστυνομικό που βρίσκεται σε καταδίωξη υπόπτου με την αποστολή της φωτογραφίας του, που προέκυψε καθ`ον χρόνο το περιστατικό βρίσκεται σε εξέλιξη και την οποία φωτογραφία θα μπορούσε να δει με μια γρήγορη ματιά στον καρπό του.
- Επείγουσες ειδοποιήσεις χρηστών (SOS / Assistance Alerts). Παρέχει τη δυνατότητα στο χρήστη να μεταβιβάσει σήμα κινδύνου, χωρίς να γίνει αντιληπτός, με

αποτέλεσμα λόγω του γεωεντοπισμού να είναι εφικτή η παροχή άμεσης συνδρομής. Στην ίδια κρίσιμης σημασίας λειτουργικότητα εντάσσεται και η δυνατότητα αναμετάδοσης ζωντανά ήχου από τη σκηνή που λαμβάνει χώρα το περιστατικό.

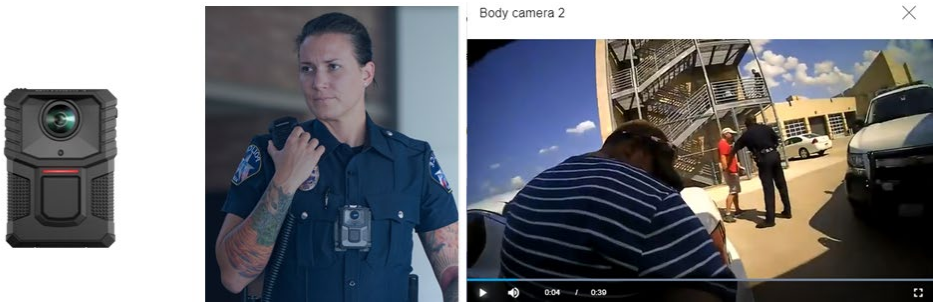
- Ειδοποίησης της αιφνίδιας αλλαγής κινητικής κατάστασης του χρήστη. Οι αισθητήρες επιταχυνσιομέτρου και γυροσκοπίου, κατάλληλα προσαρμοσμένες σε ένδυτες συσκευές (ρολόγια, γιλέκα, κ.λπ.) παρέχουν πληροφορίες σημαντικές για την κατάσταση του περιστατικού που είναι σε εξέλιξη (π.χ. ενημέρωση της έναρξης μια πεζής καταδίωξης, κ.λπ.) δίνοντας την ακριβή θέση του χρήστη και την πορεία που ακολούθησε. Για να γίνει αντιληπτό το πόσο σπουδαία είναι η συγκεκριμένη λειτουργικότητα, αρκεί να αναλογιστεί ο οποιοσδήποτε την επικινδυνότητα των καταδιώξεων, ιδιαίτερως των πεζών, αλλά και την αδυναμία του επαγγελματία κατά το χρόνο που καταδιώκει να μεταδώσει στο κέντρο τις πληροφορίες που θέλει (αυξημένος καρδιακός ρυθμός και αναπνοής, συγκεχυμένη εκφορά λόγου λόγω άγχους και λαχανιάσματος, αδυναμία χρήσης κινητού ή φορητού πομποδέκτη, κ.λπ.). Ιδιαίτερης αξίας έρευνα αποτελεί η [400], καθώς παρουσιάζεται ένα σύστημα που παρακολουθεί τους πυροσβέστες και τους άλλους ανταποκριτές μέσω ασύρματων αδρανειακών μονάδων μέτρησης (Wireless Inertial Measurement Units - WIMU), ενσωματωμένων σε αυτόνομους ιμάντες αναπνευστικής συσκευής. Τα δεδομένα μεταδίδονται από το WIMU σε ένα smartphone, που μεταφέρεται από κάθε πρώτο ανταποκριτή και η επεξεργασία των δεδομένων αυτών παρέχει ενδείξεις σχετικά με τη δραστηριότητά του. Το σύστημα έχει σχεδιαστεί για να λειτουργεί αξιόπιστα στις σκληρές και απρόβλεπτες συνθήκες έκτακτης ανάγκης, ενώ μπορεί να γίνει αναγνώριση έως και 17 διαφορετικών δραστηριοτήτων με τη χρήση αλγορίθμων μηχανικής μάθησης και προσομοίωσης μοντέλων (Support Vector Machines - SVM), k-Nearest Neighbours – kNN και Gradient Boosted Trees -GBT).
- Παρακολούθηση δεδομένων υγείας. Καρδιακός παλμός και λοιπά βιομετρικά δεδομένα μπορούν να αντληθούν από ανάλογης λειτουργικότητας αισθητήρες που είναι κατάλληλα προσαρμοσμένοι σε ένδυτα μέσα (κράνη, γιλέκα, ρολόγια, ζώνες, κ.λπ.), καταδεινύοντας τα επίπεδα του άγχους, ή εάν επηρεάζεται η λειτουργικότητα του χρήστη που επιλαμβάνεται στο περιστατικό. Σε ακραίες καταστάσεις τραυματισμών παρέχουν σημαντικότατη ενημέρωση, ενώ σε καταστάσεις ρουτίνας ενεργοποιούν την επιθυμία για βελτίωση της σωματικής αντοχής και εκπαίδευση. Μια αξιόλογη προσέγγιση των ένδυτων συσκευών που σχετίζονται με δεδομένα υγεία (Wearable Health Devices - WHDs) έχουν πραγματοποιήσει οι [401], οι οποίοι οδηγούνται στο συμπέρασμα ότι για να μπορέσουν οι συσκευές να προσφέρουν τα αναμενόμενα οφέλη, απαιτείται αξιόπιστο ευρυζωνικό δίκτυο επικοινωνίας (Εικόνα 153). Οι αρχιτεκτονικές υλοποίησης και οι προδιαγραφές των WHDs είναι εφικτό να

ενταχθούν στον εξοπλισμό των πρώτων ανταποκριτών και να παρέχουν τα οφέλη τους στο πλαίσιο της αποστολής τους. Μια επίσης αξιόλογη αναφορά σε WHDs γίνεται στο [402].

- Κάποιες ένδυτες συσκευές παρέχουν τη δυνατότητα κλήσεων (π.χ. έξυπνα ρολόγια)
- Οι ένδυτες συσκευές θα πρέπει να παρέχουν ένα ελάχιστο επίπεδο αντοχών σε λειτουργία σε εξωτερικές συνθήκες (κρύο, ζέρστη, υγρασία, σκόνη, χτυπήματα, κ.λπ.)
- Διάρκεια ζωής της μπαταρίας. Και στην περίπτωση των ένδυτων μέσων το ζήτημα της μπαταρίας είναι πρωτεύον, καθώς καθορίζει τα επίπεδα λειτουργικότητας και χρηστικότητας των συσκευών.



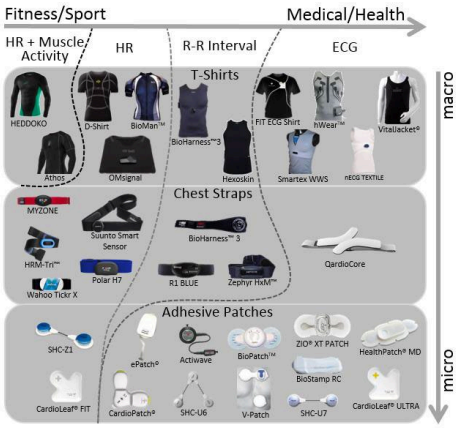
Εικόνα 150. Παραδείγματα ορισμένων φορητών συσκευών υγείας. (1)Αισθητήρας αυτιού (2)Φακοί επαφής (3)BioPatch[50] (4)Έξυπνο ρολόι (5)Ζώνη καρδιακών παλμών (6)Βιομετρικό ρούχο (7)Παρακολούθηση δραστηριότητας [401]



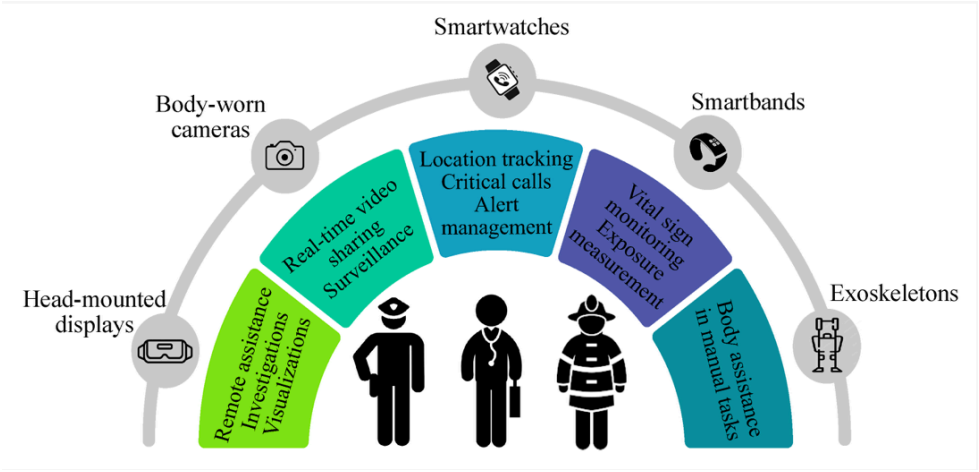
Εικόνα 151. Body Camera (συσκευή, σημείο που φέρεται, εικόνα που δίνει) [403]

Εικόνα 152. Ένδυτα μέσα (wearables) [404], [405]

[50] https://www.youtube.com/watch?v=9es1CUdU1Co&t=9s



Εικόνα 153. Διαφορετικά είδη ενδυτων μέσων και αισθητήρων υγείας [401]



Εικόνα 154. Παραδείγματα ένδυτων μέσων για τη δημόσια ασφάλεια [398]

Τέλος, με αφορμή την επισκόπηση για τα ένδυτα μέσα και την παλέτα των υφιστάμενων τεχνολογικών λύσεων του χώρου, όπως αυτή αποτυπώθηκε στην Εικόνα 154, αξίζει να αναφερθούμε σε έναν νέο όρο (2018[51]), που σχετίζεται με το συγκεκριμένο τεχνολογικό πεδίο, το διαδίκτυο των πραγμάτων που σώζουν ζωές (Internet of Life Saving Things - IoLST), το οποίο σαφέστατα αναφέρεται σε όλες τις τεχνολογικές προτάσεις που βασίζονται στο IoT και την τεχνολογία που το υποστηρίζει και πλαισιώνουν την καθημερινότητα των επαγγελματιών δημόσιας ασφάλειας [406].

5.3.2 Υπηρεσίες (MCx)

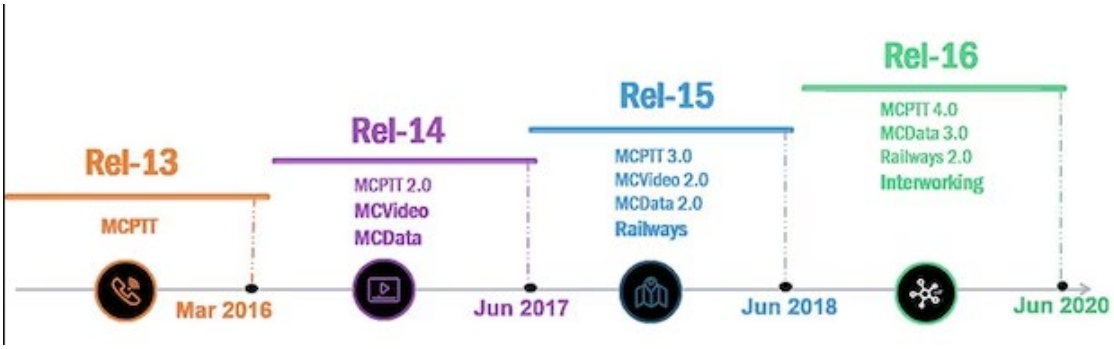
Η σύγχρονη θεώρηση των υπηρεσιών που διατίθενται για τις κρίσιμες επικοινωνίες ενέταξε το σύνολο αυτών σε έναν ορισμό – πρότυπο υπό την ονομασία Υπηρεσίες Κρίσιμης Αποστολής (Mission Critical Services - MC-x), όπου κατά τη γνωστή προσέγγιση το x περιλαμβάνει κάθε υπηρεσία που δύναται να εξυπηρετεί τις κρίσιμες επικοινωνίες. Ο ορισμός υιοθετήθηκε για πρώτη φορά στην έκδοση 13 (Release 13) του οργανισμού προτυποποίησης

[51] Στην ετήσια συνδιάσκεψη της Διεθνούς Ένωσης των Αρχηγών της Αστυνομίας (International Association of Chiefs of Police - IACP)

3GPP, στην προσπάθεια να οριοθετηθούν οι τεχνολογικές δυνατότητες τη δεδομένη χρονική στιγμή, αλλά και έκτοτε, για τη βελτίωση των παρεχόμενων υπηρεσιών στις κρίσιμες επικοινωνίες (Εικόνα 155).

Όπως επανειλημμένως έχει αναφερθεί οι τεχνολογίες στενής ζώνης ήταν ικανές να ικανοποιήσουν τις απαιτήσεις φωνής των υπηρεσιών PTT, αλλά δεν είναι σε θέση να καλύψουν τις ταχέως μεταβαλλόμενες ανάγκες κρίσιμων επικοινωνιακών υποδομών. Αυτά περιλαμβάνουν απαιτήσεις για διαλειτουργικότητα σε διάφορα δίκτυα δημόσιας ασφάλειας, υποστήριξη για δυνατότητες πολυμέσων και άλλα αναδυόμενα παραδείγματα επικοινωνίας. Φυσικό επακόλουθο ήταν η προσοχή των κρίσιμων επικοινωνιών να στραφεί στις κινητές ευρυζωνικές τεχνολογίες όπως το 4G και το 5G [407].

Οι ανάγκες των κρίσμων αποστολών περιλαμβάνουν υψηλή προσβασιμότητα, διαθεσιμότητα και αξιοπιστία της υπηρεσίας, χαμηλή καθυστέρηση, δυνατότητες λειτουργίας σε πραγματικό χρόνο, εξαιρετικά ασφαλείς λειτουργίες, διαλειτουργικότητα με άλλες υπηρεσίες και συστήματα, ιδιωτικές και ομαδικές επικοινωνίες, διαχείριση έκτακτης ανάγκης και ικανότητα παροχής προτεραιοτήτων και QoS [408]. Πέραν λοιπών των όσων αναφέρθηκαν σχετικά με τις υπηρεσίες MCX στην ανάπτυξη των τεχνολογικών πρωτύπων και στις τεχνολογίες, ειδικότερα σχετικά με το 5G στο κεφάλαιο 4.4, αποτυπώνονται στη συνέχεια επιγραμματικά τα κύρια χαρακτηριστικά των υπηρεσιών αυτών.



Εικόνα 155. 3GPP Releases for MCx [407]

5.3.2.1 Φωνητικές υπηρεσίες (MC-PTT)

Με την 13η έκδοση (Release 13), η υπηρεσία MCPTT υποστηρίζει υπηρεσίες φωνητικής επικοινωνίας μεταξύ ενός ζευγαριού χρηστών ή μιας ομάδας πολλών χρηστών, με δυνατότητες και ομαδικών κλήσεων, αλλά και προηγμένες δυνατότητες κλήσεων, συμπεριλαμβανομένων κλήσεων αποκοπής ήχου. Εκτός από την παροχή επικοινωνιών εντός προκαθορισμένων ομάδων, η υπηρεσία MCPTT επιτρέπει στους διαχειριστές να συγχωνεύουν πολλαπλές ομάδες ή χρήστες σε πραγματικό χρόνο για αποτελεσματικό χειρισμό περιστατικών που αναφέρονται [407]. Η απρόσκοπτη φωνητική λειτουργία συνιστά επίγνωση της κατάστασης και της κρίσιμης επικοινωνίας και συνεπάγεται αποτελεσματική

ανταπόκριση [126]. Το MCPTT βασίζεται στις υπηρεσίες ProSe και σε άλλες τεχνικές που παρέχονται από το δίκτυο κορμού, δηλαδη συνδυάζει πολλές τεχνολογίες για να λειτουργήσει κάτω από το ίδιο κέλυφος [91]. Το [54] το MCPTT είναι μια «απαραίτητη» δυνατότητα για κρίσιμες εφαρμογές επικοινωνίας και απαιτεί τη δυνατότητα να συνδεθεί ένας χρήστης με πολλούς, την οποία στερούνται τα εμπορικά ασύρματα δίκτυα επικοινωνίας Εικόνα 156.

Εικόνα 156. Έξυπνα κινητά και tablets για επικοινωνίες MCPTT στη δημόσια ασφάλεια [409]

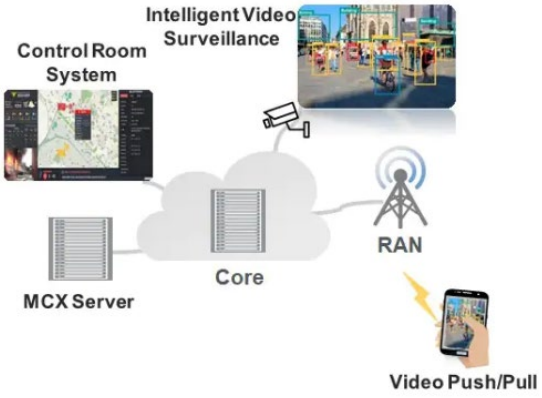
5.3.2.2 Υπηρεσίες μετάδοσης εικόνων (MC-Video)

Το MCVideo, που εισήχθη επίσης στην Έκδοση 14 και οι λειτουργικές του απαιτήσεις καθορίστηκαν στις τεχνικές εκθέσεις 3GPP TS 22.281, 3GPP TS 22.280, 3GPP TS 23.281 και 3GPP TS 23.280 [408]. Η υπηρεσία αυτή επιτρέπει στους χρήστες δημόσιας ασφάλειας να αξιοποιούν τις δυνατότητες επικοινωνίας βίντεο, συμπεριλαμβανομένων ομαδικών και ιδιωτικών βιντεοκλήσεων. Η υπηρεσία MCVideo υποστηρίζει ζωντανή ροή βίντεο, η οποία βοηθά τους διεκπεραιωτές να λαμβάνουν ακριβείς αποφάσεις για καλύτερο χειρισμό καταστάσεων. Επιτρέπει στους χρήστες να επισημάνουν τις βιντεοεπικοινωνίες τους ως «έκτακτης ανάγκης» για να αυξήσουν την προτεραιότητά της. Πρόσθετες λειτουργίες όπως η λήψη βίντεο, η αποθήκευση και αποστολή αυτού σε μεταγενέστερο χρόνο επιτρέπουν στους πρώτους ανταποκριτές να έχουν πρόσβαση σε σημαντικές πληροφορίες σε πραγματικό χρόνο. Στην Εικόνα 157 φάινεται μια στοιχειώδης αρχιτεκτονική της συγκεκριμένης υπηρεσίας, η οποία περιλαμβάνει μια σειρά από λειτουργίες και προδιαγραφές, όπως [408]:

- Λήψη και κωδικοποίηση των πληροφοριών.
- Ασφαλή ροή και αποθήκευση των πληροφοριών.
- Αποκωδικοποίηση και απόδοση των πληροφοριών.
- Επεξεργασία των πληροφοριών, συμπεριλαμβανομένης της δυνατότητας σχολιασμού καρέ και αναγνώρισης χαρακτηριστικών.

- Λειτουργικότητα κρίσιμου επιπέδου αποστολής και δημόσιας ασφάλειας (π.χ. ομαδικές συνεδρίες, συνεργασίες, εμπιστευτικότητα από άκρο σε άκρο, επικοινωνίες τύπου έκτακτης ανάγκης) και απόδοση (π.χ. χαμηλή καθυστέρηση).
- Μετάδοση και έλεγχος των παραμέτρων που σχετίζονται με αυτές τις λειτουργίες.
- Ασφαλή λειτουργία.
- Ορισμό και διαμόρφωση ομάδων και εφαρμογών MCVideo.
- Διαμόρφωση των προφίλ χρηστών MCVideo και των UE MCVideo.
- Διαλειτουργικότητα με άλλες υπηρεσίες και συστήματα.

Ενώ η ροή βίντεο αποτελεί μέρος της Υπηρεσίας MCVideo, η μεταφορά βίντεο κλιπ που είναι αποθηκευμένο ως αρχείο που περιέχει δεδομένα βίντεο, σε πραγματικό χρόνο ή εκτός σύνδεσης, καλύπτεται από την Υπηρεσία MCData, όπως ορίζεται στο 3GPP TS 22.282. Μια ροή βίντεο MCVideo μπορεί να συσχετιστεί με μια αυτόνομη ομάδα χρηστών MCVideo ή μπορεί να είναι μία από τις ροές μιας ομάδας πολυμέσων MCX Service.



Εικόνα 157. Υπηρεσίες μετάδοσης εικόνων [407]

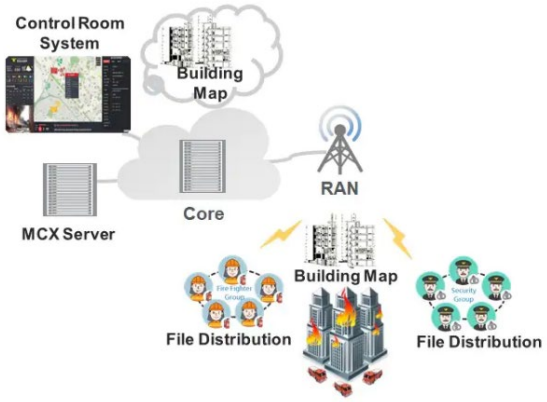
5.3.2.3 Υπηρεσίες μετάδοσης δεδομένων (MC-Data)

Η υπηρεσία MCData, που εισήχθη στο Release-14, προσφέρει λειτουργίες ανταλλαγής μηνυμάτων, διανομής αρχείων και ροής δεδομένων, οι οποίες επιτρέπουν στους χρήστες δημόσιας ασφάλειας να έχουν μια πιο εξελιγμένη εμπειρία. Χρησιμοποιώντας την υπηρεσία MCData, οι πρώτοι ανταποκριτές μπορούν να μοιράζονται προρυθμισμένα μηνύματα εντολών και να διαβιβάζουν στο κέντρο ελέγχου και διοίκησης φωτογραφίες και βίντεο του αναφερόμενου περιστατικού, κάτι που βοηθά στην αυξημένη επίγνωση της κατάστασης και στην καλύτερη λήψη αποφάσεων [407].

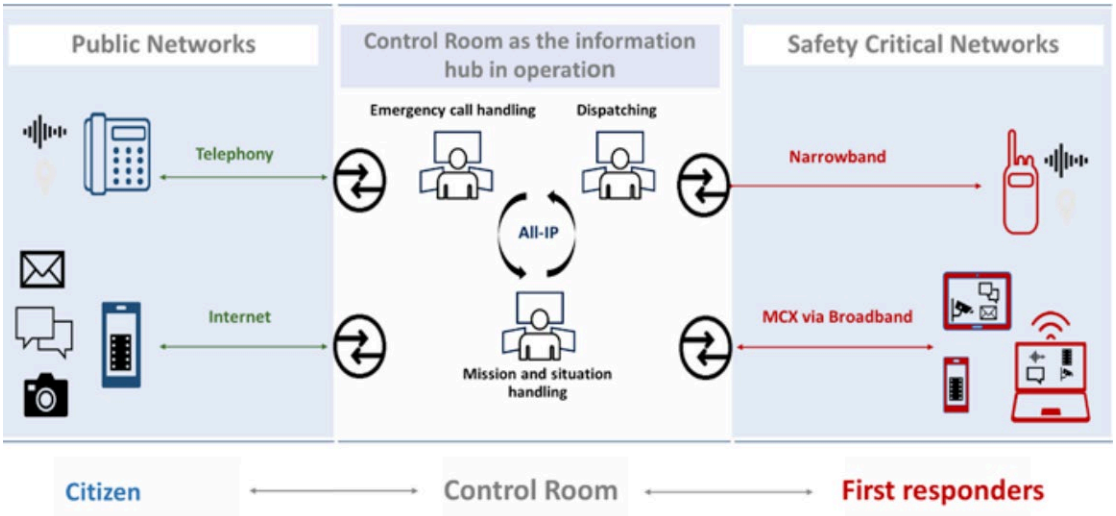
Η υπηρεσία MCData υποστηρίζει επικοινωνία μεταξύ ενός ζεύγους χρηστών (δηλαδή επικοινωνία ένας προς έναν) και πολλών χρηστών (δηλαδή ομαδική επικοινωνία), όπου κάθε χρήστης έχει τη δυνατότητα να ενεργήσει:

- κοινή χρήση δεδομένων χρησιμοποιώντας την υπηρεσία Short Data Service (SDS)
- κοινή χρήση αρχείων χρησιμοποιώντας την υπηρεσία Διανομής αρχείων (FD)

Φυσικά, όταν αναφερόμαστε σε δεδομένα, γίνεται αντιληπτό ότι μπορεί να αφορά κάθε είδους πληροφορία που συλλέγεται από τους επαγγελματίες της δημόσιας ασφάλειας και ταυτόχρονα κάθε είδους δεδομένα που θα ήθελαν να έχουν πρόσβαση στο πεδίο (Εικόνα 158) Οι MCX επικοινωνίες απαιτούν αξιόπιστα ευρυζωνικά δίκτυα (Εικόνα 159). Έτσι επεκτείνονται οι δυνατότητες των πρώτων ανταποκριτών και ουσιαστικά αντλούν πληροφορίες από τους πολίτες, διαμέσου του κέντρου ελέγχου και διοίκησης. Σημαντικό είναι στο σημείο αυτό ν` αναφερθεί ότι τα πρότυπα παρέχουν τη δυνατότητα για χαμηλή πολυπλοκότητα και κόστος, ως αντίπαλο δέος στα κυψελωειδή δίκτυα των παρόχων. Παράλληλα, με τη χρήση των ευρυζωνικών δικτύων αλλά και των τεχνολογιών στενής ζώνης, οι υπηρεσίες της δημόσιας ασφάλειας αλληλεπιδρούν με τα εμπορικά δίκτυα, αλλά διατηρούν την αυτοτέλεια και έλεγχο των PSNs [410].



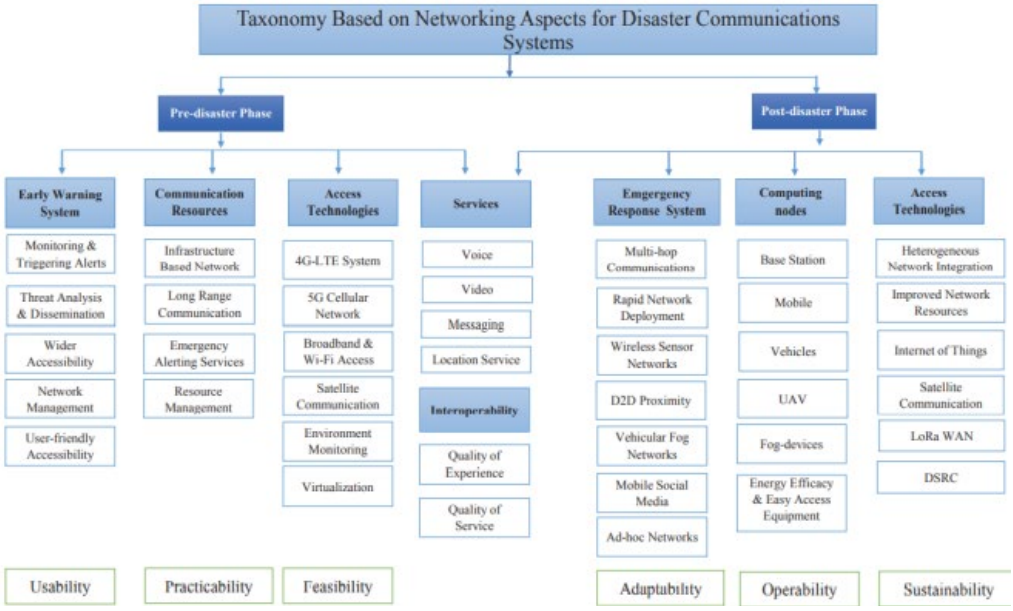
Εικόνα 158. Υπηρεσίες μετάδοσης δεδομένων [407]



Εικόνα 159. Μοντέλο επικοινωνιών πολιτών και πρώτων ανταποκριτών με το κέντρο ελέγχου και διοίκησης [410]

5.3.3 Εμπλεκόμενες τεχνολογίες

Ο εξοπλισμός και οι υπηρεσίες που διατίθενται είναι πλέον άμεσα συνυφασμένες με τις τεχνολογικές λύσεις που αναπτύσσονται στο πεδίο. Οι εξελίξεις είναι ταχύτατες και λαμβάνουν χώρα με το ρυθμό ανάπτυξης του IoT. Την εμπλοκή του IoT στη δημόσια ασφάλεια την αναλύσαμε ήδη στο κεφάλαιο 4.10.. Ωστόσο, στο σημείο αυτό κρίνεται σκόπιμο να αποτυπωθεί η επισκόπηση που επιχειρήθηκε από τους [411], με την οποία μέσα από την ανάπτυξη ενός συστήματος διαχείρισης καταστροφών αναδεικνύεται η σημασία των δικτύων του IoT και του 5G για τις έξυπνες πόλεις και κατ` επέκταση τη δημόσια ασφάλεια. Δίκτυα ισχυρά, ανθεκτικά, αξιόπιστα, αποτελεσματικά και ενεργειακά αποδοτικά παρέχουν βελτιωμένη ποιότητα υπηρεσιών, καλύτερη συνδεσιμότητα, ταχεία ανάπτυξη και μειωμένη κατανάλωση σε περίπτωση που κληθούν να αντιμετωπίσουν καταστροφικά φαινόμενα. Μάλιστα, στην ίδια έρευνα γίνεται προσέγγιση με χρονική διάκριση, δηλαδή τις εμπλεκόμενες τεχνολογίες προ της καταστροφής, οι οποίες εστιάζουν στο να παρέχουν επίγνωση της κατάστασης και σ` αυτές που εμπλέκονται μετά την καταστροφή που εστιάζουν στο να παρέχουν υπηρεσίες γρήγορης ανταπόκρισης των εμπλεκομένων οργανισμών δημόσιας ασφάλειας, με σαφή στόχο να σώσουν ζωές. Μια εποπτική ανάδειξη του συγκεκριμένου διαχωρισμού φαίνεται στην Εικόνα 160, με τη μορφή σχεδίου, τα στοιχεία του οποίου έχουν αναλυθεί διεξοδικά στο κεφάλαιο 4.

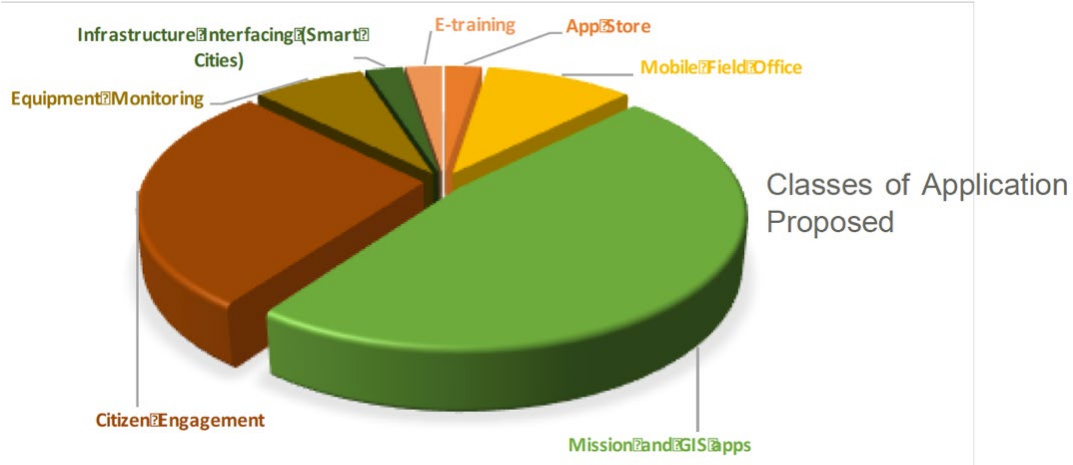


Εικόνα 160. Αρχιτεκτονική του συστήματος επικοινωνίας PPDR [411]

Το οικοσύστημα εφαρμογών είναι μια από τις ταχύτερα αναπτυσσόμενες αγορές στην Ευρώπη, αλλά και παγκοσμίως και θεωρείται βασικό στοιχείο της ψηφιακής ενιαίας αγοράς, τα οποίο έχει ξεχωριστή συμβολή στις λειτουργίες της δημόσιας ασφάλειας. Οι απαιτήσεις αυξάνουν και οι έξυπνες συσκευές από τη μία και τα ευρυζωνικά δίκτυα επικοινωνίας από

την άλλη δημιουργούν τις κατάλληλες προυποθέσεις για νέες, εξελιγμένες εφαρμογές για τους επαγγελματίες της δημόσιας ασφάλειας. Μια τέτοια κατηγοριοποίηση εφαρμογών που είναι προσανατολισμένη στη δημόσια προστασία και διαχείριση ανακούφισης των συνεπειών από καταστροφές (PPDR) έχει αποτυπωθεί στο [412]. Τα συμπεράσματα από την έρευνα αυτή είναι αξιόλογα και μπορούν να γενικευτούν, καθώς προέκυψαν από τη μελέτη των διαδικασιών ανάπτυξη 40 εφαρμογών όλων των θεματικών της Εικόνα 161. Αυτό που συνάγεται είναι ότι η ανάπτυξη των εφαρμογών σε επίπεδο λογισμικού είναι μια αρκετά εφικτή διαδικασία, καθώς δεν υπάρχει έλλειψη ιδεών ή βούλησης υλοποίησης νέων εφαρμογών, πλην όμως υπάρχουν τρία κυρίαρχα ζητήματα που χρήζουν ιδιαίτερης προσοχής και επιμέλειας:

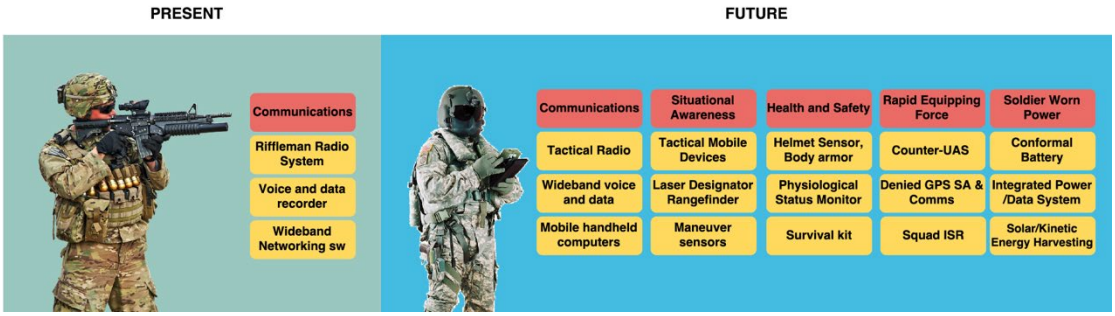
- Γενικός Κανονισμός για την Προστασία Δεδομένων - GDPR: Ο GDPR απαιτεί για τη χρήση των δεδομένων να υφίσταται συναίνεση των χρηστών. Εάν ένας χρήστης θέλει να κατεβάσει την εκάστοτε εφαρμογή, ενδέχεται να του ζητηθεί να παράσχει προσωπικά δεδομένα και πληροφορίες, επομένως αυτή η σαφής συγκατάθεση πρέπει να δοθεί από τον χρήστη παράλληλα με την παροχή σ` αυτόν των νομίμων δικαιωμάτων του για την ανάκτηση και διαγραφή των δεδομένων του.
- Απόρρητο και ιδιοκτησία δεδομένων: Όπως αναφέρθηκε προηγουμένως, το απόρρητο θα είναι ένας εξαιρετικά σημαντικός παράγοντας όσον αφορά τις εφαρμογές PPDR, καθώς ενδέχεται να μεταφέρονται ευαίσθητες πληροφορίες (ιατρικά, βιομετρικά δεδομένα, κ.λπ.).
- Εντοπισμός δεδομένων: Σε σχέση με το απόρρητο, η τοπική προσαρμογή δεδομένων θα εμπόδιζε τα κράτη μέλη να μοιράζονται δεδομένα.



Εικόνα 161. Ενδεικτικές κατηγορίες εφαρμογών για τη δημόσια ασφάλεια [412].

5.4 Επίπεδο Επεξεργασίας Δεδομένων

Με τις διεργασίες του επιπέδου επεξεργασίας δεδομένων επιτυγχάνεται η κατανόηση της διακινούμενης πληροφορίας. Εδώ εντάσσονται όλες οι ενέργειες ενσωμάτωσης της συλλεγόμενης, μεταφερόμενης, συγκεντρωθείσας και επεξεργασμένης πληροφορίας σε μια κοινή υποδομή συστήματος, που θα οδηγήσει στη συνολική επίγνωση της κατάστασης, μέσω των κέντρων ελέγχου και διοίκησης. Για την καλύτερη αποδόμηση του τρόπου που αυτό λαμβάνει χώρα, επιλέξαμε να περιγράψουμε τα κομμάτια που συνθέτουν αυτό το τμήμα της αρχιτεκτονικής ως δύο διακριτά υποεπίπεδα, αυτό της διοίκησης και ελέγχου και αυτό της επίγνωσης της κατάστασης, η οποία σε κάθε περίπτωση συνάγει μια διακριτή και σημαντική πτυχή του επιπέδου επεξεργασία δεδομένων, αυτή της έγκαιρης προειδοποίησης (early learning / alerting). Είναι απόλυτα σαφές ότι ένα από τα σημαντικότερα «όπλα» του επαγγελματία της δημόσιας ασφάλειας του μέλλοντος θα είναι η επίγνωση της κατάστασης (Εικόνα 162). Κάποια από τα στοιχεία που απαριθμούνται στην εικόνα έχουν ήδη τεθεί στη διάθεσή του, για άλλα υπάρχει ακόμη αρκετός δρόμος και εμπόδια να ξεπεραστούν ώστε να γίνουν χειροπιαστή πραγματικότητα.



Εικόνα 162. Ο επαγγελματίας δημόσιας ασφάλειας του σήμερα και του μέλλοντος [140]

5.4.1 Διοίκηση και έλεγχος

Τα κέντρα διοίκησης και ελέγχου περιλαμβάνουν συστήματα, εφαρμογές, εργαλεία, πολιτικές και άτομα που είναι υπεύθυνα για τη συντήρηση, τη διαχείριση, λειτουργία και συντονισμό ολόκληρου του κρίσιμου δικτύου επικοινωνιών με αξιόπιστο, ασφαλή και αποδοτικό τρόπο [57]. Η χωροταξική κατανομή τους και πυκνότητα σε σχέση με τις μονάδες που βρίσκονται στο πεδίο ποικίλλει και σε πολλές περιπτώσεις εξαρτάται από τη χώρα, την περιοχή, την υπηρεσία, αλλά και παράγοντες όπως το μέγεθος της περιοχής κάλυψης, τις ιδιαιτερότητες της αποστολής και του αντικειμένου, τυχόν σκοπιμότητες που σχετίζονται με την πολιτική αντιμετώπισης. Ιδανικά σε σχέση με τη διαλειτουργικότητα και απόδοση, όλα τα συστήματα αυτά θα πρέπει να συνδέονται, συντονίζονται και επικοινωνούν χωρίς προβλήματα, ενεργώντας με αυτοτέλεια, αλλά και κοινό στόχο και σκοπό. Χαρακτηριστικό παράδειγμα

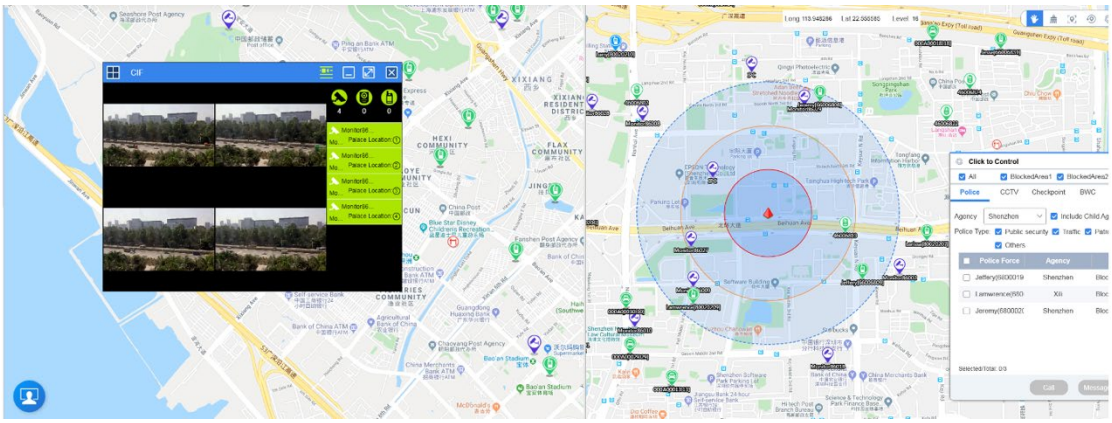
τέτοιων αυτοτελών κέντρων αποτελούν τα PSAP, για τα οποία έγινε λόγος στο κεφάλαιο 5.1.2.2.

Κάθε κέντρο διοίκησης και ελέγχου θα πρέπει να παρέχει τη δυνατότητα πλήρους συντονισμού των δυνάμεων που αναφέρονται σ` αυτό, να εντοπίζει και θεραπεύει γρήγορα τυχόν λειτουργικά προβλήματα, η προβλήματα δικτύων και συνδεσιμότητας, παρακολουθεί την απόδοσή του και εντάσσει στην αναδιοργάνωση βελτιώσεις από τρωτότητες, έχει διαρκή επικοινωνία με τις απαιτούμενες βάσεις δεδομένων που άμεσα ή έμμεσα σχετίζονται με τη δημόσια ασφάλεια. Παράλληλα, με δεδομένο ότι στα κέντρα διοίκησης και ελέγχου διαλειτουργούν τις περισσότερες φορές πολλοί και ξεχωριστοί φορείς, θα πρέπει να υπάρχει σαφής προσδιορισμός των καθηκόντων και αρμοδιοτήτων τόσο σε επίπεδο υπηρεσιών, όσο και ενδουπηρεσικά. Θεωρείται βέλτιστη πρακτική να υπάρχει μνημόνιο ενεργειών για περιπτώσεις που απασχολούν σε επίπεδο περιστατικών ρουτίνας, έως και τα μη συνήθη έκτακτα γεγονότα και καταστάσεις που απαιτούν δύσκολους και απαιτητικούς χειρισμούς. Στο πλαίσιο αυτό πρέπει να είναι σαφώς καθορισμένο ποιος επικοινωνεί με ποιους, ποιος διοχετεύει την πληροφόρηση και με ποιον τρόπο, ποιος λαμβάνει τις αποφάσεις, ποιος διαβιβάζει αυτές στους επαγγελματίες στο πεδίο και με ποιον τρόπο. Επιπλέον, οι διαδικασίες θα πρέπει να έχουν χαρακτήρα σαφήνειας, απλότητας και εμπιστευτικότητας, ενώ θα πρέπει να λαμβάνεται μέριμνα για καταγραφή των ενεργειών και αποθήκευση όλων των κρίσμων στοιχείων και δεδομένων για περαιτέρω αξιοποίηση, αλλά και εκ των υστέρων μελέτη για αξιολόγηση του περιστατικού.

Κάποιες από τις λειτουργικές δυνατότητες, αλλά και τις επιθυμητές προδιαγραφές ενός συστήματος διοίκησης και ελέγχου ενός PSN είναι (Εικόνα 163):

- Όλες οι δυνάμεις σε έναν χάρτη, για καλύτερη εποπτική αποτύπωση και αντίληψη των επιχειρησιακών δυνατοτήτων από τους συντονιστές
- Δυνατότητα πολυμεσικής επικοινωνίας, για καλύτερη αντίληψη του περιστατικού από τον συντονιστή και βέλτιστη αξιολόγηση
- Ταχύτατη επικοινωνία φωνής, σε έναν χρήστη ή σε ομάδα χρηστών, πολυμεσικής επικοινωνίας με τις δυνάμεις στο πεδίο (PTT, MCx) με τις ελάχιστες δυνατές ενέργειες ή κινήσεις (ένα κλικ, ένα διαδραστικό εικονίδιο επί της οθόνης ελέγχου, ένα αναδυόμενο παράθυρο πληροφοριών για κλήση ή απσοτολή βίντεο, κ.λπ.)
- Γρήγορη και εύκολη δυνατότητα εντοπισμό δυνάμεων που βρίσκονται πλησίον του περιστατικού, εκτίμησης του χρόνου μετάβασης, ανάδειξης επί της οθόνης της βέλτιστης διαδρομής, ώστε να κατευθύνονται, συντονίζονται και ελέγχονται οι διαθέσιμοι πόροι με τον καλύτερο δυνατό τρόπο
- Καταγραφή όλων των ενεργειών (φωνής, εικόνων, βίντεο, διαδρομών, κ.λπ.), για όλους τους λόγους που έχουν αναλυθεί ήδη παραπάνω

- Εύκολη διαλειτουργικότητα με συναφείς υπηρεσίες και συνεργασία χωρίς να απαιτείται πολύτιμος χρόνος και ενέργεια.



Εικόνα 163. Χαρακτηριστικά στιγμιότυπα κέντρου διοίκησης και ελέγχου και λειτουργικότητες αυτών – Hytera Command and Control center[52]

5.4.2 Επίγνωση της κατάστασης

Η έννοια της επίγνωσης της κατάστασης συναντάται σε πολλές περιπτώσεις στη βιβλιογραφία ως συνώνυμη της κοινής επιχειρησιακής εικόνας (Common Operational Picture - COP). Ωστόσο, αφορά μια κατάσταση που συνιστά το αποτέλεσμα της COP, καθώς όλα τα στοιχεία του PSN που έχουμε αναλύσει ως τώρα παρέχουν τη δική τους συνεισφορά ώστε να προκύψει το επιθυμητό, ώστε να οδηγηθούμε σε λήψη απόφασης. Οι χρόνοι μεταξύ των σταδίων που παρουσιάζονται στην Εικόνα 164 είναι το πρώτο κρίσιμο στοιχείο, ενώ εξίσου σημαντικά κρίνονται η πληρότητα της πληροφορίας, η εγκυρότητα και έγκαιρη αποστολή της, η αδιάλειπτη ροή κρίσιμων δεδομένων, καθώς υφίσταται εξέλιξη και σε όλες σχεδόν περιπτώσεις δυναμική μεταβολή των συνθηκών.

Τα στοιχεία που συγκετρώνονται στο κέντρο διοίκησης και ελέγχου, επεξεργάζονται και επαναδιαβιβάζονται στο πεδίο, ώστε οι πρώτοι ανταποκριτές να συνεισφέρουν και πάλι πρόσθετα στοιχεία. Η διαδικασία αυτή ακολουθεί μια επαναλαμβανόμενη διαδικασία μεταφοράς δεδομένων και πληροφόρησης, καθώς το ζητούμενο είναι το υποκειμενικό στοιχείο της αντίληψης κάθε πρώτου ανταποκριτή, αλλά και των χειριστών στο κέντρο ελέγχου να μετατραπεί σε αντικειμενικό στοιχείο που συνθέτει ένα περιστατικό.

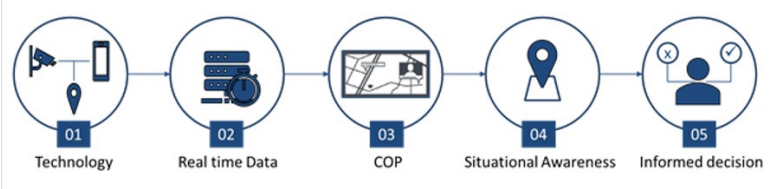
Στο σημείο αυτό αξίζει να σταθούμε στην πολύτιμη συμβολή της τεχνολογίας. Και σαφώς δεν αναφερόμαστε στην τεχνολογία που έχει «αναλάβει» να συλλέξει την πληροφορία από το πεδίο, ή να τη μεταδόσει στο κέντρο ελέγχου, αλλά στην τεχνολογία που επωμίζεται την ταχύτατη επεξεργασία της πληροφορίας. Ο όγκος των δεδομένων στις περισσότερες περιπτώσεις κρίσιμων περιστατικών είναι τεράστιος και η επεξεργασία τους θα πρέπει να

[52] https://www.hytera.com/en/product-new/command-dispatch/public-safety-command-control.html

λάβει χώρα ιδανικά σε ελάχιστο χρόνο, ή σε κάθε περίπτωση σε χρόνο που δεν θα αποβεί επιζήμιος και θα έχει ως αποτέλεσμα την απώλεια ανθρώπινων ζωών. Η ανθρώπινη παρέμβαση και ευφυία στην περίπτωση αυτή έχει σημαντικούς αντιπάλους, όπως ο χρόνος και διαθεσιμότητα πόρων. Συνεπώς τη λύση καλείται να δώσει η τεχνολογία μέσω της τεχνητής νοημοσύνης και των διαδικασιών αποδοτικής επεξεργασίας μεγάλων δεδομένων, με τη συμβολή αλγορίθμων της μηχανικής μάθησης. Το πεδίο αυτό εμφανίζει, όπως είναι αντιληπτό, τεράστιες προκλήσεις, ωστόσο έχει βασικά προβλήματα που θα πρέπει να ξεπεραστούν και το κύριο εξ αυτών είναι η αξιοπιστία που δύναται να παρέχει.

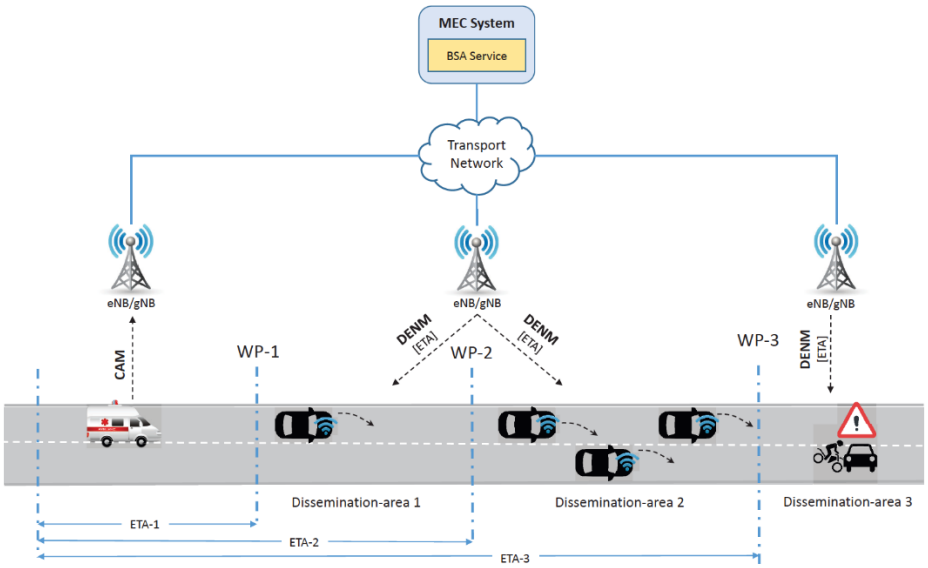
Είναι αυτονόητο ότι η επίγνωση της κατάστασης περιλαμβάνει ένα ευρύ φάσμα εξοπλισμού, λογισμικού και υλικού που συνεργάζεται για να οδηγήσει στο επιθυμητό αποτέλεσμα. Αυτό συνάγεται και από το παράδειγμα της επισκόπηση που παρουσιάστηκε στο [413] για τα συστήματα επιτήρησης χώρων στο πλαίσιο της δημόσιας ασφάλειας, όπου εκτός των άλλων αναδείχθηκαν τα προβλήματα αξιολόγησης των δεδομένων που συλλέγονται από τα διάφορα μέρη του δικτύου, καθώς ο απώτερος στόχος των συστημάτων επιτήρησης είναι η αυτόματη αξιολόγηση των δραστηριοτήτων του περιβάλλοντος και η επισήμανση και παρουσίαση των ύποπτων συμβάντων σε πραγματικό χρόνο στον χειριστή για την πρόληψη επικίνδυνων καταστάσεων. Στη συγκεκριμένη εργασία, για αποδοτική αξιοποίηση των δεδομένων προτάθηκαν τεχνικές συγχώνευσης αυτών που δύνανται να οδηγήσουν σε βελτιώμενες εκτιμήσεις, αλλά και τη γενικότερη ευρωστία του συστήματος, αξιοποιώντας τον πλεονασμό που προσφέρουν πολλοί αισθητήρες που παρατηρούν την ίδια σκηνή. Σύμμαχοι στην προσπάθεια αυτοί καθίστανται οι ευφυείς αισθητήρες, οι οποίοι είναι εξοπλισμένοι με μικροεπεξεργαστές για την εκτέλεση κατανεμημένης επεξεργασίας και υπολογισμών δεδομένων, μειώνοντας τον υπολογιστικό φόρτο ενός κεντρικού κόμβου επεξεργασίας.

Τέλος, ο πλέον σημαντικός σύμμαχος στην επίτευξη βελτιωμένης επίγνωσης της κατάστασης είναι τα ευρυζωνικά δίκτυα επικοινωνίας και συγκεκριμένα το 5G. Χαρακτηριστικό παράδειγμα τέτοιας υλοποίησης στη βιβλιογραφία είναι η εφαρμογή που πρότειναν οι [414], οι οποίοι αξιοποίησαν τις δυνατότητες του 5G MEC για τη βελτιωμένη επίγνωση της κατάστασης σε συγκεκριμένη περίπτωση χρήσης, κατά την οποία το ζητούμενο είναι να δημιουργηθεί από τα οχήματα άμεσης επέμβασης των υπηρεσιών δημόσιας ασφάλειας ασφαλής και ανοιχτή διαδρομή διέλευσης ασθενοφόρου, που μεταφέρει επείγον περιστατικό.



Εικόνα 164. Στάδια μέχρι τη λήψη απόφασης σε ένα PSN[53]

[53] https://www.comtechlocation.com/blog/situational-awareness-in-public-safety



Εικόνα 165. Επίγνωση της κατάστασης με αναδρομολόγηση δεδομένων θέσης, ταχύτητας, χώρου σε πραγματικό χρόνο και χρήση συστήματος 5G MEC [414]

5.5 Επίπεδο εφαρμογών

Στο επίπεδο εφαρμογών συλλέγουμε και επεξεργαζόμαστε τα δεδομένα που μεταδίδονται από το επίπεδο δικτύου ώστε να πραγματοποιηθούν κάποιες περαιτέρω διεργασίες στο πλαίσιο αξιολόγησης και αξιοποίησης της πληροφορίας. Συγκεκριμένα, στο επίπεδο αυτό:

(i)Πραγματοποιείται ξεκαθάρισμα και απόρριψη τυχόν περιττών ή μη χρήσιμων δεδομένων για την αποφυγή υπερφόρτωσης του δικτύου.

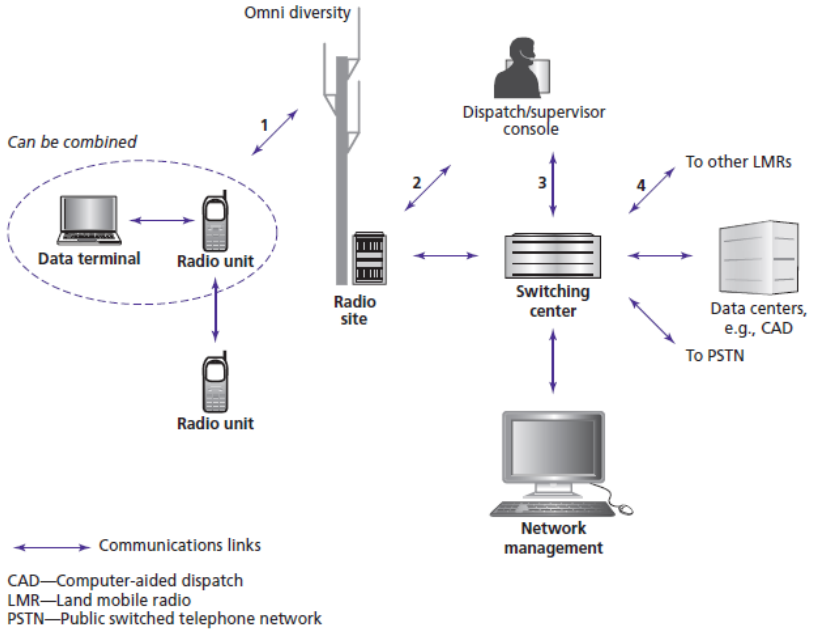
(ii)Υλοποιείται μια αρχική ομαδοποίηση των πληροφοριών που θα οδηγήσει αποδοτικά σε ικανοποιητικά επίπεδα κατανόησης και συνειδητοποίησης της κατάστασης,

(iii)Γίνεται σύγκριση των πληροφοριών που δεχόμαστε με γνωστά καταγεγραμμένα μοντέλα αντίδρασης, που οδηγεί σε ικανοποιητικές πρώτες εκτιμήσεις τόσο σε τεχνολογικό, όσο και σε ρεαλιστικό επίπεδο. Μέσα από τέτοιες διαδικασίες είναι εφικτό να οδηγηθούμε σε βέλτιστη ανάπτυξη υποστηρικτικών δομών του δικτύου επικοινωνίας (UAVs/ρομπότ, κ.λπ.), σε επιλογές κατάλληλων διαδρομών και θέσεων των πρώτων ανταποκριτών στο πεδίο και άλλες σημαντικές αποφάσεις που λαμβάνονται σε πραγματικό χρόνο.

(v)Συγκεντρώνονται πληροφορίες που οδηγούν σε εξαγωγή γνώσης συμβάντων έκτακτης ανάγκης και δραστηριοτήτων αντίδρασης και αξιοποιούνται κατάλληλα άλλες βοηθητικές βάσεις δεδομένων (π.χ. Συστήματα Γεωγραφικών Πληροφοριών (GIS)), Ηλεκτρονικά μητρώα υγεία, κ.αλ.).

Σε απόλυτη αναλογία ορισμών, οι διεργασίες που εντάσσονται στο επίπεδο εφαρμογών ορίζονται ως Mission-x Platform. Με τον τρόπο αυτό περιγράφεται η συνολική πλατφόρμα

που περιλαμβάνει όλες τις υπηρεσίες και τις εφαρμογές της αποστολής, τόσο των πρώτων ανταποκριτών, όσο και των ανθρώπων της δημόσιας ασφάλειας που δρουν στα κέντρα ελέγχου και διοίκησης. Δύο μεγάλες κατηγορίες περιγράφουν όσα ήδη αναφέρθηκαν. Ο έλεγχος και η ομαδοποίηση δεδομένων και η αξιολόγηση και αξιοποίηση της διακινούμενης πληροφορίας. Για αμφότερες εξ αυτών και τα στοιχεία που τις συνθέτουν έχει γίνει εκτενής αναφορά. Ωστόσο, πλήρως συνοπτικά θα αναφερθούμε σε στοιχεία που θεωρούνται αξιοσημείωτα για κάθε θεματική. Θα ήταν χρήσιμο στο σημείο αυτό να γίνει μια επισκόπηση της τυπικής δομής της αρχιτεκτονικής ενός PSN και των στοιχείων που το συνθέτουν, όπως αυτά αποτυπώνονται στην Εικόνα 166, ώστε στη συνέχεια να μπορέσουμε να αντιληφθούμε τα σημεία αναφοράς για το επίπεδο εφαρμογών, το οποίο ουσιαστικά υλοποιεί την επεξεργασία των δεδομένων.



Εικόνα 166. Τυπική αρχιτεκτονική ενός PSN [415]

5.5.1 Έλεγχος και ομαδοποίηση δεδομένων

Κύρια συμβολή στον έλεγχο και ομαδοποίηση των δεδομένων, λειτουργίες κατά τις οποίες μεγάλες ποσότητες δεδομένων συγκετρώνονται και επεξεργάζονται έχουν δύο βασικές τεχνολογίες:

(α)Υπολογισμός αιχμής πολλαπλής πρόσβασης (Multi-access Edge Computing - MEC)

(β)Συγχώνευση δεδομένων (Data Fusion)

5.5.1.1 Υπολογισμός αιχμής πολλαπλής πρόσβασης (MEC)

Το MEC είναι ένας τύπος αρχιτεκτονικής δικτύου που παρέχει δυνατότητες υπολογιστικού νέφους στην άκρη του δικτύου. Ο στόχος του MEC είναι να μειώσει τον λανθάνοντα χρόνο,

να εξασφαλίσει εξαιρετικά αποτελεσματική λειτουργία δικτύου και υπηρεσιών και να βελτιώσει την εμπειρία του πελάτη. Όπως αναφέραμε ήδη στο κεφάλαιο 4.11.2 αφορά σε μια εξέλιξη και βελτίωση του cloud computing, καθώς με στόχο να λύσει τα προβλήματα που αυτό εμφανίζει μεταφέρει τους υπολογισμούς στο άκρο του δικτύου και επομένως πιο κοντά στο χρήστη ή στην πηγή των δεδομένων. Τα τεχνικά και αρχιτεκτονικά πρότυπα για υπολογιστές αιχμής πολλαπλής πρόσβασης έχουν αναπτυχθεί κυρίως από το ETSI και μάλσιτα στην 17η έκδοση, στο πλαίσιο της ανάπτυξης του 5G.

Βασικά πλεονεκτήματα του MEC είναι ότι οι εφαρμογές αποδίδουν καλύτερα και οι εργασίες επεξεργασίας γίνονται πιο γρήγορα καθώς εκτελούνται κοντά στο σημείο που χρησιμοποιούνται. Το περιβάλλον MEC επιτρέπει εξαιρετικά χαμηλό λανθάνοντα χρόνο και υψηλό εύρος ζώνης, μαζί με δεδομένα και πληροφορίες του ραδιοδικτύου που μπορούν να χρησιμοποιηθούν από εφαρμογές σε πραγματικό χρόνο. Τα δίκτυα ραδιοπρόσβασης (RAN) είναι κρίσιμα σημεία σύνδεσης μεταξύ των συσκευών τελικού χρήστη και του υπόλοιπου δικτύου ενός χειριστή. Το RAN συνδέει συσκευές τελικού χρήστη με υπηρεσίες που ενεργοποιούνται από τον πάροχο. Επιπλέον, οι υλοποιήσεις MEC καθιστούν το RAN προσβάσιμο σε εξουσιοδοτημένους προγραμματιστές εφαρμογών και παρόχους, γεγονός που τους επιτρέπει να χρησιμοποιούν υπολογιστική ακμή σε επίπεδο εφαρμογής, καθώς και σε χαμηλότερο επίπεδο λειτουργιών δικτύου και επεξεργασίας πληροφοριών [416].

Από την ίδια πηγή προκύπτει ότι τα βασικά πεδία εφαρμογής της αρχιτεκτονικής MEC είναι:

- Αναλύσεις δεδομένων και βίντεο
- Υπηρεσίες παρακολούθησης τοποθεσίας για κινητές συσκευές
- IoT και διασύνδεση συσκευών IoT
- Επαυξημένη πραγματικότητα και εικονική πραγματικότητα

5.5.1.2 Συγχώνευση δεδομένων (Data Fusion)

Το Data Fusion περιλαμβάνει την ενοποίηση δεδομένων και γνώσης από διάφορες πηγές μέσα από διάφορες μεθόδους και τη χρήση σχετικών αλγορίθμων [417]. Στην ίδια επιστημονική επισκόπηση αναφέρεται ότι η συγχώνευση δεδομένων είναι ένας πολυεπιστημονικός τομέας που περιλαμβάνει πολλά πεδία και είναι δύσκολο να καθοριστεί μια σαφή και αυστηρή ταξινόμηση. Οι χρησιμοποιούμενες μέθοδοι και τεχνικές μπορούν να χωριστούν σύμφωνα με διάφορα κριτήρια που μεταξύ άλλων περιλαμβάνουν τις σχέσεις μεταξύ των πηγών δεδομένων, τους τύπους και τη φύση δεδομένων, το είδος τους (μετρήσεις, σήματα, χαρακτηριστικά, αποφάσεις, κ.λπ.), το επίπεδο ανάμειξής τους και τέλος τον τύπο της αρχιτεκτονικής τους (κεντρική, αποκετρωμένη, κατανεμημένη).

Ο κόσμος της δημόσιας ασφάλειας, ειδικότερα με τη μετάβαση στην ευρυζωνική τεχνολογία επικοινωνίας και τις εφαρμογές του IoT, παράγει πλέον μεγάλο όγκο δεδομένων. Επιπλέον, τα ακατέργαστα δεδομένα που συλλέγονται από διάφορα περιβάλλοντα είναι ετερογενή,

σύνθετα, ατελή και εξαιρετικά μεγάλης κλίμακας, γεγονός που δημιουργεί τη βασική πρόκληση της μετατροπής αυτών σε χρήσιμες και επεξεργάσιμες πληροφορίες. Όλα τα είδη τεχνολογιών επεξεργασίας δεδομένων, συμπεριλαμβανομένης ενδεικτικά της προεπεξεργασίας, της αποθήκευσης, της μεταφοράς, της συγχώνευσης, της ανάλυσης και της ανάκτησης πληροφοριών είναι σημαντικά για την επίλυση αυτών των προβλημάτων [418].

Ωστόσο, επιλέξαμε να αναφερθούμε εντελώς ενδεικτικά στη συγχώνευση των δεδομένων, καθώς παρέχει τη δυνατότητα εφαρμογής ένα ευρύτατου πεδίο έρευνας και μεθόδων. Μια από αυτές που ξεχωρίζει είναι η μηχανική μάθηση, καθώς σε πολλές περιπτώσεις έχουμε να χειριστούμε ατελή και ακατέργαστα δεδομένα, από τα οποία πρέπει να συνάγουμε αξιόπιστες, πολύτιμες και σημαντικές πληροφορίες. Μια έρευνα σχετικά με τις μεθόδους συγχώνευσης δεδομένων που βασίζονται στη μηχανική μάθηση παρουσιάζεται από τους [418], οι οποίοι αναδεικνύουν ένα μοντέλο που ενεργεί Data Fusion με μηχανική μάθηση και υπερέχει συγκριτικά με τις κλασσικές πιθανοτικές τεχνικές, καθώς ανανεώνει εντυπωσιακά τις τεχνικές σύντηξης προσφέροντας την ισχυρή ικανότητα υπολογισμού και πρόβλεψης.

5.5.2 Αξιολόγηση και αξιοποίηση πληροφοριών

Η βασική λειτουργικότητα που περιγράφεται εδώ είναι η εξαγωγή γνώσης συμβάντων έκτακτης ανάγκης και δραστηριοτήτων αντίδρασης. Σ` αυτό συνεισφέρουν σημαντικά τα δεδομένα από άλλες βοηθητικές βάσεις δεδομένων, τα οποία είτε λαμβάνονται έτοιμα, είτε επεξεργάζονται κατάλληλα και δίνουν τη δική τους προστιθέμενη αξία στις εφαρμογές της δημόσιας ασφάλειας. Στο σημείο αυτό ξεχωρίσαμε και θα αναφερθούμε σε δύο βασικά στοιχεία που συμμετέχουν στο επίπεδο επεξεργασίας, το οποίο για λόγους ευρύτητας όρων ονομάσαμε εφαρμογών:

(α)Συστήματα διαχείρισης αρχείων (Records Management Systems - RMSs)

(β)REST APIs

5.5.2.1 Συστήματα διαχείρισης αρχείων (Records Management Systems - RMSs)

Τα συστήματα διαχείρισης αρχείων αποθηκεύουν, ανακτούν, διατηρούν, αρχειοθετούν και προβάλλουν αρχεία, αυτοματοποιώντας τις διαδικασίες και μειώνοντας τις πιθανότητες ανθρώπινου λάθους. Η συμβολή τους λοιπόν στη δημόσια ασφάλεια είναι σημαντική καθώς διαθέτουν λειτουργικότητες αποθήκευσης αρχείων για κινητές συσκευές, για την παρακολούθηση των δραστηριοτήτων στο πεδίο [419]. Στην ίδια πηγή γίνεται μια εκτενής αποτύπωση στατιστικών εγκληματολογικών στοιχείων των Η.Π.Α., εκ της οποίας προκύπτουν τα δυσθεώρητα μεγέθη και η εξ αυτού αναγκαιότητα να υπάρξει εξαγωγή γνώσης, που στην προκειμένη περίπτωση αφορά σε κρίσιμης σημασίας πληροφορίες, μέσω της τεχνητής νοημοσύνης και άλλων τεχνολογικών λύσεων που θα μας απασχολήσουν στο

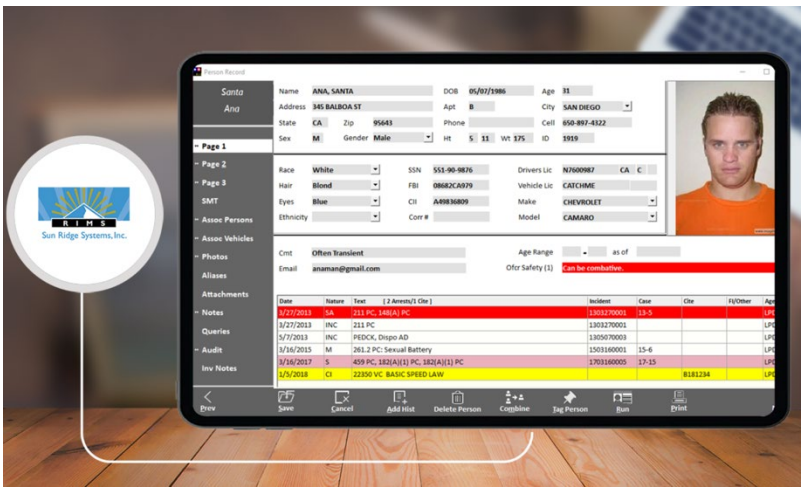
εγγύς τεχνολογικό μέλλον. Ως συμπέρασμα καταδεινύεται ότι τα RMSs έχουν συγκεκριμένες ωφέλειες που συνοψίζονται στ` ακόλουθα [419]:

- Συλλογή και ανάλυση δεδομένων. Η κοινή χρήση δεδομένων βελτιώνει την ομαδική εργασία και τη λήψη αποφάσεων, καθώς επίσης την αστυνόμευση και τις έρευνες.
- Συγκεντροποίηση ερευνητικών δεδομένων. Μια κεντρική βάση δεδομένων περιέχει στοιχεία, οικογενειακά αρχεία, βιομετρικά στοιχεία και ποινικό ιστορικό. Τα πρότυπα και οι τάσεις δεδομένων επιτρέπουν την προληπτική στελέχωση και την κατανομή πόρων.
- Εγκληματολογικές πληροφορίες. Η χαρτογράφηση συμβάντων επιτρέπει στην αστυνομία να παρακολουθεί σκηνές εγκλήματος, να βρίσκει μοτίβα (modus operanti) και να προβλέπει την επανάληψη, βελτιστοποιώντας τους χρόνους αντίδρασης και την κατανομή πόρων.

Μια σειρά από αξιόλογες εφαρμογές RMS έχουν υλοποιηθεί και έχουν ενταχθεί σε υπηρεσίες δημόσιας ασφάλειας παγκοσμίως. Από την πράξη και την ανατροφοδότηση, συνδυαστικά με την επικαιροποίηση των τεχνολογιών που τις υποστηρίζουν διαρκώς βελτιώνονται. Τα κύρια χαρακτηριστικά αυτών αναλύονται στη συνέχεια (Εικόνα 167), ενώ ένα στιγμιότυπο οθόνης χρήστη του κέντρου ελέγχου παρουσιάζεται στην Εικόνα 168 [420]:

- Λειτουργίες βοήθειας. Φιλικά προς τον χρήστη διαδικτυακά σεμινάρια, εύκολα κατανοητά μηνύματα σφάλματος, υποστήριξη και εκπαίδευση από τον εκάστοτε προμηθευτή
- Μενού και εντολές. Κατανοητά και οργανωμένα με λογικό τρόπο
- Ταχύτητα και ακρίβεια. Να υποστηρίζεται δυνατότητα γρήγορης εισαγωγής και ανάκτησης
- Δημιουργία τυπικών αναφορών. Εύκολες και εκτυπώσιμες φόρμες αναφορών
- Ευκολία χρήσης. Λογισμικό φιλικό προς το χρήστη
- Προσαρμογή. Εύκολη παραμετροποίηση του λογισμικό σύμφωνα με τις ανάγκες του οργανισμού
- Δυνατότητα διαχείρισης εγγραφών καθ` όλη τη διάρκεια του κύκλου ζωής
- Δυνατότητα διαχείρισης εγγραφών σε όλες τις μορφές. Να είναι εφικτή η διαχείριση εγγραφών σε οποιαδήποτε μορφή, είτε εγγράφων σε χαρτί, είτε ηλεκτρονικά, μικρογραφικά, είτε οπτικοακουστικά
- Αναζήτηση ελεύθερου κειμένου μεταξύ πεδίων. Να επιτρέπεται η αναζήτηση ελεύθερου κειμένου ή λέξεων-κλειδιών σε όλα τα πεδία

Εικόνα 167. Κύρια χαρακτηριστικά των συστημάτων RMS [420]



Εικόνα 168. Παράδειγμα RMS συστήματος και στιγμιότυπο οθόνης – RIMS RMS [420]

5.5.2.2 REST APIs

Τα Web API είναι η ψυχή της ανάπτυξης ιστού, παρέχοντας το back-end και τις εσωτερικές επικοινωνίες για τη συντριπτική πλειοψηφία των σύγχρονων εφαρμογών ιστού και κινητών. Οι κλήσεις Web API αντιπροσωπεύουν πάνω από το 80% του συνόλου της επισκεψιμότητας ιστού, ενώ τα REST APIs είναι μακράν ο πιο κοινός τύπος web API για υπηρεσίες web και μικροϋπηρεσίες [421].

Με δεδομένη την ενεργή εμπλοκή του cloud και τη μετάβαση στις μικροϋπηρεσίες, ένα API καθίσταται πλέον βασικό στοιχείο, καθώς επιτρέπει στις εφαρμογές λογισμικού να αλληλεπιδρούν μεταξύ τους και να ελέγχουν τον τρόπο με τον οποίο γίνονται τα αιτήματα. Υπάρχουν πλέον περισσότερα από 24.000 δημόσια API που χρησιμοποιούνται από εκατομμύρια προγραμματιστές και εκατοντάδες χιλιάδες οργανισμούς σε όλο τον κόσμο. Επομένως τα APIs γίνονται η ραχοκοκαλιά των περισσότερων σύγχρονων εφαρμογών,

κάποιες από τις οποίες υποστηρίζουν και τη δημόσια ασφάλεια. Στα οφέλη των APIs εντάσσεται ότι οι χρήστες έχουν πρόσβαση σε ευαίσθητα δεδομένα και άλλους πόρους δικτύου, όπως τις εφαρμογές και τις συσκευές IoT. Ωστόσο, τα APIs είναι ιδιατέρω ευάλωτα σε μια ποικιλία επιθέσεων που μπορεί να οδηγήσουν σε παραβιάσεις δεδομένων και σε παραβιάσεις δικτύων [422].

Υπάρχουν δύο κυρίαρχες επιλογές για πρόσβαση σε υπηρεσίες ιστού μέσω API:

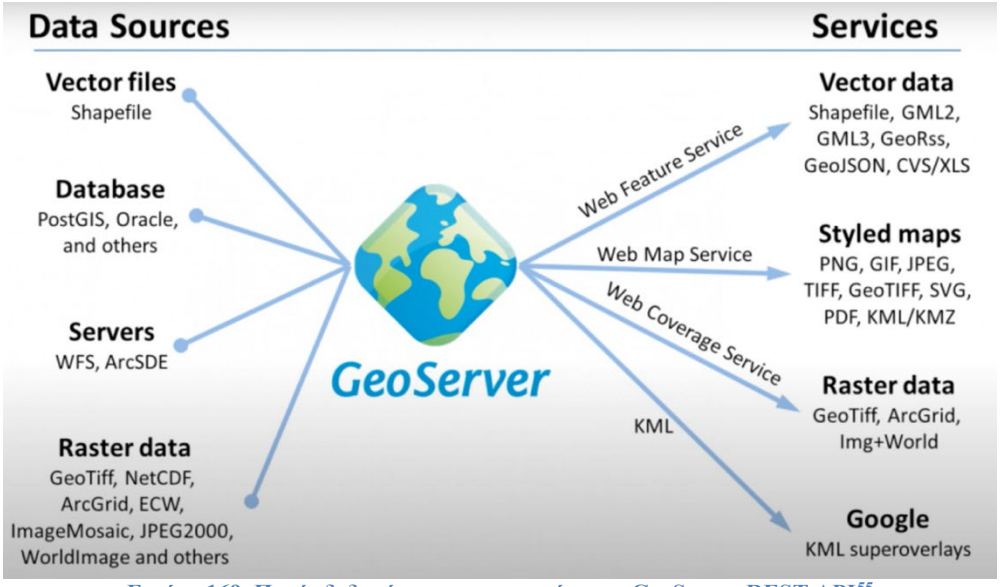
- Πρωτόκολλο πρόσβασης απλού αντικειμένου (Simple Object Access Protocol - SOAP), που αφορά σε πρωτόκολλο επικοινωνίας
- Αντιπροσωπευτική κατάσταση μεταβίβασης (Representational State Transfer API - REST API ή RESTful API), που αφορά σε ένα σύνολο αρχιτεκτονικών αρχών για τη μετάδοση δεδομένων.

Η χρήση των REST APIs σε εφαρμογές δημόσιας ασφάλειας παρουσιάζουν οφέλη που ταυτίζονται με τις επιθυμητές λειτουργικές απαιτήσεις των δικτύων αυτών, καθώς χαρακτηρίζονται από:

- Ευελιξία: Εξαιρετικά ευέλικτα, ικανά να χειρίζονται ένα ευρύ φάσμα αιτημάτων και να παρέχουν δεδομένα στους χρήστες σε πολλές μορφές, ώστε να παρέχουν καλύτερη εμπειρία στον χρήστη.
- Απλότητα: Ενσωματώνουν τεχνολογίες ιστού που έχουν ήδη εφαρμοστεί, επομένως είναι απλά στη δημιουργία και χρήση τους.
- Επεκτασιμότητα: Ο συνδυασμός απλότητας και ευελιξίας τα καθιστά εξαιρετικά επεκτάσιμα. Μπορούν να χρησιμοποιηθούν για την επικοινωνία μεταξύ οποιουδήποτε λογισμικού, ανεξάρτητα από τα μεγέθη ή τις δυνατότητες αυτών των κομματιών λογισμικού. Ακόμη και όταν μια εφαρμογή μεγαλώνει και συλλέγει περισσότερα δεδομένα, το REST API θα μπορεί να επεξεργάζεται τα αιτήματα γρήγορα και με ακρίβεια.
- Τεχνολογική ανεξαρτησία. Παραμένουν ανεξάρτητα από τη γλώσσα προγραμματισμού και το πλαίσιο στο οποίο αναπτύσσονται οι αντίστοιχες εφαρμογές.

Ένα βασικό εργαλείο για τη δημόσια ασφάλεια, που υλοποιεί εφαρμογές γεωεντοπισμού και «ντύνει» σχετικές εφαρμογές είναι το REST API GeoServer[54]. Εποπτική αποτύπωση των πηγών δεδομένων που συνδέεται και των υπηρεσιών που προσφέρει προκύπτει στην Εικόνα 169.

[54] https://docs.geoserver.org/stable/en/user/rest/index.html



Εικόνα 169. Πηγές δεδομένων και υπηρεσίες του GeoServer REST API[55]

5.6 Ασφάλεια

Εκτός από την αξιοπιστία, η ασφάλεια είναι το κορυφαίο κριτήριο αξιολόγησης και μία από τις αδιαπραγμάτευτες απαιτήσεις των δικτύων δημόσιας ασφάλειας. Επομένως, η ανησυχία σχετικά με τα παρεχόμενα επίπεδα ασφαλείας κάθε PSN είναι δικαιολογημένη, καθώς το διακύβευμα είναι μεγάλο και ο αντίκτυπος μιας αποτυχίας, ή έστω αστοχίας ακόμη μεγαλύτερος.

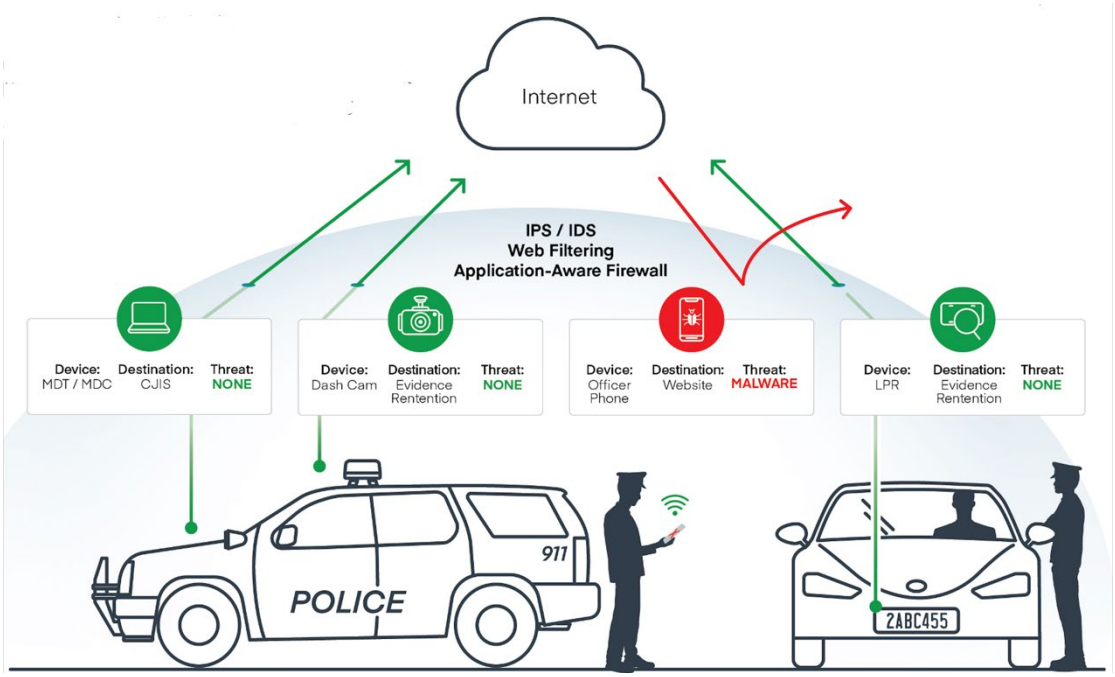
Είναι απολύτως απαραίτητο το προσωπικό της δημόσια ασφάλεια να έχει πρόσβαση στις πληροφορίες που χρειάζεται για να διεκπεραιώσει την αποστολή του, όπως για παράδειγμα οι πληροφορίες εγκληματικής δραστηριότητας ατόμων που περιέχονται σε βάσεις δεδομένων του κεντρικού συστήματος της εγκληματολογικής υπηρεσίας, ωστόσο το τρίπτυχο της ασφάλειας θεωρείται «εκ των ων ουκ άνευ». Η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα εντάσσονται στις βασικές απαιτήσεις κάθε PSN [423]. Στο πλαίσιο της ίδιας έρευνας προέκυψε ότι οι επαγγελματίες της δημόσιας ασφάλειας εμφανίζουν μεγαλύτερο ποσοστό απομακρυσμένων συνδέσεων σε σχέση με άλλους τομείς, γεγονός που αυξάνει την επιφάνεια επίθεσης. Παράλληλα, φαίνεται ότι έχουν σαφή επίγνωση της κατάστασης και κατατάσουν την ασφάλεια δεύτερη σε σπουδαιότητα στην ιεραρχία της λίστας των απαιτήσεων με ποσοστό 61%, πίσω από την αξιοπιστία (85%) και μπροστά από την ταχύτητα ανάπτυξης (44%), την ευελιξία (33%) και την ανθεκτικότητα (32%). Μάλιστα, αξιοσημείωτο είναι ότι οι περισσότερες από τις Υπηρεσίες δημόσιας ασφάλειας φέρονται να χρησιμοποιούν περισσότερες από εννιά (9) διαφορετικές δισυνδεδεμένες τεχνολογίες στο πεδίο (Εικόνα 170).

[55] https://www.youtube.com/watch?v=Na79e-eK4Ik

Όμως, ακόμη και στον τομέα της δημόσιας ασφάλειας έχουν καταγραφεί πολύ σοβαρά περιστατικά παραβιάσεων και κυβερνοεπιθέσεων. Μάλιστα, τον καιρό της πανδημίας του COVID19 οι επιθέσεις αυτές αυξήθηκαν σημαντικά σε παγκόσμιο επίπεδο. Μέχρι τώρα έχει αναφερθεί αρκετές φορές η σπουδαιότητα να διασφαλιστεί με κάθε τρόπο αυτή η ιδιαίτερη απαίτηση.

Το κύριο και βασικό πρώτο βήμα που θα πρέπει να λαμβάνει χώρα αφορά στην ανίχνευση και απομόνωση της απειλής. Σύμφωνα με το [423] τμηματική στόχευση των συστημάτων ασφαλείας των PSNs θα πρέπει να αποτελούν:

- Ο έλεγχος της κυκλοφορίας και χρήσης, ώστε να παρέχεται ασύρματη πρόσβαση, χωρίς να παρεμποδίζεται η συνολική ασφάλεια του δικτύου.
- Η κατά το δυνατό ανίχνευση και ελαχιστοποίηση των εισβολών στο δίκτυο
- Η τμηματοποίηση του δικτύου και μάλιστα σε διακριτούς τύπους κυκλοφορίας δεδομένων, ώστε σε ενδεχόμενη επίθεση να είναι εφικτό να αποκόπτονται τμήματα και να δημιουργούνται στεγανά δεδομένων
- Η διατήρηση και διαχείριση ασφαλείας και κρυπτογράφισης δεδομένων, ιδανικά από άκρο σε άκρο



Εικόνα 170. Διασυνδεδεμένες υπηρεσίες δημόσιας ασφάλειας στο πεδίο [423]

5.6.1 Απειλές

Οι απειλές είναι ποικίλες και σχετίζονται με τα πρότυπα ή τα πρωτόκολλα επικοινωνίας που χρησιμοποιεί κάθε PSN. Χαρακτηριστικά παραδείγματα αυτών ομοιάζουν με τις απειλές στα κοινά δίκτυα και αφορούν σε [424], [425], [426]:

- Εισβολή σε ένα δίκτυο (Intrusion). Η εισβολή σε ένα δίκτυο είναι ο συνηθέστερος τρόπος επίθεσης και έχει στόχο οι επιτιθέμενοι να αποκτήσουν τα δικαιώματα των νόμιμων χρηστών
- Επιθέσεις άρνησης υπηρεσίας (Denial of Service, DoS). Ονομάζονται οι επιθέσεις εναντίον υπολογιστών / υπηρεσιών, που έχουν σκοπό να τους καταστήσουν ανίκανους να δεχτούν άλλες συνδέσεις και να μην μπορούν να εξυπηρετήσουν άλλους πελάτες. Αυτό πραγματοποιείται είτε με την αναγκαστική κατάρρευση της υπηρεσίας και την ανάγκη για επανεκκίνηση, είτε με την αποστολη υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων με αποτέλεσμα η υπηρεσία να μην μπορεί να εξυπηρετήσει πραγματικές αιτήσεις, λόγω κατανάλωσης πόρων. Οι κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (Distributed Denial-of-Service attacks - DDoS) χρησιμοποιούν πολλαπλές επιθέσεις μέσω άλλων θυμάτων ή και θυτών.
- Υποκλοπή ευαίσθητων πληροφοριών. Συμβαίνει όταν ένας επιτιθέμενος αποκτά πρόσβαση σε ευαίσθητες πληροφορίες εξ΄ αποστάσεως, χωρίς την άμεση επαφή με το μηχάνημα. Συνήθως, οι επιθέσεις αυτού του είδους εκμεταλλεύονται δικτυακές υπηρεσίες σχεδιασμένες για χρήση σε ασφαλή τοπικά δίκτυα και όχι στο Internet.

Οι τρόποι με τους οποίους πραγματοποιούνται οι αναφερόμενες απειλές ποικίλλουν και μπορεί να είναι:

- Επίθεση σε ιστοσελίδες
- Επίθεση στην υπηρεσία ονοματολογίας (Domain Name Servers -DNS)
- Επίθεση με Δούρειους Ίππους (Trojan Horses). Οδηγίες κρυμμένες μέσα σε ένα κατά τα άλλα χρήσιμο πρόγραμμα που μπορεί να κάνει ζημιά. Συνήθως ο όρος Δούρειος ίππος χρησιμοποιείται όταν οι κακόβουλες οδηγίες εγκαθίστανται τη στιγμή που γράφεται το πρόγραμμα (και ο όρος ιός χρησιμοποιείται εάν οι οδηγίες προστεθούν στο πρόγραμμα αργότερα).
- Επιθέσεις με ιούς. Χαρακτηριστικό παράδειγμα αποτελούν ιοί που εισάγονται στο σύστημα μέσω οδηγιών σε μηνύματα ηλεκτρονικού ταχυδρομείου που, όταν εκτελούνται, προκαλούν την αποστολή του κακόβουλου κώδικα σε άλλους χρήστες.
- Επιθέσεις με σκουλίκια (worm). Είναι ένα πρόγραμμα που αναπαράγει τον εαυτό του εγκαθιστώντας αντίγραφα του σε άλλα μηχανήματα σε ένα δίκτυο.
- Επίθεση στο ηλεκτρονικό ταχυδρομείο και στο πρωτόκολλό του (Simple Mail Transfer Protocol- SMTP)
- Επίθεση από υποκλοπή κωδικών πρόσβασης, στις οποίες ηθελημένα ή όχι έχουν εμπλοκή οι χρήστες
- Sniffing
- Πλαστογράφηση(Spoofing)

5.6.2 Λύσεις

Αναφερόμαστε σε ασφάλεια των PSNs και ουσιαστικά περιγράφουμε τις αρχές, τις πολιτικές και τις διαδικασίες που απαιτούνται για την προστασία τους από κάθε είδους απειλή, είτε αφορά σε σκόπιμη, είτε σε τυχαία ενέργεια. Επιπλέον, αναφερόμαστε σε σύγχρονες τεχνικές και μέτρα που απαιτούνται για την παροχή της ασφάλειας των δικτύων αυτών και σε κάθε περίπτωση προϋπόθεση αποτελεί η απρόσκοπτη διακίνησης της πληροφορίας

Η βασική άμυνα των PSNs όπως είδαμε από δεκαετίες πρίν μέσω του TETRA είναι η κρυπτογράφηση. Χρησιμοποιούνται γνωστοί αλγόριθμοι κρυπτογράφησης, είτε δημοσίου, είτε ιδιωτικού κλειδιού:

- Πρότυπο κρυπτογράφησης δεδομένων (Data Encryption Standard - DES). Είναι ένας συμμετρικός αλγόριθμος δέσμης, ο οποίος υιοθετήθηκε ως επίσημο πρότυπο και η ασφάλειά του βασίζεται στο κλειδί και όχι στη μυστικότητα του αλγορίθμου. Ωστόσο επειδή διέθετε μικρό μήκος κλειδιού, ήταν ευάλωτος σε επιθέσεις εξαντλητικής αναζήτησης (brute force attacks)
- Τριπλός DES αλγόριθμος. Επέκταση του DES που έλυσε το πρόβλημα του μικρού μήκους κλειδιού, με την εισαγωγή και δεύτερου κλειδιού.
- AES. Επίσης ένας συμμετρικός αλγόριθμος δέσμης που ήταν ουσιαστικά ο αντικαταστάτης του DES, με απλότητα στη σχεδιάση, ταχύτητα εκτέλεσης και οικονομία κώδικα.
- RSA. Ένας από τους πρώτους αλγόριθμους δημοσίου κλειδιού που είναι ιδανικός για δεδομένα μικρού μεγέθους.

Πλέον των αλγορίθμων, σημαντική εμπλοκή στην άμυνα των συστημάτων ενός PSN έχουν οι ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά, τεχνικές οι οποίες ισχυροποιούν τις διαδικασίες με δεδομένη τη μεγάλη διακίνηση εγγράφων και τις πολύπλοκες εφαρμογές της δημόσιας ασφάλειας. Χαρακτηριστικό παράδειγμα αυτού αποτελεί η προσέγγιση που επιχειρούν οι [427], οι οποίοι εισάγουν μια ξεχωριστής φύσης κωδικοποίηση στην αυθεντικοποίηση του χρήστη, αυτή του δακτυλικού αποτυπώματος, που λειτουργεί ως μυστικό βιβλίο κωδικών, το οποίο εγγράφηκε στην πρώτη είσοδο του χρήστη με δακτυλικό αποτύπωμα.

Βέβαια, εξίσου σημαντικές θεωρούνται και οι συνήθεις λύσεις που αφορούν:

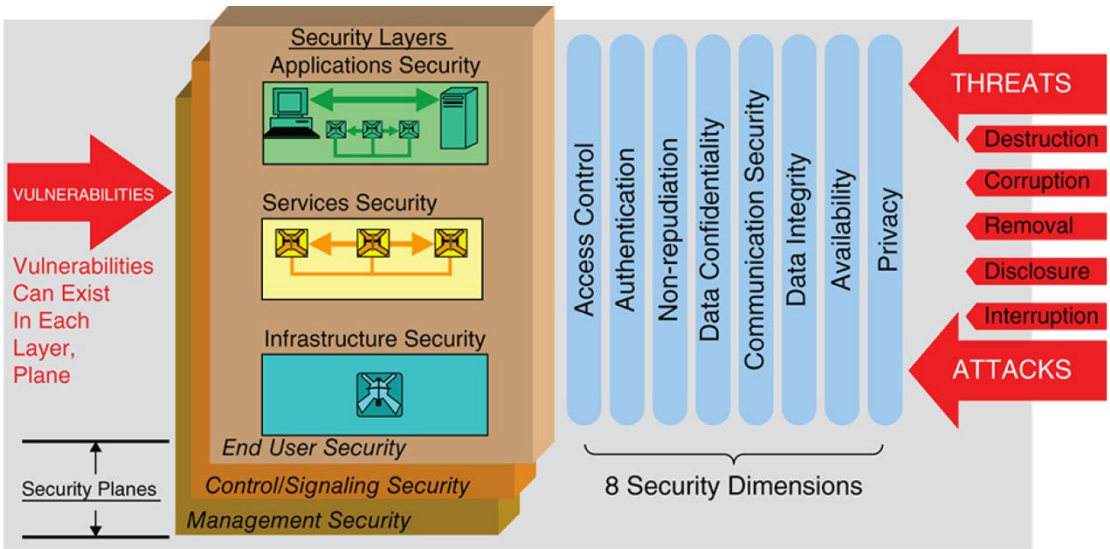
- Τείχη Προστασίας (Firewalls)
- Συστήματα Ανίχνευσης Εισβολής (Intrusion Detection Systems - IDS)
- Συστήματα Ανίχνευσης και Πρόληψης Εισβολής (Intrusion Detection and Prevention Systems - IDPS)

Χαρακτηριστικές προσεγγίσεις υπάρχουν εκατοντάδες στη βιβλιογραφία. Στο [51] αναφέρεται ότι η κρυπτογράφηση στην κίνηση των χρηστών μεταξύ των κόμβων σε ένα PSN

μπορεί να αποτρέψει την ασύρματη υποκλοπή. Άμεση συμβολή σ` αυτό έχουν οι κρυπτογραφικοί αλγόριθμοι AES 128 bit και 256 bit, καθώς μπορούν να παρέχουν πολύ αποτελεσματική ασφάλεια. Επιπλέον, στα ασύρματα δίκτυα πλέγματος (wireless mesh networks) που υποστηρίζουν εφαρμογές δημόσιας ασφάλειας ιδιαιτέρως αποδοτικές υπηρεσίες ασφάλειας παρέχουν οι ψηφιακές υπογραφές που επιτρέπουν την πρόσβαση μόνο σε εξουσιοδοτημένα άτομα. Συμπληρωματικά, λύσεις όπως εικονικά ιδιωτικά δίκτυα (VPN), τείχος προστασίας (firewall), έλεγχος ανίχνευσης εισβολής (IDS) και στοιχεία ελέγχου εφαρμογών όπως HTTP παρέχουν εξίσου καλή προστασία, κατά περίπτωση.

Από την προσέγγιση της ITU για παροχή υπηρεσιών ασφαλείας σε συστήματα επικοινωνιών από άκρο σε άκρο (E2E) [428] προκύπτει ότι λαμβάνονται υπόψη οι απειλές και τα τρωτά σημεία στο σύνολο των στοιχείων της εφαρμογής που θέλουμε να προστατέψουμε. Στην Εικόνα 171 προκύπτει ένα μοντέλο ασφάλειας με διαστρωμάτωση επιπέδων που στοχεύει να παρέχει ασφάλεια από άκρο σε άκρο σε κάθε επίπεδο. Οι πτυχές ασφαλείας χωρίζονται σε:

- έλεγχο πρόσβασης
- αυθεντικοποίηση
- μη απόρριψη
- εμπιστευτικότητα δεδομένων
- ασφάλεια επικοινωνίας
- ακεραιότητα δεδομένων
- διαθεσιμότητα
- ιδιωτικότητα



Εικόνα 171. Αρχιτεκτονική ασφαλείας για ασφάλεια δικτύου από άκρο σε άκρο [428]

Οι [429] αναφέρουν ότι τα συστήματα των πρώτων ανταποκριτών είναι επιρρεπή σε κακόβουλες επιθέσεις από μη εξουσιοδοτημένους εξωτερικούς χρήστες και από κακόβουλους και μη εξουσιοδοτημένους χρήστες και ομαδοποιεί τις απειλές σε τρεις μεγάλες κατηγορίες:

(α)Άρνηση υπηρεσίας. Η οποία συμβαίνει με τρεις διαφορετικούς τρόπους και συγκεκριμένα είτε πλημμυρίζοντας το δίκτυο, διακόπτοντας τις συνδέσεις μεταξύ ομότιμων κόμβων, είτε τέλος παρεμποδίζοντας έναν συγκεκριμένο χρήστη από την πρόσβαση σε υπηρεσίες του δικτύου.

(β)Χειραγώγηση δεδομένων. Εκτός από τους μηχανισμούς επικοινωνίας, τα μηνύματα που μεταδίδονται υπόκεινται σε απειλές. Το περιεχόμενο των μηνυμάτων υπό απειλή μπορεί να είναι είτε δεδομένα χρήστη, οπότε οι επιτιθέμενοι θα μπορούσαν να παρακολουθούν και να τροποποιούν το περιεχόμενο των πακέτων αποστολής, αναπαράγοντας ή αναδρομολογώντας αυτό, είτε πληροφορίες αξιοπιστίας, που χρησιμοποιούνται για τη δημιουργία μιας κρίσιμης και αξιόπιστης επικοινωνίας (περιπτώσεις κλοπής κωδικών αυθεντικοποίησης, κ.λπ.), είτε τέλος πληροφορίες δραστηριότητας, καθώς η τακτική της απλής παρακολούθησης του όγκου της εισερχόμενης και εξερχόμενης κίνησης μπορεί να δώσει πληροφορίες δραστηριότητας.

(γ)Φυσικές επιθέσεις. Οι επιτιθέμενοι θα μπορούσαν να καταστρέψουν τις συσκευές φυσικά και να προκαλέσουν σημαντικότατη ζημία ειδικότερα εάν η λειτουργικότητα των συσκευών δεν αντιγράφεται επαρκώς,

Αυτό το τελευταίο στοιχείο αναφέρεται σε μια σημαντική παράμετρο. Αυτή της φυσικής ασφάλειας που σχετίζεται με την υποδομή των δικτύων PSNs. Στον τομέα αυτό, οι φορείς της δημόσιας ασφάλειας με δεδομένο ότι έχουν στον πυρήνα της λειτουργίας τους την παροχή υπηρεσιών ασφαλείας υπερέχουν έναντι των υπολοίπων κρίσιμων υποδομών. Σε κάθε περίπτωση όμως, η τρωτότητα των δικτύων δημόσιας ασφάλειας και της φυσικής υποδομής τους εντάσσεται στο σχεδιασμό που υλοποιούν οι υπηρεσίες αυτές και απαιτεί ξεχωριστούν πόρους για να επιτευχθεί. Για τις περιπτώσεις δε που βάλλονται από τις συνέπειες φυσικών φαινομένων (σεισμοί, πυρκαγιές, πλημμύρες, κ.λπ.) προβλέπεται σχέδιο ταχείας ανάκαμψης και ανάπτυξης εναλλακτικών στοιχείων που καλύπτουν τις απαιτήσεις, όπως διεξοδικά έχει αναλυθεί ήδη.

5.6.3 Ποιότητα Υπηρεσίας (QoS)

Η ανάπτυξη των ευρυζωνικών ασύρματων δικτύων επιτυγχάνει ενοποίηση προϊόντων, προτύπων και υπηρεσιών σε αντίθεση με την προγενέστερη τάση για κατακερματισμό των στοιχείων των ασύρματων δικτύων. Ο οδηγός των εξελίξεων πλέον είναι η κινητικότητα των χρηστών και τα διαφορετικά περιβάλλοντα χρήσης, τα οποία απαιτούν κύρια χαρακτηριστικά και των PSNs και τα οποία αποτελούν τους κυριότερους παράγοντες διατήρησης και προσφοράς εναλλακτικών συστημάτων και υπηρεσιών. Τις υπηρεσίες συνήθως τις εξετάζουμε με βάση τρία χαρακτηριστικά:

- τον ελάχιστο απαιτούμενο ρυθμό μετάδοσης,
- το μέγιστο ανεκτό ρυθμό σφαλμάτων,

- τη μέγιστη ανεκτή καθυστέρηση.

Αντιλαμβανόμαστε καλύτερα τα βασικά χαρακτηριστικά του QoS μέσα από συγκεκριμένα παραδείγματα. Οι υπηρεσίες τηλεειδοποίησης, ή μετάδοσης γραπτών μηνυμάτων δεν έχουν απαιτήσεις υψηλού ρυθμού μετάδοσης και ορίου καθυστερήσεων. Οι υπηρεσίες φωνής έχουν μικρές απαιτήσεις σε ρυθμό μετάδοσης και είναι ανεκτικές σε υψηλούς ρυθμούς σφαλμάτων, ωστόσο η συνολική καθυστέρηση δεν θα πρέπει να υπερβαίνει ένα χρονικό όριο που θα την καιστά αντιληπτή στο χρήστη. Αντίστοιχα, οι υπηρεσίες δεδομένων απαιτούν υψηλούς ρυθμούς μετάδοσης, με μικρούς ρυθμούς σφαλμάτων, χωρίς όμως να έχουν ιδιαίτερες απαιτήσεις καθυστέρησης μετάδοσης. Τέλος, οι εφαρμογές αποστολής βίντεο πραγματικού χρόνου απαιτούν και υψηλούς ρυθμούς μετάδοσης και χαμηλές καθυστερήσεις [430].

Επομένως, η διασφάλιση της QoS γίνεται εξαιρετικά σημαντική στα δίκτυα δημόσιας ασφάλειας, καθώς εντάσσεται στον κύκλο των σημαντικότερων απαιτήσεών τους. Είναι απαραίτητο προκειμένου να δοθεί προτεραιότητα σε κρίσιμα δεδομένα τα οποία πρέπει να προηγηθούν από οποιαδήποτε άλλα τη δεδομένη στιγμή και να φτάσουν στον χρήστη χωρίς καθυστέρηση. Οι μετρήσεις απόδοσης που ποσοτικοποιούν το QoS μιας ροής δεδομένων μπορεί να περιλαμβάνει ρυθμό σφάλματος bit, καθυστέρηση, jitter και απώλεια πακέτων, κ.λπ.. Ο τρόπος που επιτυγχάνεται και διατηρείται ένα ελάχιστο επίπεδο QoS, χωρίς να παραβιάζεται άλλος σχεδιασμός ενεργειακής κατανάλωσης και ασφάλειας, είναι με τα ισχυρά πρωτόκολλα δρομολόγησης. Για παράδειγμα, τα πρωτόκολλα δρομολόγησης μπορεί να χρησιμοποιούν ad-hoc δίκτυα για την επέκταση του αποτελεσματικού εύρους επικοινωνίας των συσκευών, χωρίς να μειώνεται απαράδεκτα η καθυστέρηση σε περιβάλλον έκτακτης ανάγκης. Ωστόσο, τα πρωτόκολλα δρομολόγησης μπορεί να γίνουν ευάλωτα σε εξωτερικές επιθέσεις και να υποβαθμίσουν το QoS ενός συστήματος έκτακτης ανάγκης δραστικά [52].

Είναι εξαιρετικά δύσκολο να ικανοποιηθεί το σύνολο των διαφορετικών απαιτήσεων κάθε εφαρμογής από ένα μοναδικό ασύρματο σύστημα επικοινωνίας. Μάλιστα, η ολοκλήρωση των απαιτήσεων στα ασύρματα συστήματα υλοποιήθηκε με την είσοδο στην εποχή της ευρυζωνικής επικοινωνίας. Ωστόσο, το αποτέλεσμα δεν είναι ακόμη το απολύτως επιθυμητό και οι προκήσεις στον τομέα αυτό εξακολουθούν να υφίστανται. Ιδανικά, ένα σύστημα θα υποστήριζε το σύνολο των εφαρμογών και θα ανταποκρινόταν στο σύνολο των απαιτήσεων [430].

6 *Βέλτιστες Πρακτικές*

Ο εντοπισμός των βέλτιστων πρακτικών συνδέεται συχνά με τη συγκριτική αξιολόγηση, η οποία σύμφωνα με το Ευρωπαϊκό Ίδρυμα Διαχείρισης Ποιότητας (European Foundation for Quality Management – EFQM[56]) βοηθά έναν οργανισμό να συνειδητοποιήσει τις τεχνικές, τις μεθόδους, ή τις διαδικασίες που κατέστησαν κάποιον άλλον επιτυχημένο, καθώς επίσης να μεταφράσει τις συγκεκριμένες πρακτικές σε υλοποιήσιμο μέγεθος, δηλαδή πετυχημένες δικές του εφαρμογές για να φέρει βελτιωμένα αποτελέσματα. Επομένως, το πρώτο και βασικό στάδιο της εξεύρεσης των βέλτιστων πρακτικών εμπεριέχει τη συγκριτική αξιολόγηση, η οποία εκτός των άλλων προωθεί την καλλιέργεια μιας κουλτούρας απόκτησης γνώσεων μέσα στους οργανισμούς ή τις επιχειρήσεις, ως σημαντικό παράγοντα για συνεχείς μακροπρόθεσμες βελτιώσεις. Η σπουδαιότητα των όρων αυτών έγινε γρήγορα αποδεκτή τόσο από την επιστημονική κοινότητα, όσο και από τον επιχειρηματικό κόσμο, καθώς πολύ γρήγορα συνδυάστηκε με σημαντικότατα κέρδη. Πρωτοπόρος ήταν η εταιρία Xerox, που το έτος 1979 εφάρμοσε επιτυχημένα τη συγκριτική αξιολόγηση με στόχο να υπερκεράσει το διεθνή ανταγωνισμό στην αγορά φωτοαντιγραφικών μηχανημάτων. Σήμερα, το συγκεκριμένο πεδίο αποτελεί ένα αυτοτελές γνωστικό αντικείμενο στην επιχειρηματική πραγματικότητα και ένα εργαλείο στη μείωση του κόστους, την αύξηση της παραγωγικότητας και τη μείωση του κύκλου παραγωγής. Οι βέλτιστες πρακτικές επιφέρουν και βέλτιστη επίδοση σε όλα τα επίπεδα. Η πορεία μέχρι την υιοθέτηση βέλτιστων πρακτικών περιλαμβάνει διακριτές φάσεις. Ο σχεδιασμός, η ανάλυση, η ολοκλήρωση, η δράση και η ωριμότητα, δημιουργούν στους οργανισμούς και στις επιχειρήσεις περισσότερες ευκαιρίες να αποκομίσουν στρατηγικό, λειτουργικό και οικονομικό πλεονέκτημα.

Στην περίπτωση που μελετούμε, επιλέξαμε να προβούμε αρχικά σε μία αναλυτική αναφορά στις λύσεις που έχουν υλοποιήσει διάφορες χώρες παγκοσμίως για τα τηλεπικοινωνιακά

[56] https://efqm.org/

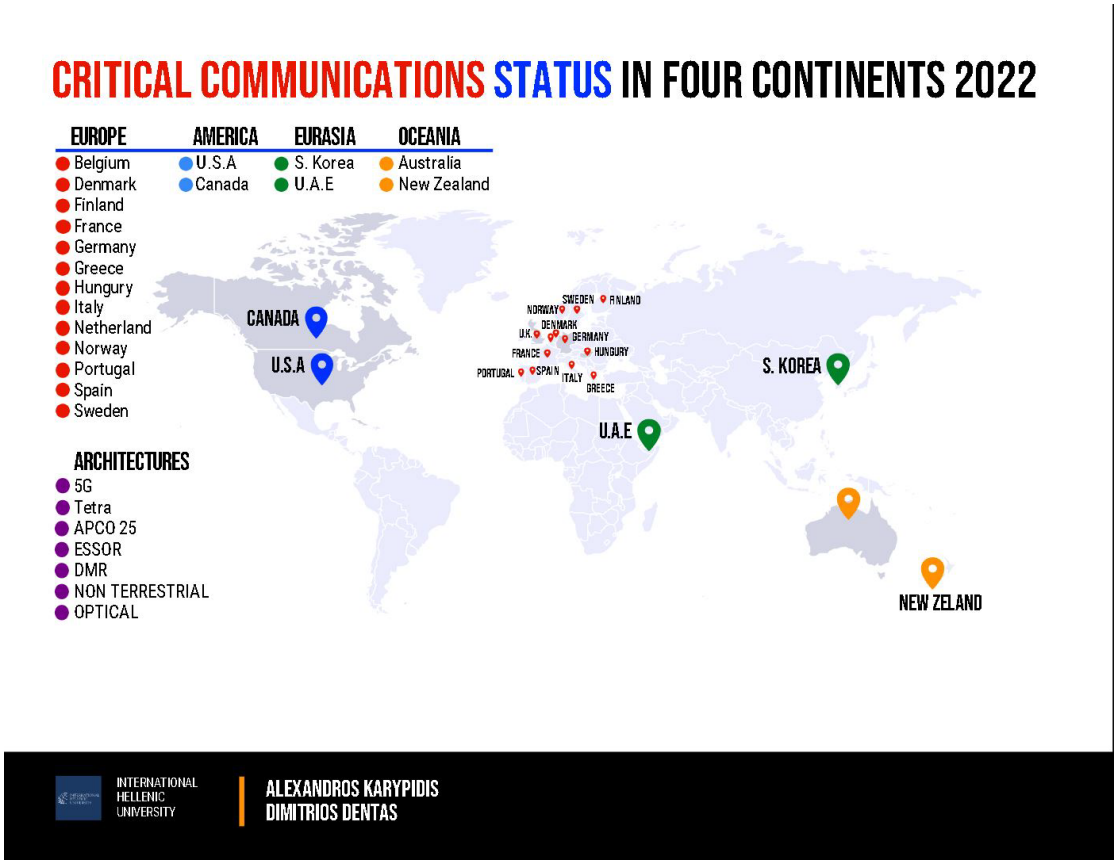
δίκτυα δημόσιας ασφάλειας. Η επιλογή των χωρών έγινε έπειτα από μελέτη και αξιολόγηση της βιβλιογραφίας, από όπου επιλέγησαν έργα υψηλού προφίλ, έργα που εφαρμόζονται αρκετές δεκαετίες και θεωρούνται δοκιμασμένα και έως ένα σημαντικό επίπεδο επιτυχημένα, στα οποία έγιναν διορθωτικές βελτιώσεις ώστε να καλύπτουν τις ανάγκες του σήμερα, καθώς και προγράμματα που σε εθνικό επίπεδο σημειώνουν σημαντική πρόοδο, εισάγουν καινοτόμες λύσεις και βρίσκονται σε καίριο σημείο δοκιμών, ή ανάπτυξης προϊόντων. Κάθε χώρα στην οποία αναφερόμαστε έχει κάνει τη δική της επιλογή αρχιτεκτονικής δικτύου δημόσιας ασφάλειας, θέτοντας συγκεκριμένες προτεραιότητες.

Ακολούθως, προβήκαμε σε συγκριτική αξιολόγηση των έργων αυτών, με βάσει διαφορετικές «οπτικές τεχνολογικές γωνίες», ώστε να καταλήξουμε στις βέλτιστες πρακτικές. Ειδικότερα, αξίζει ν‘ αναφερθεί ότι η συγκριτική αξιολόγηση που παραθέτουμε είναι επηρεασμένη από τα μοντέλα και τις τεχνικές που έχουν καθιερωθεί στη βιβλιογραφία και σέβεται τους βασικούς κανόνες και τις διαδικασίες, πλην όμως έγινε με κριτήρια που ορίσθηκαν από τους συγγραφείς και δεν υπάγονται αυτοτελώς σε συγκεκριμένο μοντέλο. Στόχος άλλωστε είναι η μέτρηση των επιδόσεων των δικτύων δημόσιας ασφάλειας και των αρχιτεκτονικών που παρουσιάζονται, η μέτρηση της αποδοτικότητάς τους, η μέτρηση του επιπέδου που καλύπτουν τις λειτουργικές απαιτήσεις επικοινωνίας των πρώτων ανταποκριτών, αλλά και των ανθρώπων της δημόσιας ασφάλειας, η καινοτομία που παρουσιάζουν, η τεχνολογία και οι δημιουργούμενες προοπτικές. Είναι γνωστή η ρήση: «*Ό,τι δεν μπορείς να μετρήσεις, δεν μπορείς να το βελτιώσεις*»[57]. Ως καταστάλαγμα αυτών, οδηγηθήκαμε στη θεώρηση των βέλτιστων πρακτικών, όχι βέβαια ως απλή αντιγραφή επιτυχημένων μεθόδων, αλλά ως πρόταση αποδοτικής προσαρμογής αυτών των λύσεων και υβριδικού συνδυασμού τους.

6.1 Τεχνολογίες, αρχιτεκτονικές και έργα διαφόρων χωρών

Μια επιπλέον κατηγοριοποίηση έγινε με βάση τις Ηπείρους, λαμβάνοντας υπόψη αφενός τις διαφορετικές γεωπολιτικές προσεγγίσεις και αφετέρου τις διαφορές σε τεχνολογίες και φάσμα που χρησιμοποιείται, ως ήδη εκτενώς αναφέρθηκε στο αντίστοιχο κεφάλαιο (Εικόνα 172). Στη συνέχεια θα αναλύσουμε τις πρακτικές που εφάρμόζουν σήμερα κάποιες από τις Χώρες αυτές, ως αντιπροσωπευτικά παραδείγματα.

[57] *Peter Drucker.* https://en.wikipedia.org/wiki/Peter_Drucker

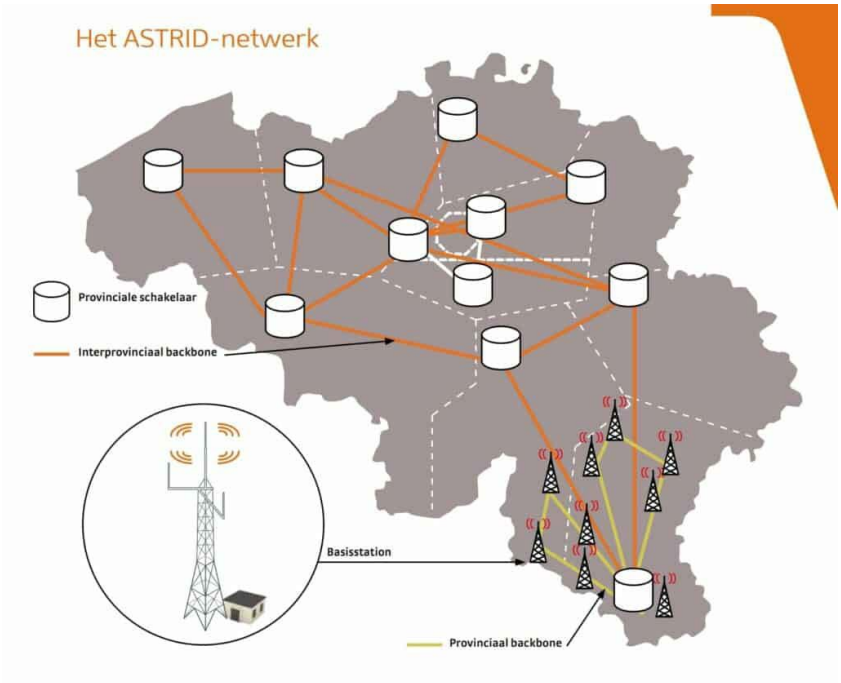


Εικόνα 172. Κρίσιμες επικοινωνίες σε τέσσερις Ηπείρους.

6.1.1 Ευρώπη

6.1.1.1 Βέλγιο

Από το 1998, η ASTRID (All-round Semi-cellular Trunking Radio with Integrated Dispatching) αναπτύσσει, διαχειρίζεται και συντηρεί το εθνικό δίκτυο ραδιοεπικοινωνιών, ένα δίκτυο τηλεειδοποίησης καθώς και αίθουσες ελέγχου (Control Rooms). Το δίκτυο ASTRID TETRA (Εικόνα 173) είναι μια πρωτοβουλία που δημιουργήθηκε από τις βελγικές ομοσπονδιακές αρχές και η σύμβαση διαχείρισης του καταρτίστηκε με βασιλικό διάταγμα της 8ης Φεβρουαρίου 1999 (Βελγική Επίσημη Εφημερίδα της 27ης Φεβρουαρίου 1999 [431]. «*Η αποστολή της ASTRID είναι να δημιουργήσει, να διατηρήσει και να εφαρμόσει όλες τις αναγκαίες αναβαθμίσεις που απαιτούνται με στόχο τη διεύρυνση ενός δικτύου ραδιοεπικοινωνιών για μεταδόσεις φωνής και δεδομένων για τις βελγικές υπηρεσίες έκτακτης ανάγκης και ασφάλειας, κρατικές και θεσμικές υπηρεσίες ασφαλείας και εταιρείες ή ενώσεις, δημόσιες ή ιδιωτικές , που παρέχουν υπηρεσίες στον τομέα των υπηρεσιών έκτακτης ανάγκης και ασφάλειας*» (άρθρο 3 του νόμου ASTRID) [431].



Εικόνα 173. Σχηματική αναπαράσταση του δικτύου ASTRID TETRA (512 BS)

6.1.1.1.1 Οργανισμοί που υποστηρίζει

Οι υποστηριζόμενοι οργανισμοί είναι:

- Ομοσπονδιακή αστυνομία
- Τοπικά αστυνομικά τμήματα
- Πυροσβεστική υπηρεσία
- Υπηρεσίες ασθενοφόρων
- Πολιτική Προστασία
- Κρατική υπηρεσία πληροφοριών
- Τελωνειακές αρχές
- Στρατός
- Δημόσιες Μεταφορές
- Εγκαταστάσεις νερού
- Εταιρείες διανομής ενέργειας
- Διεθνείς οργανισμούς με έδρα το Βέλγιο

6.1.1.1.2 Χαρακτηριστικά του δικτύου TETRA:

Τα κυριότερα χαρακτηριστικά του δικτύου TETRA που χρησιμοποιεί η ASTRID είναι:

- Συχνότητες λειτουργίας: 380-385/390-395 MHz [431]
- >550 Σταθμοί βάσης TETRA
- >70.000 χρήστες του δικτύου
- >2.000.000 κλήσεις / ημέρα

6.1.1.1.3 Τα πλεονεκτήματα του ASTRID και το πρόγραμμα Blue Light Mobile

Το δίκτυο ASTRID TETRA παρουσιάζει κάποια πλεονεκτήματα, όπως:

- Μέγιστη εμπιστευτικότητα χάρη στην κρυπτογράφηση της επικοινωνίας και τον έλεγχο ταυτότητας
- Βέλτιστη ποιότητα ήχου
- Γρήγορες και αξιόπιστες συνδέσεις
- Ομαδικές επικοινωνίες
- Υποστήριξη φωνής και δεδομένων
- Πολλαπλές υπηρεσίες
- Κάλυψη σε όλη τη χώρα (Εικόνα 174)

Το 2014 η ASTRID με το πρόγραμμα Blue Light Mobile [431] ξεκίνησε την παροχή υπηρεσιών δεδομένων στους χρήστες της. Ωστόσο η υπηρεσία παρείχε περιορισμένο όγκο δεδομένων που δεν εξασφάλιζε τις mission - critical απαιτήσεις. Το 2015 η ASTRID έπρεπε να αποφασίσει για το μέλλον του δικτύου με δεδομένο πως ο τότε εξοπλισμός της είχε ολοκληρώσει τον κύκλο του. Παρά το γεγονός πως τόσο οι LTE αλλά και άλλες τεχνολογίες δεν ήταν ώριμες η ASTRID αποφάσισε να προχωρήσει σε επέκταση του κύκλου ζωής του δικτύου έως το 2030, σύμφωνα με τον Christophe Gregoire διευθυντή τεχνολογίας και λειτουργίας της ASTRID. [432] Το 2017 - 2018 η ASTRID σχεδίασε την στρατηγική για ένα νέο δίκτυο. Τμήμα αυτής της στρατηγικής αποτέλεσε η μελέτη των αναγκών αλλά και των απαιτήσεων που είχαν οι χρήστες και με αυτά τα δεδομένα καθόρισε τις συνθήκες που θα διασφάλιζαν πως το νέο αυτό δίκτυο θα ικανοποιούσε τις ανάγκες των χρηστών. Η ASTRID επίσης εξέτασε διαφορετικά μοντέλα χρηστών και κατέληξε πως μια υβριδική λύση βασισμένη στη χρήση ενός Mobile Virtual Network Operator (MVNO) θα αποτελούσε την καλύτερη επιλογή σε σύγκριση με ένα αποκλειστικό δίκτυο δημόσιας ασφάλειας ή χρησιμοποιώντας κάποιο εμπορικό δίκτυο μόνο.

Οι τεχνολογικές εξελίξεις πρόλαβαν τον σχεδιασμό της ASTRID, η ανάπτυξη του 5G πρόσφερε νέες δυνατότητες όπως τον τεμαχισμό (slicing) του δικτύου, γεγονός που οδήγησε στον επανασχεδιασμό της στρατηγικής αφού πρώτα εξερευνηθούν όλες οι δυνατότητες του 5G με στόχο η ASTRID να προσφέρει τις καλύτερες δυνατές επικοινωνίες για τη δημόσια ασφάλεια [432].

Ένα από τα βασικά πλεονεκτήματα του Blue Light Mobile είναι η μεγαλύτερη δυνατή κάλυψη περιοχών στο Βέλγιο με δυνατότητα χρήσης όλων των εμπορικών δικτύων τρίτων παρόχων (Proximus, Orange και BASE). Οι χρήστες έχουν δυνατότητα χειροκίνητης επιλογής συγκεκριμένου δικτύου με βάση τις ανάγκες τους. Το πρόγραμμα παρέχει στους χρήστες δυνατότητα διεθνούς περιαγωγής γεγονός που διασφαλίζει τις επικοινωνίες ακόμη

και σε υπηρεσίες που λειτουργούν πολύ κοντά στα σύνορα. Στους συνδρομητές του Blue Light Mobile ακόμη και εάν τα δίκτυα είναι κορεσμένα εξασφαλίζονται τόσο η προτεραιότητα των κλήσεων τους όσο και οι υψηλές ταχύτητες των δεδομένων. Οι κλήσεις των συνδρομητών προηγούνται όλων των άλλων συνδρομητών κινητής τηλεφωνίας.

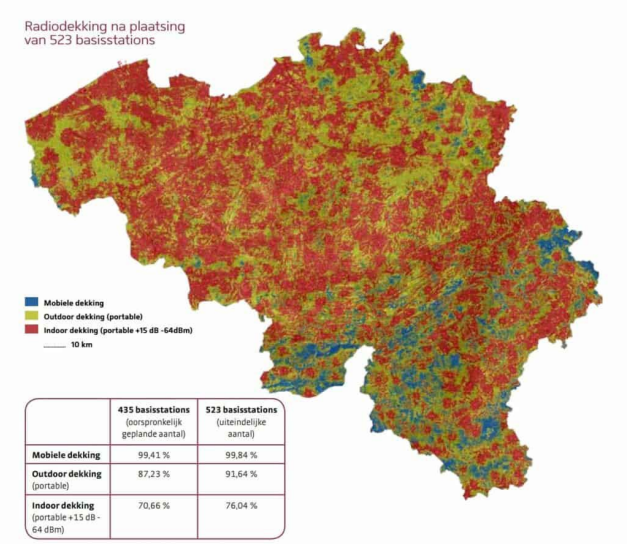
Παρά το γεγονός πως τα δεδομένα κινούνται μέσω των εμπορικών δικτύων κινητής τηλεφωνίας η ασφάλεια είναι εξασφαλισμένη. Για κάθε σύνδεση, η ASTRID δημιουργεί ένα είδος “tunnel” (VPN) μεταξύ του τερματικού κινητού σταθμού και του κέντρου δεδομένων της ASTRID.Αυτή η χρήση του Virtual Private network εξασφαλίζει την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Πρόσβαση στο «νέφος» καθώς και στο τοπικό δίκτυο (LAN). Η κάρτα SIM της ASTRIDπαρέχει πρόσβαση του χρήστη στο «νέφος» με δυνατότητα να χρησιμοποιήσει εφαρμογές στις οποίες έχει λάβει εξουσιοδότηση από την υπηρεσία του.

Διαχείριση του προϋπολογισμού. Ο οργανισμός που ανήκει ο κάθε χρήστης μπορεί να αποφασίσει για το τι θα συμβεί εφόσον καταναλωθεί το όριο των δεδομένων. Ο χρήστης (σε επίπεδο υπηρεσίας) θα μπορούσε να ενεργοποιήσει ένα σύστημα προειδοποίησης για να προσθέσει δεδομένα ή να διακόψει τη χρήση σε έναν ή περισσότερους τελικούς χρήστες.

Υποστήριξη 24/7. Το κέντρο επισκευών ASTRID Service Center (ASC) [433] λειτουργεί όλο το 24ώρο επτά ημέρες την εβδομάδα και είναι προσαρμοσμένο στις απαιτήσεις των υπηρεσιών δημόσιας ασφάλειας.

6.1.1.1.4 Το μέλλον του δικτύου

Το Βέλγιο εκτιμά πως η μετάβαση από το TETRA στο LTE θα ξεκινήσει το 2025-2030 και η τεχνολογία θα ενσωματωθεί σταδιακά, με το TETRA να συνεχίζει να λειτουργεί παράλληλα με το LTE [434].



Εικόνα 174. Η κάλυψη του δικτύου ASTRID TETRA (523 B.S.)

6.1.1.2 Ηνωμένο Βασίλειο

6.1.1.2.1 Ιστορικό

Τη δεκαετία του 1990, η κυβέρνηση του Ηνωμένου Βασιλείου ανέθεσε σε μια κοινοπραξία υπό την ηγεσία της British Telecommunications (BT), τη δημιουργία ενός δικτύου για την κάλυψη των αναγκών των υπηρεσιών δημόσιας ασφαλείας [435]. Η εταιρεία διαχείρισης του δικτύου που ιδρύθηκε ήταν η BT Airwave, η οποία ανέλαβε αρχικά τη διασφάλιση των επικοινωνιών σε όλες τις αστυνομικές δυνάμεις του Ηνωμένου Βασιλείου. Αργότερα η κάλυψη επεκτάθηκε και στις παρακάτω υπηρεσίες:

- Διακομιδές με Ασθενοφόρα
- Πυροσβεστική υπηρεσία
- Εξουσιοδοτημένοι κυβερνητικοί οργανισμοί

Το 2000 υπογράφηκε η συμφωνία μεταξύ της κοινοπραξίας και της Βρετανικής κυβέρνησης για τη λειτουργία του δικτύου [435]. Το Airwave είναι ένα δίκτυο τεχνολογίας TETRA το οποίο παρέχει υπηρεσίες φωνής και σύντομων μηνυμάτων. Σήμερα διαθέτει περίπου 300.000 χρήστες σε περισσότερες από 300 υπηρεσίες δημόσιας ασφάλειας και καλύπτει το 99% της χερσαίας επικράτειας του Ηνωμένου Βασιλείου [436].

Παρά το γεγονός πως οι επιδόσεις των υπηρεσιών της Airwave θεωρούνται πολύ καλές, ο περιορισμός της τεχνολογίας TETRA που δεν επιτρέπει τη μεταφορά μεγάλης ταχύτητας δεδομένων σε συνδυασμό με την εκτίμηση του Υπουργείου Εσωτερικών ότι το κόστος των υπηρεσιών της Airwave ήταν πολύ υψηλό, αποφασίστηκε το 2011 η αντικατάσταση του δικτύου με τη δημιουργία ενός νέου ευρυζωνικού ESN βασισμένου στις τεχνολογίες 4G/LTE. Εκτιμάται ότι περισσότεροι από 300.000 χρήστες δημόσιας ασφάλειας, 45.000 οχήματα και 66 αεροσκάφη στην Αγγλία, τη Σκωτία και την Ουαλία θα χρησιμοποιούν το νέο αυτό δίκτυο, ενώ η διοίκηση και η εποπτεία του θα πραγματοποιείται σε περισσότερα από 100 κέντρα ελέγχου [436]. Χαρακτηριστικό στιγμιότυπο χρήσης εξοπλισμού ESN από προσωπικό της Αγγλικής Αστυνομίας φάινεται στην Εικόνα 175.

Εικόνα 175. ESN χρήση smartphone από στελέχη της βρετανικής αστυνομίας [437]

6.1.1.2.2 Διαμόρφωση του δικτύου

Το ESN χρησιμοποιεί το δίκτυο LTE ενός εμπορικού MNO με εκτεταμένη κάλυψη. Ο MNO είναι η εταιρεία EE, μέλος του ομίλου της British Telecom. Οι υπηρεσίες δημόσιας ασφάλειας έχουν εξασφαλισμένη πρόσβαση σε λειτουργίες QPP.H Βρετανική κυβέρνηση έχει νομοθετήσει τη χρήση αποκλειστικού ραδιοφάσματος για τις επικοινωνίες αέρος - εδάφους στη ζώνη 40 του LTE με εύρος ζώνης 5MHz για τους χρήστες δημόσιας ασφαλείας. Αντίθετα στις επίγειες επικοινωνίες, χρησιμοποιείται το φάσμα του συγκεκριμένου MNO.

Το ESN [438] διαθέτει περισσότερους από 19.500 ιστούς σε όλη την Αγγλία, τη Σκωτία και την Ουαλία, όπως επίσης και χιλιάδες θέσεις μετάδοσης για την κάλυψη του οδικού δικτύου που ξεπερνά τα 540.000 Km. Έως τον Μάρτιο του 2022 είχαν επίσης κατασκευαστεί πάνω από 650 νέες τοποθεσίες 4G, παρέχοντας για πρώτη φορά κρίσιμης σημασίας ευρυζωνικές υπηρεσίες σε πολλές κοινότητες.

Το ESN διαθέτει επίσης έναν στόλο οχημάτων ταχείας αντίδρασης, συμπεριλαμβανομένων των κυψελών σε τροχούς (Cell-on-wheels), με δυνατότητα παροχής έκτακτης και προσωρινής κάλυψης απομακρυσμένων περιοχών με απόκριση λίγων ωρών (Εικόνα 176).

Το πρόγραμμα Διευρυμένης Υπηρεσίας Περιοχής (Extended Area Services-EAS) του Υπουργείου Εσωτερικών, αποσκοπεί στην κατασκευή 292 πρόσθετων θέσεων για τη βελτίωση της κάλυψης στις αγροτικές και απομακρυσμένες περιοχές. Σε αυτές τις τοποθεσίες θα είναι επίσης δυνατή η χρήση των υπηρεσιών και από άλλους φορείς εκμετάλλευσης [438].

Άλλες προγραμματισμένες δραστηριότητες για την επέκταση της κάλυψης περιλαμβάνουν το μετρό του Λονδίνου καθώς και τις επικοινωνίες αέρος - εδάφους από τα 500 έως τα 10.000 πόδια. Επίσης το ESN προσφέρει παράκτια κάλυψη που φτάνει τα 7 ναυτικά μίλια [439].

Εικόνα 176. Δίκτυο υπηρεσιών έκτακτης ανάγκης της BT [437]

6.1.1.2.3 Επιχειρηματικό μοντέλο

Το επιχειρηματικό μοντέλο του ESN βασίζεται στη κοινή χρήση του δικτύου (Εικόνα 177). Η ΕΕ είναι ο MNO και είναι υπεύθυνος για:

- τις υπηρεσίες MC RAN και την επέκταση της κάλυψης με την δημιουργία νέων τοποθεσιών του ραδιοδικτύου.
- την παροχή του απαραίτητου ραδιοεξοπλισμού,
- την ανάπτυξη των υπηρεσιών εκτεταμένης περιοχής
- την εγκατάσταση και συντήρηση του εξοπλισμού

Η ΕΕ εξασφαλίζει επίσης το κεντρικό δίκτυο για:

- τις υπηρεσίες δημόσιας ασφάλειας
- την παροχή υπηρεσιών υποστήριξης
- την διαχείριση της διαθεσιμότητας και χωρητικότητας
- την δοκιμή των κινητών συσκευών

Η ΕΕ ανέλαβε αρχικά τη σύμβαση του ESN τον Δεκέμβριο του 2015, η οποία επρόκειτο να διαρκέσει έως το 2021. Λόγω καθυστερήσεων στο έργο, η σύμβαση παρατάθηκε το 2019 με νέα ημερομηνία λήξης τον Δεκέμβριο του 2024. Η αξία της σύμβασης ανέρχεται σε 895,7 εκατομμύρια GBP. Η ΕΕ πληρώνεται για την παράδοση των επεκτάσεων του δικτύου με βάση την υλοποίηση συγκεκριμένων στόχων, ακολουθώντας το συμφωνηθέν χρονοδιάγραμμα [439].

Για την υλοποίηση του έργου απαιτείται η σύμπραξη και συνεργασία πολλών εταιρειών και οργανισμών στους παρακάτω τομείς:

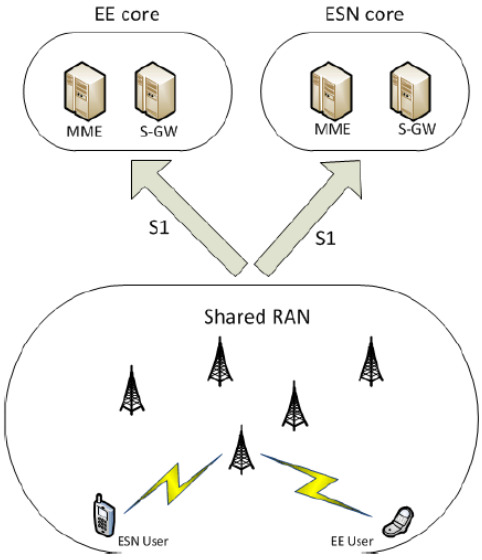
- Στην παροχή εξειδικευμένων λύσεων (παράδειγμα η ανάπτυξη της εφαρμογής MCPTT)
- Στον τομέα διαχείρισης των χρηστών και των συσκευών
- Στη διαχείριση των καρτών SIM
- Στην υποστήριξη πελατών
- Στη διαχείριση των υπηρεσιών
- Στη προμήθεια των συσκευών για τους χρήστες
- Την ανάπτυξη λύσεων κάλυψης σε εξειδικευμένα περιβάλλοντα όπως τα αεροσκάφη και το μετρό του Λονδίνου.

Αυτή η πολυπλοκότητα του έργου απαιτεί από το Υπουργείο Εσωτερικών του ΗΒ να αναλάβει έναν κεντρικό συντονιστικό ρόλο για την επίβλεψη των επιμέρους σταδίων υλοποίησης και διαχείρισης του έργου. Ωστόσο, υπάρχουν ακόμη ασάφειες αναφορικά με το ποιος φορέας ασκεί τον έλεγχο για την ολοκλήρωση των υπηρεσιών από άκρο σε άκρο,

γεγονός που οδηγεί και σε σημαντικές καθυστερήσεις του έργου σύμφωνα με την έκθεση του Εθνικού Ελεγκτικού Γραφείου που εκπονήθηκε το 2019 (National Audit Office).

6.1.1.2.4 Κατάσταση

Το ESN βρίσκεται επί του παρόντος στη φάση της υλοποίησής του. Αρχικά, το έργο αποσκοπούσε στην αντικατάσταση του δικτύου Airwave με το ESN έως το τέλος του 2019- ωστόσο, λόγω διαφόρων λόγων, όπως η ασυμβατότητα των προτύπων ανάμεσα στους προμηθευτές, η ύπαρξη διαφωνιών για θέματα σχετικά με την ολοκλήρωση του συστήματος και τις αρμοδιότητες τεχνικού σχεδιασμού, καθώς και καθυστερήσεων στην παράδοση συμφωνηθέντων έργων, το έργο οδηγήθηκε σε επανεκκίνηση το 2018 [439]. Το Υπουργείο Εσωτερικών επέλεξε ένα μοντέλο υλοποίησης του έργου σε στάδια λαμβάνοντας υπόψη τις προτεραιότητες των οργανισμών-χρηστών έναντι μιας προσέγγισης "Μεγάλης έκρηξης". Η διανομή του νέου χρονοδιαγράμματος πραγματοποιήθηκε το 2021, με τη μετάβαση των χρηστών στο νέο δίκτυο να εκτιμάται για το 2024 και τις υπηρεσίες του δικτύου Airwave να διακόπτονται έως τα τέλη του 2026.



Εικόνα 177. Πρακτική χρήση του MOCN στο ESN [440]

6.1.1.3 Γαλλία

6.1.1.3.1 Ιστορικό

Η Γαλλία διαθέτει δύο εθνικά δίκτυα δημόσιας ασφάλειας βασισμένα στη τεχνολογία Tetrapol [441]:

a. Το πρώτο είναι το RUBIS [442] το οποίο λειτουργεί από το 1992 και σχεδιάστηκε για να καλύψει τις ανάγκες της Γαλλικής χωροφυλακής που δραστηριοποιείται στις αγροτικές

περιοχές της χώρας. Διαθέτει 470 σταθμούς βάσης και οι μεταδόσεις πραγματοποιούνται στη συχνότητα των 80MHz.Το RUBIS εξυπηρετεί 90 χιλιάδες χρήστες σε όλη την επικράτεια της Γαλλίας [443]

b. Το δεύτερο είναι το INPT [444] που ξεκίνησε τη λειτουργία του το1994 και διαθέτει 1500 σταθμούς βάσης με ζώνη εκπομπής 380-400 Mhz, παρέχοντας υπηρεσίες στους παρακάτω οργανισμούς:

   - Γαλλική αστυνομία
   - Πυροσβεστική
   - Υπηρεσίες υγειονομικής περίθαλψης έκτακτης ανάγκης
   - Τελωνεία
   - Ένοπλες Δυνάμεις εντός της εθνικής επικράτειας
   - Χωροφυλακή (Κινητές μονάδες)
   - Αρχές Τοπικής Αυτοδιοίκησης
   - Διοίκηση σωφρονιστικών καταστημάτων με κύρια εφαρμογή στις μεταγωγές κρατουμένων.

Το INPT και το RUBIS είναι διασυνδεδεμένα και παρέχουν πλήρη διαλειτουργικότητα μεταξύ των δυνάμεων των παραπάνω οργανισμών. Μαζί, τα δυο δίκτυα αυτά εξυπηρετούν περίπου 300 χιλιάδες χρήστες. Τα δίκτυα αυτά ανήκουν και διαχειρίζονται από την Γαλλική κυβέρνηση.

Οι περιορισμοί της τεχνολογίας στενής ζώνης και οι απαιτήσεις των πρώτων ανταποκριτών για μετάδοση βίντεο, εικόνας αλλά και δεδομένων οδήγησαν την Γαλλική κυβέρνηση στην απόφαση να αναπτύξει ένα νέο ασύρματο ευρυζωνικό δικτύο δημόσιας ασφάλειας ικανό να ανταπεξέλθει στις σύγχρονες απαιτήσεις των ειδικών δυνάμεων [443] αλλά και όλων των άλλων υπηρεσιών προστασίας του πολίτη.

Το γαλλικό υπουργείο εσωτερικών τον Οκτώβριο του 2022 υπέγραψε τις δημόσιες συμβάσεις για την ανάπτυξη του Réseau Radio du Futur (RRF) με χρονοδιάγραμμα υλοποίησης το2024 όπου και θα είναι έτοιμο για τους θερινούς ολυμπιακούς αγώνες που θα πραγματοποιηθούν στο Παρίσι. Το RRF έχει ως στόχο να φέρει κινητές ευρυζωνικές υπηρεσίες σε όλες τις δημόσιες υπηρεσίας ασφαλείας στη Γαλλία, με τελικό στόχο να εξυπηρετεί 700 χιλιάδες χρήστες [443].

6.1.1.3.2 Διαμόρφωση δικτύου

Το RRF βασίζεται στον διαμοιρασμό δικτύου με την λειτουργία ενός Κινητού Εικονικού Διαχειριστή του Δικτύου (Mobile Virtual Network Operator – MVNO) [441], σε συνεργασία με δύο MNO οι οποίες θα παρέχουν υπηρεσίες MC RAN και υπηρεσίες δικτύου πυρήνα στο χαμηλότερο επίπεδο. Κύριος στόχος του αποτελεί η παροχή στους χρήστες συγκεκριμένη Ποιότητα υπηρεσιών με Προτεραιότητα και Προαίρεση (Quality of Service Priority and Preemption – QPP). Οι υπηρεσίες του RRF ακολουθούν τα πρότυπα MCS του 3GPP για να εξασφαλιστεί η συμβατότητα με άλλους παρόχους υπηρεσιών, διασφαλίζοντας ταυτόχρονα και τη διαλειτουργικότητα με γειτονικές χώρες.

Η κάλυψη του RRF βασίζεται στην κάλυψη των δικτύων των MNOs. Το σχέδιο περιλαμβάνει επίσης αναπτυσσόμενα δίκτυα και πρόσθετες σταθερές ραδιοεγκαταστάσεις για την επέκταση της κάλυψης και της χωρητικότητας ανάλογα με τις προκύπτουσες ανάγκες. Στη Γαλλία, υπάρχουν δύο αποκλειστικές ζώνες για τη δημόσια ασφάλεια, η B28 και B68, στη ζώνη των 700 MHz τις οποίες και θα χρησιμοποιεί το RRF.

Επίσης έχει εξασφαλιστεί και η δυνατότητα εθνικής περιαγωγής με στόχο την επέκταση της κάλυψης και της χωρητικότητας με την προσθήκη του δικτύου και άλλων παρόχων.

6.1.1.3.3 Επιχειρηματικό μοντέλο

Οι συμβάσεις για την προμήθεια των υπηρεσιών και του εξοπλισμού για το RRF χωρίζεται σε τρία τμήματα και πραγματοποιήθηκε τον Οκτώβριο του 2022 [445].

- Το πρώτο τμήμα αφορά υπηρεσίες MC RAN με δύο MNO, συμπεριλαμβανομένων των χαμηλότερων πυρήνων για υπηρεσίες δικτύου.
- Στο δεύτερο τμήμα περιλαμβάνονται, το ανώτερο δίκτυο πυρήνα LTE, μια λύση για τις υπηρεσίες MCS, μια πύλη Tetrapol για διασύνδεση με τα προηγούμενα δίκτυα, συσκευές χρηστών, κάρτες SIM καθώς και λύσεις που αφορούν την ασφάλεια του δικτύου.
- Το τρίτο τμήμα περιλαμβάνει λύσεις διαχείρισης καθώς και υπολογιστικά συστήματα υποστήριξης των φορέων.

Το επιχειρηματικό μοντέλο για την παροχή υπηρεσιών του RRF υλοποιείται σύμφωνα με τις παραπάνω συμβάσεις, και περιλαμβάνει δύο MNO που θα παρέχουν το MC RAN και ενός ελεγχόμενου από την κυβέρνηση φορέα παροχής υπηρεσιών, υπεύθυνο για την συνολική λειτουργία του RRF.

6.1.1.3.4 Κατάσταση Σήμερα

Το υπουργείο εσωτερικών και υπερπόντιων περιοχών της Γαλλίας στις 13 Οκτωβρίου 2022 υπέγραψε την έναρξη του έργου που θα κοστίσει περισσότερο από 700 εκ. ευρώ με ένα

κονσόρτσιουμ εταιριών [445]. Ηγετική θέση σε αυτή την σύμπραξη έχουν οι παρακάτω εταιρίες, οι οποίες ανέλαβαν και τα συγκεκριμένα τμήματα του έργου [446]:

1ο τμήμα: Οι Orange και Bouygues Telecom οι οποίοι είναι οι δυο MNO και θα προσφέρουν υπηρεσίες MCRAN.

2ο τμήμα: η Airbus που θα αναλάβει το τεχνολογικό κομμάτι διασύνδεσης όλων των μερών μαζί με την Capgemini. Η αξία του συμβολαίου είναι 500εκ. ευρώ. Επίσης σε αυτή την προμήθεια η ATOS αναλαμβάνει την ενσωμάτωση του τμήματος του πυρήνα του δικτύου, τις MCX υλοποιήσεις καθώς και τα τερματικά του ραδιοδικτύου.

3ο τμήμα: Η εταιρία ATOS και οι υπόλοιποι συνεργάτες της αναλαμβάνουν την προσφορά λύσεων υπολογιστικής διαχείρισης για περίοδο 7 ετών με συμβόλαιο υπηρεσιών αξίας 43 εκατομμυρίων ευρώ.

Οι στόχοι της γαλλικής κυβέρνησης είναι, να καταστήσει το RRF λειτουργικό κατά την διάρκεια των Ολυμπιακών Αγώνων που θα πραγματοποιηθούν στο Παρίσι το 2024 και να ολοκληρώσει την μετάβαση των χρηστών από τα δίκτυα INPT και RUBIS στο RRF έως το 2025.

6.1.1.4 Φινλανδία

6.1.1.4.1 Ιστορικό

Ο όμιλος «Erillisverkot» που σημαίνει «ειδικό δίκτυο» αποτελεί μια μη κερδοσκοπική εταιρεία που ανήκει στο κράτος της Φινλανδίας. Ιδρύθηκε το 1999 με σκοπό την λειτουργία του εθνικού δημόσιου δικτύου ασφαλείας βασισμένο στην τεχνολογία TETRA με την ονομασία VIRVE. Το δίκτυο αυτό ξεκίνησε την λειτουργία του το 2002 παρέχοντας υπηρεσίες σε κρίσιμους για τη δημόσια ασφάλεια και προστασία του πολίτη οργανισμούς [447], [448], [449].

Οι οργανισμοί που χρησιμοποιούν τις υπηρεσίες του δικτύου είναι:

- Πυροσβεστική υπηρεσία
- Αστυνομία
- Υπηρεσίες επείγουσας ιατρικής διακομιδής (Ασθενοφόρα)
- Συνοριοφυλακή
- Στρατός
- Υπηρεσίες Τελωνίων
- Νοσοκομεία
- Οργανισμοί διαχείρισης Σιδηροδρομικού δικτύου

- Κέντρο Αντιμετώπισης Εκτάκτων Αναγκών
- Υπηρεσία πολιτικής αεροπορίας
- Άλλες αρχές και εταιρείες που σχετίζονται με τις κρίσιμες υποδομές

Σήμερα το δίκτυο διαθέτει 1400 σταθμούς βάσης, παρέχοντας υπηρεσίες, φωνής, σύντομων μηνυμάτων και ομαδικών κλήσεων σε περίπου 51 χιλιάδες συνδρομητές. Το Virve εξυπηρετεί 2 εκατομμύρια ομαδικές κλήσεις / εβδομάδα και 74 εκ. σύντομα μηνύματα / εβδομάδα ενώ η γεωγραφική κάλυψη του δικτύου φτάνει στο 96,7% (Εικόνα 178) με τους χρήστες να δηλώνουν ικανοποιημένοι έως πολύ ικανοποιημένοι από την ποιότητα των παρεχόμενων υπηρεσιών. Ωστόσο, ο ρυθμός μετάδοσης δεδομένων είναι περιορισμένος λόγω της τεχνολογίας TETRA, και το δίκτυο δεν υποστηρίζει σύγχρονες εφαρμογές δεδομένων που απαιτούν οι χρήστες.

Για αυτούς τους λόγους το 2019, η Φινλανδική κυβέρνηση αποφάσισε την ανάπτυξη ενός νέου δικτύου δημόσιας ασφαλείας με φορέα υλοποίησης την Erillisverkot η οποία ανέλαβε την υλοποίηση του Virve 2.0 για την ανάπτυξη κινητών ευρυζωνικών υπηρεσιών δημόσιας ασφάλειας βασισμένο στα πρότυπα του 3GPP και της τεχνολογίας 4G/5G.

6.1.1.4.2 Η διαμόρφωση του δικτύου

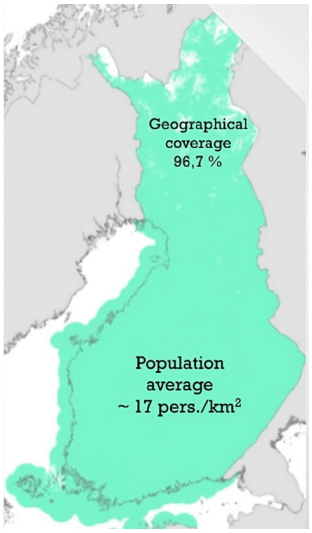
Η αρχιτεκτονική του μοντέλου της Φινλανδίας αποτελείται από:

- Το Ραδιοδίκτυο, το οποίο η Errilisverkot νοικιάζει από έναν ιδιωτικό τηλεπικοινωνιακό πάροχο ο οποίος εξασφαλίζει πως οι χρήστες του δικτύου Virve 2.0 έχουν πάντα προτεραιότητα στις υπηρεσίες του ραδιοδικτύου (RAN) έναντι των συνδρομητών του τηλεπικοινωνιακού παρόχου.
- Το αποκλειστικό δίκτυο πυρήνα (EPC) που ανήκει στην Errilisverkot και αναπτύχθηκε σε συνεργασία με την Ericsson [450].
- Το Ραδιοφάσμα, το οποίο είναι το ίδιο που χρησιμοποιεί ο τηλεπικοινωνιακός πάροχος, λαμβάνοντας υπόψη πως στη Φινλανδία δεν έχει θεσμοθετηθεί συγκεκριμένη συχνότητα (π.χ.700Mhz) για τα δημόσια δίκτυα ασφαλείας όπως έχει νομοθετηθεί σε άλλες χώρες.

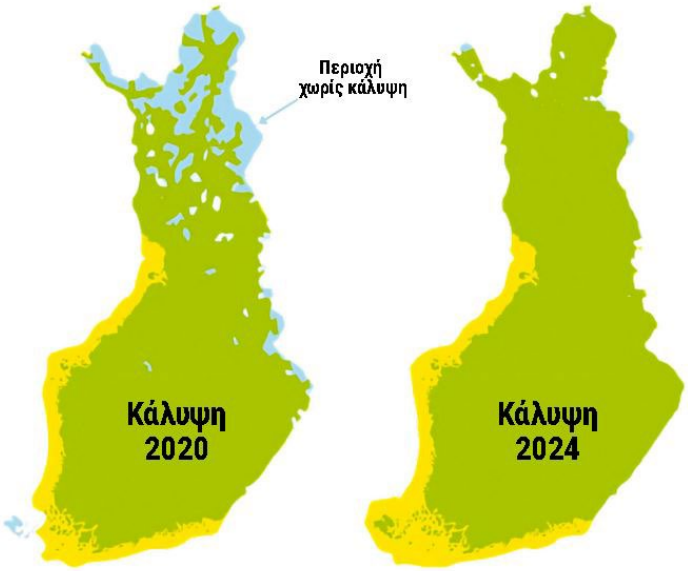
6.1.1.4.3 Επιχειρηματικό μοντέλο

Η Erillisverkot είναι ο κρατικός φορέας υπεύθυνος για την παροχή υπηρεσιών του δικτύου δημόσιας ασφαλείας Virve 2.0. Η Erillisverkot είναι υπεύθυνη για την διαχείριση, συντήρηση και ανάπτυξη του Virve 2.0. καθώς επίσης και για την παροχή ολοκληρωμένων υπηρεσιών σε όλους τους οργανισμούς που σχετίζονται με την δημόσια ασφάλεια στην Φινλανδία.

Η Elisa συγκαταλέγεται στις τρείς μεγαλύτερες εταιρείες παροχής κινητής τηλεφωνίας της Φινλανδίας, και αποτελεί τον κύριο πάροχο προσφοράς κρίσιμων υπηρεσιών ραδιοδικτύου (MCRAN) στην Erillisverkot [451]. Η Φινλανδία έχει επίσης νομοθετήσει την εθνική περιαγωγή ώστε να υπάρχει η δυνατότητα αξιοποίησης των υπηρεσιών και άλλων παρόχων κινητής τηλεφωνίας όπου αυτό κριθεί απαραίτητο.



Εικόνα 178. Γεωργαφική κάλυψη του δικτύου VIRVE (2020)



Εικόνα 179. Προγραμματισμός γεωργραφικής κάλυψης δικτύου VIVRE2 [447]

Ως πρωτεύων πάροχος, η Elisa καλείται να επεκτείνει την κάλυψη, να αυξήσει τη χωρητικότητα και την ανθεκτικότητα του δικτύου ώστε να εκπληρώσει τις απαιτήσεις του Virve 2.0. και των χρηστών δημόσιας ασφάλειας. Ο στόχος της κάλυψης είναι να επιτευχθεί 97% γεωγραφική κάλυψη και 99,98% πληθυσμιακή κάλυψη μέχρι το 2024 (Εικόνα 179).

Η Erillisverkot και η Elisa έχουν συνάψει 10ετή συμφωνία [451], και στο τέλος αυτής θα επαναπροκηρυχθεί διαγωνισμός για τις υπηρεσίες ραδιοπρόσβασης. Σύμφωνα με τη

φινλανδική νομοθεσία, η Erillisverkot έχει το αποκλειστικό δικαίωμα παροχής επικοινωνιών σε υπηρεσίες δημόσιας ασφάλειας. Ως εκ τούτου, η Erillisverkot και η Elisa δεν βρίσκονται υπό καθεστώς μεταξύ τους ανταγωνισμού στις επικοινωνίες δημόσιας ασφάλειας. Απώτερος στόχος είναι η μετάβαση όλων των χρηστών του Virve στο Virve 2.0. Όταν οι υφιστάμενες υπηρεσίες του Virve δεν είναι πλέον χρήσιμες, το δίκτυο θα κλείσει. Άλλωστε το Virve 2.0 δεν αποτελεί προσθήκη στο υπάρχον δίκτυο αλλά αποτελεί ένα νέο δίκτυο (Εικόνα 180).

6.1.1.4.4 Σημερινή Κατάσταση

Το δίκτυο Virve 2.0 που περιλαμβάνει 4G και 5G RAN βρίσκεται ήδη στο στάδιο της υλοποίησης. Το 2020 υπογράφηκαν οι συμφωνίες τόσο για τον κύριο τηλεπικοινωνιακό πάροχο του ραδιοδικτύου όσο και για την εταιρεία που ανέλαβε την υλοποίηση του δικτύου πυρήνα. Η περίοδος μετάβασης από το Virve στο Virve 2.0 έχει προγραμματιστεί για το 2023-2025 όπου και τα δυο δίκτυα θα λειτουργούν ταυτόχρονα. Ο εκτιμώμενος αριθμός χρηστών του Virve 2.0 εκτιμάται πως θα φτάσει τις 51 χιλιάδες.

6.1.1.4.5 Διδάγματα και Προκλήσεις

Σύμφωνα με τον Kari Junttila, Αναπτυξιακό διευθυντή της Erillisverkot τα διδάγματα και οι προκλήσεις που αντιμετώπισαν στη διάρκεια του έργου [447] ήταν:

- Ο σχεδιασμός της μετάβασης για τους χρήστες απαιτεί πολύ καλό προγραμματισμό, προετοιμασία και συντονισμό.
- Δεν ήταν εύκολο το εγχείρημα ειδικά όταν είσαι ο πρώτος που το υλοποιεί.
- Είναι πολύ σημαντική η διαχείριση των προσδοκιών λαμβάνοντας υπόψη ότι γίνεται χρήση νέας μη δοκιμασμένης τεχνολογίας.
- Η κάλυψη του ραδιοδικτύου απαιτεί αντίστοιχες επιδόσεις των τερματικών RF
- Σημαντική επίσης παράμετρος δυσκολίας αποτελεί η μεγάλη έκταση της χώρας και ο μικρός αριθμός χρηστών.

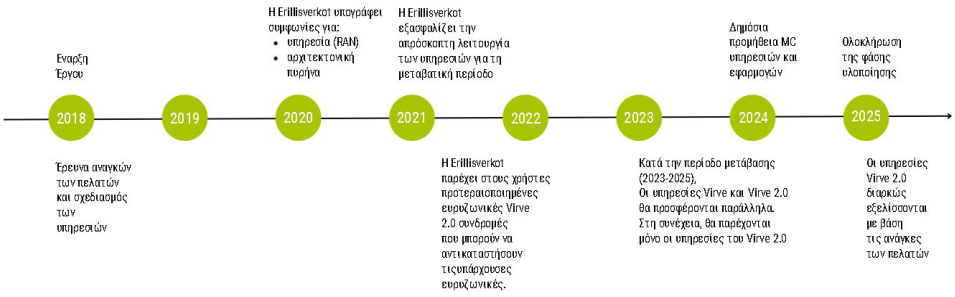
6.1.1.4.6 Το Μέλλον του δικτύου

Οι μελλοντικοί στόχοι της Erillisverkot είναι:

- Η δημιουργία ενός αναβαθμισμένου ευρυζωνικού διασυνδεδεμένου δικτύου στα πρότυπα του σημερινού δικτύου TETRA με τις υπόλοιπες σκανδιναβικές χώρες (Νορβηγία και Σουηδία).

- Η προετοιμασία του ευρωπαϊκού προγράμματος Broadway και η εξέλιξη του ως Broadnet με στόχο την περιαγωγή μεταξύ των δημόσιων δικτύων ασφαλείας και αποκατάστασης καταστροφών των ευρωπαϊκών χωρών.
- Προσθήκη εθνικής περιαγωγής με στόχο την βελτίωση της ανθεκτικότητας του δικτύου σε περιπτώσεις βλάβης εξοπλισμού με μικρό πρόσθετο κόστος. Όχι για την αντικατάσταση της κύριας κάλυψης.

Η Φινλανδία ως χώρα παραγωγός καινοτομίας και τεχνολογίας, πρωταγωνιστεί σε παγκόσμιο επίπεδο στην ανάπτυξη ευρυζωνικού δικτύου δημόσιας ασφάλειας με ενεργό συμμετοχή στις ομάδες εργασίας προτυποποίησης του 3GPP για MCX υπηρεσίες, γεγονός που αποτελεί εξαιρετική μελέτη περίπτωσης και για άλλες χώρες που επιθυμούν να αποκτήσουν ευρυζωνικά δημόσια δίκτυα ασφαλείας βασισμένα στις τεχνολογίες 4G/5G.



Εικόνα 180. VIVRE 2. Οδικός χάρτης του έργου [452]

6.1.2 Αμερική

6.1.2.1 Ηνωμένες Πολιτείες Αμερικής

Αναλυτική αναφορά για το επίγειο δίκτυο δημόσιας ασφάλειας P25 που χρησιμοποιούν οι Η.Π.Α. εδώ και τρεις δεκαετίες έγινε ήδη στο κεφάλαιο 5.2.1.1.1, ενώ όμοια για το ευρυζωνικό δίκτυο δημόσιας ασφάλειας FirstNet που υλοποιήθηκε και τέθηκε σε λειτουργία από το 2018 έχει ήδη πραγματοποιηθεί στο κεφάλαιο 5.2.1.3.1.

6.1.3 Ασία – Ειρηνικός

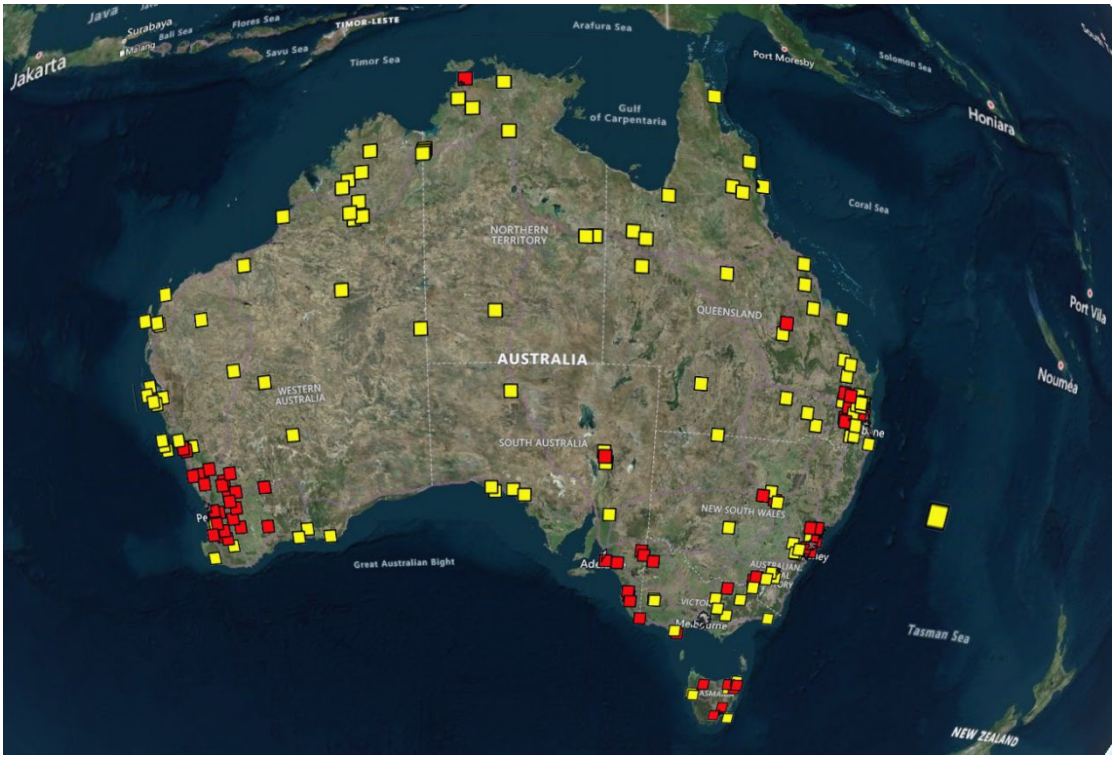
6.1.3.1 Αυστραλία

Η Αυστραλία βρίσκεται σήμερα σε ένα μεταβατικό στάδιο από τα συστήματα APCO25 και DMR/PMR σε LTE συστήματα ταυτόχρονα με τη χρήση μη επίγειων επικοινωνιών [453]. Σύμφωνα με την [454] εκτιμάται πως έως το 2028 θα συνυπάρχουν αυτές οι τεχνολογίες πριν γίνει η μετάβαση σε υβριδικά ευρυζωνικά συστήματα (5G και Non Terrestrial Networks). Αρμόδια υπηρεσία για την ανάπτυξη της κυβερνητικής στρατηγικής για την

διασυνδεσιμότητα είναι η NSW Telco Authority (NSWTA) καθώς επίσης και για την παροχή υπηρεσιών κρίσιμων επικοινωνιών προς το κράτος μέσω του δημόσιου δικτύου ασφαλείας (PSN). Κύριος στόχος της κυβέρνησης της Αυστραλίας αποτελεί η «*δημιουργία ενός δημόσιου δικτύου ασφάλειας που θα συγκαταλέγετε στα μεγαλύτερα του κόσμου*» σύμφωνα με την Kylie De Courteney Διευθύνουσα σύμβουλο του Οργανισμού τηλεπικοινωνιών της Αυστραλίας (NSW Telco Authority) [455]

6.1.3.1.1 Κάλυψη του δικτύου

Τον Αύγουστο του 2022 προστέθηκαν επιπλέον 250 σταθμοί καλύπτοντας το 97% του πληθυσμού της χώρας και 44.5% της γεωγραφικής έκτασης, ενώ με την ολοκλήρωση αυτού του δικτύου θα υπάρχουν 675 σταθμοί οι οποίοι θα καλύπτουν το 99,7% του πληθυσμού με γεωγραφική κάλυψη 85% της επικράτειας [455].



Εικόνα 181. Πρόγραμμα Mobile Black Spot - Χρηματοδοτούμενοι σταθμοί βάσης. Φάση 5 [456]

Το PSN της NSW Telco με αριθμούς:

- 13 εκατομμύρια κλήσεις / μήνα
  - ❖ 60 Υπηρεσίες που το χρησιμοποιούν
  - ❖ 99.95 Διαθεσιμότητα του δικτύου
- 45% Γεωγραφική κάλυψη

Ή Αυστραλία επίσης πραγματοποίησε μια δοκιμή (Μάιος 2021 - Δεκέμβριος 2022) [457], [458] ενός κοινόχρηστου δικτύου PSMB (Public Safety Mobile Broadband) στο οποίο η κυβέρνηση χειρίζεται το κεντρικό δίκτυο και τις εφαρμογές ενώ χρησιμοποιεί τα δίκτυα

ραδιοπρόσβασης δύο παρόχων εμπορικών υπηρεσιών (CSP) για να επεκτείνει την εμβέλεια, την ανθεκτικότητα και την αξιοπιστία του. Αυτή η δοκιμή πραγματοποιήθηκε για πρώτη φορά με χρήση δυο παρόχων σε αντίθεση με άλλες χώρες όπως οι Η.Π.Α (FirstNet) το Ηνωμένο Βασίλειο (ESN) και τη Φινλανδία (Vivre2) που χρησιμοποιούν ένα πάροχο. [4]

6.1.3.1.2 Χρήση μη επίγειων συστημάτων επικοινωνιών

Παράλληλα στις 21 Δεκεμβρίου 2021 ανακοινώθηκε η κύρια φάση ανάπτυξης δορυφορικών υπηρεσιών [453], οι οποίες θα προσδώσουν μια σημαντική βελτίωση στις επείγουσες επικοινωνίες τόσο για τις κοινότητες όσο και για τους οργανισμούς που δραστηριοποιούνται και διαχειρίζονται επείγουσες καταστάσεις. Η ανάπτυξη των υπηρεσιών θα πραγματοποιηθεί σε συνεργασία με τον δορυφορικό οργανισμό Inmarsat και στο πλαίσιο αυτής της συμφωνίας η κυβέρνηση της Αυστραλίας θα εξοπλίσει με δορυφορικό εξοπλισμό περισσότερα από 4200 οχήματα [459], με σκοπό να αντιμετωπίσει προβλήματα όπως:

- Ανομοιόμορφη κάλυψη περιοχών
- Συνδυασμό δικτύων (LMR/Cellular)
- Διασυνδεσιμότητα ανάμεσα στις υπηρεσίες
- Την τεράστια έκταση της χώρας σε συνδυασμό με την αραιή κατοίκηση

Για τον λόγο αυτό, η χώρα έθεσε ορισμένες απαιτήσεις για τις υπηρεσίες εκτάκτου ανάγκης:

- Ομοιόμορφη κάλυψη
- Απλότητα και Ευχρηστία
- Ελαχιστοποίηση της επανεκπαίδευσης του προσωπικού
- MC Voice (MCPTT) & MC Data

Η λύση αυτή δόθηκε σε συνεργασία με την Inmarsat και ουσιαστικά οδηγήθηκαν στο «μια υπηρεσία παντού» η οποία περιλάμβανε:

- Σενάριο πολλαπλών φορέων
- Λειτουργία των οχημάτων ως πύλες
- Αυτόματη μετάβαση ανάμεσα στους φορείς
- Wi-Fi bubble for dismounted personal
- Ασφαλή δικτυακή ενσωμάτωση
- Διαχειρίσιμη υποδομή και κόστη συντήρησης

6.1.3.1.3 Στρατηγική για το μέλλον

Ένας από τους στόχους της NSW Telco για το PSN με βάση την κάλυψη των αναγκών των πρώτων ανταποκριτών αλλά και των χρηστών του δικτύου αποτελεί η αύξηση της ποικιλίας των τεχνολογιών που χρησιμοποιεί. Αν και οι τεχνολογίες LTE καθώς και οι μη επίγειες θα

μπορούσαν να προσφέρουν μεγαλύτερη κάλυψη, χωρίς σημαντικές υποδομές, ωστόσο έχουν μια σειρά από προκλήσεις που θα πρέπει να αντιμετωπίσουν, όπως διαλειτουργικότητα, καθυστέρηση, χωρητικότητα, κόστος και αξιοπιστία.

Το 2022 η NSWTA δημιούργησε ένα πλαίσιο εργασίας όπου δοκιμάστηκαν τεχνολογικές προτάσεις «επόμενης γενιάς», συμπεριλαμβανομένων και μη επίγειων επιλογών (Satellite) καθώς επίσης και δυνατότητες επέκτασης της κάλυψης με χρήση WiFi, LTE (4G/5G) σε οχήματα (Cells on Wheels, COW), με μεταδώσεις μηνυμάτων Mission Critical Messages (MCM) σε LTE (4G/5G) [460]. Η στρατηγική [59] για το 2023 βασίζεται σε 5 κύριους άξονες μαζί με 22 επιμέρους προτεραιότητες. Οι σημαντικότερες από αυτές είναι:

a. Αύξηση της κάλυψης των ευρυζωνικών δικτύων μέσω των προγραμμάτων Mobile Black Spot Program (MBSP) και Connecting Communities (CCC).
b. Βελτίωση της χωρητικότητας της αξιοπιστίας και της διαλειτουργικότητας ανάμεσα στις υπηρεσίες.
c. Δημιουργία νέων εγκαταστάσεων (Critical Communication Enhancement Program, CCEP) και διαχείριση της μετάβασης των πελατών σε αυτές. Πιο συγκεκριμένα έως τα τέλη Ιουνίου (2023) θα πρέπει να έχει επιτευχθεί κάλυψη:
    - 50% γεωγραφική και 98% πληθυσμιακή
    - 89% των εγκαταστάσεων σε επίπεδο σχεδιασμού (598 από 675)
    - 54% των εγκαταστάσεων σε πλήρη λειτουργία (365 από 675)
d. Παροχή νέων καινοτόμων προϊόντων και υπηρεσιών που θα καλύπτουν τις επιχειρησιακές ανάγκες των πελατών. Τουλάχιστον ένα προϊόν ή υπηρεσία για κάθε βασικό πελάτη του δικτύου.
e. Εξέλιξη του προγράμματος Κινητού Ευρυζωνικού Δικτύου Δημόσιας ασφάλειας Public Safety Mobile Broadband, PSMB με εξακρίβωση των δυνατοτήτων υλοποίησης των προτεινόμενων λύσεων σε εθνικό επίπεδο. Στο πλαίσιο αυτό, υλοποιείται η συνεργασία σε διεθνές επίπεδο με αντίστοιχους οργανισμούς άλλων κρατών (Η.Π.Α. Η.Β. Βέλγιο, Φινλανδία, Γαλλία, Γερμανία, Νότια Κορέα κ.α.) με στόχο την λήψη τεχνογνωσίας και την αξιοποίηση για την ανάπτυξη της εθνικής στρατηγικής.

6.1.3.2 Δημοκρατία Νότιας Κορέας

6.1.3.2.1 Ιστορικό

Το 2014, μετά το τραγικό συμβάν στο πλοίο MV Sewol που στοίχισε τη ζωή σε 303 ανθρώπους [461] το υπουργείο εσωτερικών και ασφάλειας (Ministry of the Interior and Safety - MOIS) της Δημοκρατίας της Κορέας αποφάσισε να κατασκευάσει ένα δημόσιο ευρυζωνικό δίκτυο για τη διασφάλιση της δημόσιας ασφάλειας [462]. Στα πλαίσια

υλοποίησης του έργου νομοθετήθηκε ο καθορισμός αποκλειστικής ζώνη συχνοτήτων (B28 - 700MHz) για τις τηλεπικοινωνίες δημόσιας ασφάλειας. Εως τότε η κάλυψη εξασφαλιζόταν από πολυάριθμα δίκτυα διαφορετικής τεχνολογίας (αναλογικά / ψηφιακά - TETRA) τα οποία δεν εξασφάλιζαν τη μεταξύ τους διαλειτουργικότητα. Στόχος του safe-net ήταν η αντικατάσταση αυτών των δικτύων με ένα νέο που θα πρόσφερε τη ζωντανή μετάδοση βίντεο, δεδομένων καθώς και βιομετρικών στοιχείων, με εξασφαλισμένη διαλειτουργικότητα μεταξύ των υπηρεσιών, αποσκοπώντας στη μείωση του χρόνου ανταπόκρισης σε περιστατικά εκτάκτου ανάγκης.

6.1.3.2.2 Διαμόρφωση Δικτύου

Το Safe-Net αποτελείται από τρία επιμέρους δίκτυα που βασίζονται στην τεχνολογία LTE τα όποια εξυπηρετούν διαφορετικές ανάγκες υπηρεσιών:

- Το PS-LTE για τη δημόσια ασφάλεια, το
- LTE-R (Railways) για τους σιδηροδρόμους και το
- LTE-M (Marine) για τους ναυτιλιακούς χρήστες.

Και τα τρία δίκτυα μοιράζονται την ίδια ζώνη συχνοτήτων (B28 στη ζώνη των 700 MHz, 2 × 10 MHz). Το PS-LTE παρέχει υπηρεσίες σε 333 υπηρεσίες στους παρακάτω οκτώ τομείς:

- Πυροσβεστική,
- Πάροχους ηλεκτρικής ενέργειας
- Ακτοφυλακή
- Ένοπλες Δυνάμεις
- Αστυνομία
- Το προσωπικό των ασθενοφόρων
- Πάροχους φυσικού αερίου
- Τοπικές Αρχές

Η αρχιτεκτονική του δικτύου (Εικόνα 182) σχεδιάστηκε με τρείς βασικούς στόχους:

α. την παροχή ενοποιημένων ευρυζωνικών κλήσεων αποσκοπώντας στην ταχεία αντίδραση των υπηρεσιών.

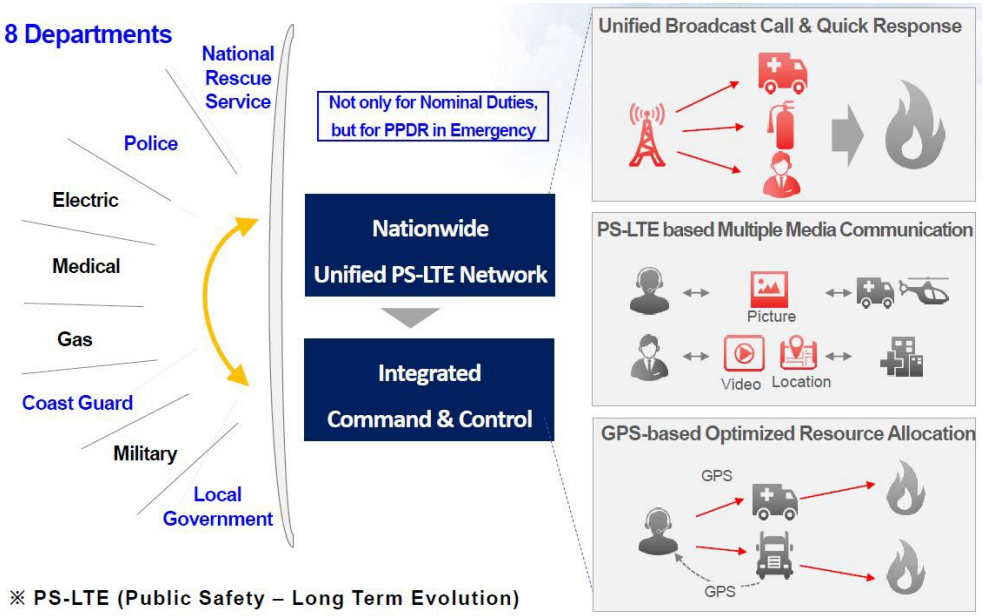
β. την δυνατότητα ανταλλαγής βίντεο, εικόνας και γεωγραφικού στίγματος μεταξύ των πρώτων ανταποκριτών διαφορετικών οργανισμών.

γ. Την σωστή γεωγραφική κατανομή των πόρων για την αντιμετώπιση των φυσικών καταστροφών αξιοποιώντας την τεχνολογία GPS.

Ο εκτιμώμενος αριθμός συσκευών χρηστών ανέρχεται σε 240 χιλιάδες για το PS-LTE, 10 χιλιάδες για το LTE-R και 35 χιλιάδες για το LTE-M [463]. Πριν την ανάπτυξη του δικτύου υπήρξε μια πιλοτική φάση δοκιμής της τεχνολογίας σε ένα μεγάλο αθλητικό γεγονός και ακολούθησαν τρείς επόμενες κατά τις οποίες σταδιακά αναπτύχθηκε το δίκτυο σε όλη τη

χώρα [462]. Η πιλοτική φάση του έργου υλοποιήθηκε με επιτυχία από το MOIS κατά τη διάρκεια των Χειμερινών Ολυμπιακών Αγώνων που διεξήχθησαν στη Pyeong Chang το 2018. Η ανάπτυξη του δικτύου πραγματοποιήθηκε σε τρείς φάσεις. Στη πρώτη φάση η οποία ολοκληρώθηκε τον Σεπτέμβριο του 2019, εγκαταστάθηκαν σταθμοί βάσης σε πέντε μεγάλες πόλεις καθώς και στις επαρχίες της κεντρικής Κορέας. Η δεύτερη φάση ολοκληρώθηκε τον Σεπτέμβριο του 2020, όπου οι σταθμοί βάσης εγκαταστάθηκαν σε εννέα πόλεις και σε επαρχίες του νοτίου τμήματος της χώρας. Στην τρίτη φάση με την οποία ολοκληρώθηκε το Safe-Net τον Μάρτιο του 2021 εγκαταστάθηκαν οι σταθμοί βάσης στη Σεούλ και στις γύρω μητροπολιτικές περιοχές, συμπεριλαμβανομένης και της πόλης Incheon.

Για λόγους ασφαλείας και αποκέντρωσης, κατασκευάστηκαν τρία ανεξάρτητα κέντρα ελέγχου και λειτουργίας σε διαφορετικές πόλεις της χώρας [464]: Στη Σεούλ, στη Daegu και στη νήσο Jeju. Τα κέντρα αυτά εξασφαλίζουν την παροχή υπηρεσιών πυρήνα LTE, υπηρεσίες MCPTT και είναι υπεύθυνα για τη διαχείριση του δικτύου.

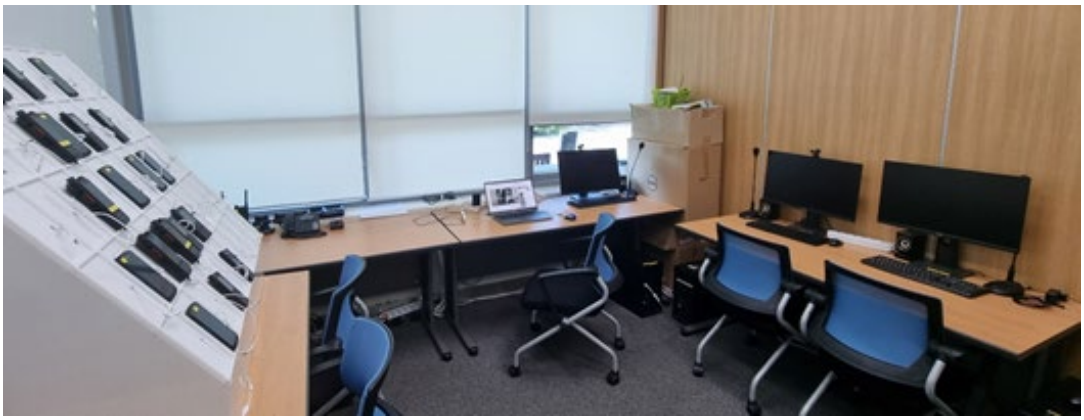


Εικόνα 182. Η αρχιτεκτονική του SafeNet [462]

Type	Phase 1 (Central Korea) Dec. 2018 - Sep. 2019	Phase 2 (Southern Korea) Nov. 2019 - Sep. 2020	Phase 3 (Capital Region) Jun. 2020 - Mar. 2021
			
Zone A	Daejeon, Sejong, Chungnam	Daegu, Gyeongbuk, Jeju	Seoul
Zone B	Gangwon	Gwangju, Jeonbuk, Jeonnam	Gyeonggi
Zone C	Chungbuk	Busan, Ulsan, Gyeongnam	Incheon

Εικόνα 183. Οι φάσεις ολοκλήρωσης του SafeNet [462]

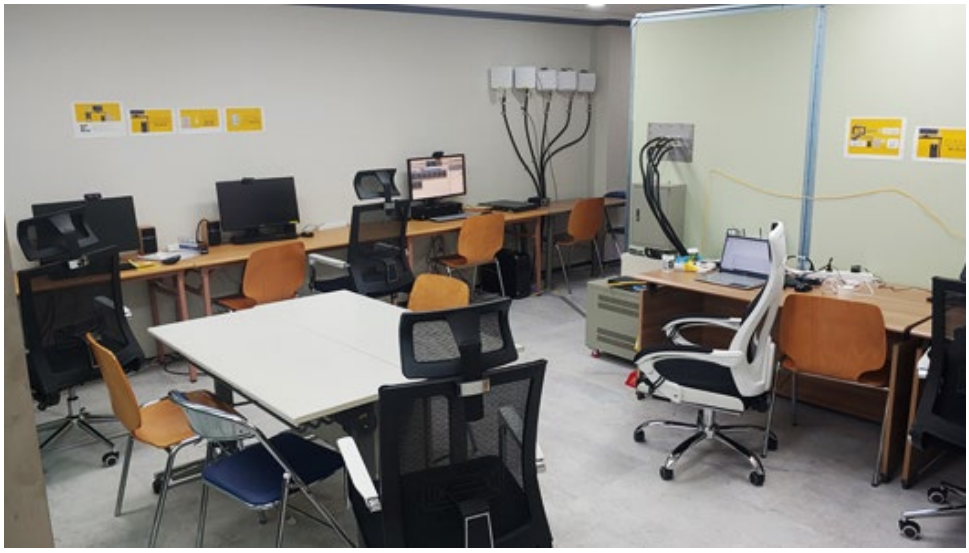
.



Εικόνα 184. Κέντρο Daegu [464]

Εικόνα 185. Κέντρο Daegu - Θωρακισμένο δωμάτιο [464]

Η κάλυψη του δικτύου PS-LTE [463] επιτεύχθηκε με την δημιουργία αποκλειστικών τοποθεσιών (sites) ραδιοεπικοινωνίας LTE με περισσότερους από 17 χιλιάδες σταθμούς βάσης. Η επέκταση τόσο της κάλυψης όσο και της αύξησης της χωρητικότητας μπορεί επιπρόσθετα να εξασφαλιστεί με την κοινή χρήση και άλλων δικτύων, συμπεριλαμβανομένων των εμπορικών κινητών LTE ραδιοδικτύων αλλά και των LTE-R και LTE-M. Ένα ακόμη στοιχείο για την κάλυψη ορεινών περιοχών είναι η χρήση ad-hoc δικτύων που μπορούν να αναπτυχθούν, είτε με χρήση οχημάτων είτε με φορητές λύσεις, όπως κυψέλες τοποθετημένες σε ειδικά σακίδια των πρώτων ανταποκριτών. Το LTE-M παρέχει κάλυψη σε απόσταση έως 100 χιλιόμετρα από την ακτή ενώ το LTE-R παρέχει κάλυψη σε περισσότερα από 4.800 σιδηροδρομικά χιλιόμετρα.



Εικόνα 186. Κέντρο Σεούλ [464]

6.1.3.2.3 Επιχειρηματικό μοντέλο

Η κατασκευή του PS-LTE ανατέθηκε στις Korea Telecom (KT) και SK Telecom (SKT). Η KT είναι υπεύθυνη για δύο περιφέρειες, και η SKT είναι υπεύθυνη για μία. Η KT ανέλαβε επίσης την κατασκευή των τριών κέντρων λειτουργίας. Η επίβλεψη των λειτουργιών του δικτύου καθώς και των κρίσιμων υπηρεσιών (MCPTT4) του Safe-Net πραγματοποιείται από τρία υπουργεία. Το Υπουργείο Εσωτερικών και Ασφάλειας εποπτεύει PS-LTE, το Υπουργείο Ωκεανών και Αλιείας εποπτεύει το LTE-M, και το Υπουργείο Γης, Υποδομών και Μεταφορών επιβλέπει το LTE-R. Έχει επίσης δημιουργηθεί ένα φόρουμ (Safe-Net Forum) το οποίο συντονίζει την έρευνα, την τυποποίηση και εφαρμόζει τις κυβερνητικές πολιτικές που αφορούν το Safe-Net.

6.1.3.2.4 Κατάσταση Σήμερα

Οι υπηρεσίες του δικτύου PS-LTE ξεκίνησαν το 2020 και η ολοκλήρωση της κάλυψης σε εθνικό επίπεδο επιτεύχθηκε το 2021. Η μετάβαση όλων των χρηστών δημόσιας ασφάλειας στο νέο δίκτυο προγραμματίζεται να πραγματοποιηθεί την περίοδο 2020 έως 2027. Οι τομείς στους οποίους έχει δοθεί προτεραιότητα για μελλοντική ανάπτυξη του δικτύου, περιλαμβάνουν τις επικοινωνίες μεταξύ συσκευών (D2D) με στόχο την επέκταση του δικτύου σε περιοχές χωρίς κάλυψη, την αέρος-εδάφους επικοινωνία με χρήση και UAVs, την χρήση αισθητήρων IoT στη δημόσια ασφάλεια και τη σταδιακή εισαγωγή στο 5G η οποία ήδη σήμερα βρίσκεται σε εξέλιξη.

6.2 Συγκριτική αξιολόγηση – βέλτιστες πρακτικές

Από την προσεκτική μελέτη των προσεγγίσεων των παραπάνω χωρών καταλήξαμε στα παρακάτω συμπεράσματα, αφού αποτυπώσαμε τα χαρακτηριστικά τους σε σχετικό ώστε να είναι εφικτή η συγκριτική τους αξιολόγηση:

1. Το κόστος των επενδύσεων που απαιτείται για την ανάπτυξη αποκλειστικών δικτύων ασφαλείας είναι ιδιαίτερα υψηλό και δεν αποτελεί πρώτη επιλογή για τα κράτη.
2. Διαπιστώσαμε επίσης τρία κυρίαρχα μοντέλα που επιλέγουν οι αρμόδιοι φορείς των κρατών για την ανάπτυξη των PSNs.

    α. Κοινή χρήση δικτύου με έναν πάροχο. Σε αυτή την κατηγορία βρίσκονται τρεις χώρες: Οι Η.Π.Α. το Ηνωμένο Βασίλειο και η Φινλανδία. Οι Η.Π.Α. στη μελέτη που πραγματοποίησαν θεώρησαν οικονομικά ασύμφορη την κατασκευή ενός αποκλειστικού δικτύου ασφαλείας και έτσι οδηγήθηκαν στη σύμπραξη με έναν MNO με ένα μακροχρόνιο συμβόλαιο 25 ετών με προσυμφωνημένη ελάχιστη καταβολή ανά έτος, συνολικής αξίας 100 δις δολαρίων. Ευθύνη της AT&T ήταν να αναπτύξει το δίκτυο σε όλη την επικράτεια και να αναλάβει τη συντήρηση, διαχείριση και επέκταση του δικτύου καθώς και των αντίστοιχων υπηρεσιών προς τους χρήστες. Το αποτέλεσμα αυτής της συνεργασίας μπορούμε να το κρίνουμε πως είναι ιδιαίτερα πετυχημένο, απόδειξη οι 3.3 εκατομμύρια χρήστες του First Net που συνεχώς αυξάνονται. Το Ηνωμένο Βασίλειο επέλεξε και αυτό την κοινή χρήση του δικτύου με έναν μόνο πάροχο και παρά τις σημαντικές καθυστερήσεις, σήμερα δείχνει πως η μετάβαση στο LTE 4G ξεκίνησε. Η Τρίτη χώρα που ακολούθησε την επιλογή ενός MNO είναι η Φινλανδία. Το μοντέλο που επέλεξε βασίστηκε στην απλότητα και στην σταδιακή μετάβαση από τα παλαιότερης γενιάς δίκτυα στα ευρυζωνικής τεχνολογίας LTE 4G/5G.Η διαχείριση του δικτύου πυρήνα αποφασίστηκε να ασκείται από την κρατική εταιρία Erillisverkot για λόγους ασφαλείας και το κόστος ανάπτυξης του

δικτύου ανέρχεται στα 1.2 δις δολάρια για το δεκαετές πρόγραμμα που έχει υπογραφεί με τον MNO. Το Μοντέλο της Φινλανδίας κρίνεται πετυχημένο αν λάβουμε υπόψη μας δυο σημαντικές παραμέτρους: ο μικρός αριθμός χρηστών και η τεράστια έκταση που το δίκτυο καλείται να καλύψει, στοιχεία που οδήγησαν την Φινλανδία στην αναζήτηση συνεργασιών σε διεθνές επίπεδο αλλά και στην ανάγκη για προώθηση της επιτάχυνσης της προτυποποίησης με στόχο τη μείωση του κόστους του τηλεπικοινωνιακού εξοπλισμού αλλά και των τελικών συσκευών.

β. Κοινή χρήση δικτύου με περισσότερους από έναν παρόχους**.** Σε αυτή την κατηγορία ανήκουν δυο χώρες, η Γαλλία και το Βέλγιο. Η Γαλλία επέλεξε αυτό το μοντέλο για να εξασφαλίσει τη μεγαλύτερη δυνατή κάλυψη του δικτύου για τις υπηρεσίες της. Το RRF φιλοδοξεί να λύσει τα προβλήματα διασύνδεσης μεταξύ των υπηρεσιών που υπήρχαν στο παρελθόν λόγω του πλήθους διαφορετικών δικτύων. Το Βέλγιο ανέπτυξε την υπηρεσία Blue Light που ουσιαστικά αξιοποιεί και τα τρία ραδιοδίκτυα των MNOs.Με μια ειδική SIM κάρτα τα μέλη των υπηρεσιών ασφαλείας αποκτούν πρόσβαση και στα τρία δίκτυα εξασφαλίζοντας την καλύτερη δυνατή ευρυζωνική σύνδεση ανάλογα με την περιοχή στην οποία επιχειρούν. Με αυτό τον τρόπο κράτησε παράλληλα και το προηγούμενο TETRA δίκτυο το οποίο θα αντικατασταθεί λίγο πριν το 2030.

γ. Αποκλειστικό Δίκτυο δημόσιας ασφάλειας**.** Μια αντίθετη από τις Η.Π.Α διαδρομή ακολούθησε η Νότια Κορέα στο δικό της μοντέλο. Το υπουργείο εσωτερικών αποφάσισε να κατασκευάσει ένα αποκλειστικό δίκτυο δημόσιας ασφαλείας αναθέτοντας την κατασκευή του σε δυο Κορεατικές εταιρείες τηλεπικοινωνιών. Το σκεπτικό ήταν εντελώς διαφορετικό από αυτό των Η.Π.Α, ο στόχος ήταν η Νότια Κορέα να πρωταγωνιστήσει στο συγκεκριμένο τομέα, αναπτύσσοντας τη δική της τεχνολογία και βιομηχανία και αυξάνοντας παράλληλα τις θέσεις εργασίας στο εσωτερικό της. Τα οικονομικά δεδομένα των εξαγωγών στον τηλεπικοινωνιακό κλάδο αποτέλεσαν σημαντικά επιχειρήματα για την επιτυχία του συγκεκριμένου μοντέλου. Σήμερα η Ν. Κορέα είναι πρωτοπόρα στον τομέα αυτό και η φιλοσοφία της είναι να μοιραστεί τις γνώσεις της σε διεθνές επίπεδο με χώρες που επιθυμούν να αναπτύξουν τα δικά τους εθνικά δίκτυα ασφαλείας. Το ποσό που επένδυσε η κυβέρνηση για την κατασκευή του Safe-Net ήταν στα 1.5δις δολάρια.

3. Η διαδικασία μετάβασης προς το 5G θα διαρκέσει έως το 2028, είναι ιδιαίτερα πολύπλοκη και απαιτεί εξαιρετική προετοιμασία για τις χώρες που θα το επιλέξουν. Χαρακτηριστικό παράδειγμα η Αυστραλία που έχει θέσει πολύ υψηλούς στόχους για την ανάπτυξη του δικτύου έχοντας ήδη προγραμματίσει την ολοκλήρωση της μετάβασης στο 5G στην επόμενη 5ετία.

4. Χώρες όπως το Ηνωμένο Βασίλειο και η Γαλλία διέθεταν αξιόπιστα συστήματα επικοινωνίας κρίσιμων επικοινωνιών, με τα οποία οι χρήστες ήταν σε μεγάλο βαθμό ικανοποιημένοι. Η μετάβαση στο LTE που θα εξασφάλιζε την ευρυζωνικότητα έπρεπε πρώτα να περάσει από αρκετά στάδια ωρίμανσης ώστε να εξασφαλίσει αντίστοιχης ποιότητας MCX υπηρεσίες με τα υπάρχοντα δίκτυα. Αυτό το γεγονός οδήγησε σε καθυστερήσεις και υπερβάσεις του προϋπολογισμού του έργου σε αρκετά σημεία και στις δυο χώρες.
5. Η ανάπτυξη κουλτούρας συνεργασίας σε διακρατικό επίπεδο και ειδικότερα η συμμετοχή σε διεθνείς φορείς και ενώσεις με στόχο την ανταλλαγή τεχνογνωσίας , την συμφωνία σε θέματα προτυποποίησης αποτελούν προϋπόθεση για την μεσοπρόθεσμη μείωση του κόστους κατασκευής, συντήρησης, επέκτασης αλλά και αναβάθμισης των PSN.
6. Τέλος η αύξηση του ρυθμού διάδοσης του 5G έχει άμεσο αντίκτυπο στη μείωση του κόστους του UE. Γεγονός που μπορεί να λειτουργήσει θετικά σε εθελοντικούς οργανισμούς πρώτων ανταποκριτών όπου μέλη αυτών, χρησιμοποιούν τη δική τους συσκευή στο πεδίο, και υπό προϋποθέσεις μπορούν και αυτά, να αποκτήσουν πρόσβαση σε MCX υπηρεσίες.

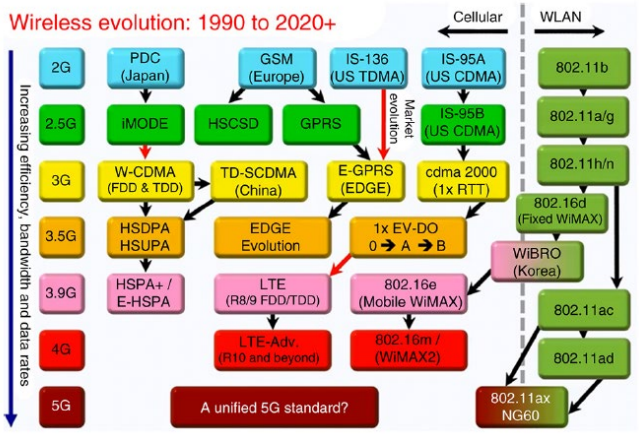
Σε αυτή την ενότητα παρουσιάσαμε τα συμπεράσματα από τις συγκρίσεις ανάμεσα σε έξι χώρες με πολύ διαφορετικές προσεγγίσεις και χαρακτηριστικά. Η επιλογή αυτών των χωρών έγινε διότι μέσα από αυτές τις μελέτες περίπτωσης μπορέσαμε να αντλήσουμε συγκεκριμένες βέλτιστες πρακτικές με δυνατότητα εφαρμογής τους στη χώρα μας.

6.3 Σπουδαιότητα της προτυποποίησης

Στην παρούσα εργασία έχουν γίνει πλείστες αναφορές σε τεχνολογικά πρότυπα και κανονισμούς. Από έρευνες, έχει προκύψει η καθολική επιρροή του παγκόσμιου εμπορίου από τα πρότυπα, που σε κάποιες περιπτώσεις ξεπερνάει το 90% [465]. Οι προσπάθειες προτυποποίησης που αφορούν στα ασύρματα δίκτυα επικοινωνιών αποτελούν χαρακτηριστικό παράδειγμα της σημαντικότητας, αλλά και της συμβολής της στην εξέλιξη της τεχνολογίας και μια εποπτική αποτύπωσή τους παρουσιάζεται στην Εικόνα 187, παράλληλα με τις εξελίξεις, οι οποίες επιτεύχθηκαν προϊόντος του χρόνου (αποδοτικότητα, εύρος ζώνης και ρυθμός μετάδοσης δεδομένων) [51]. Ο λόγος για το έργο προτυποποίησης της δημόσιας ασφάλειας είναι απλός και αφορά στο γεγονός ότι οι χρήστες αυτής έχουν ανάγκες επικοινωνίας που δεν καλύπτονται από πρότυπα που έχουν καθοριστεί για χρήση από τους καταναλωτές [466].

Ο στόχος της αυτοτελούς αναφορά στην αξία της προτυποποίησης για τα δίκτυα δημόσιας ασφάλεια στο σημείο αυτό δεν είναι η ανάδειξη των επι μέρους προτύπων, η οποία σε κάθε περίπτωση αναφέρεται στο σύνολο της εργασίας, αλλά να υπερτονίσει τα οφέλη από αυτή. Τα παγκόσμια πρότυπα και τα μέτρα συμμόρφωσης που διασφαλίζουν την αποτελεσματική χρήση τους συμβάλλουν [465]:

- Διαλειτουργικότητα συσκευών και πλατφορμών επικοινωνίας
- Μειωμένο κόστος απόκτησης και βελτίωση της ανταγωνιστικότητας της αγοράς
- Επεκτασιμότητα της υποδομής και δυνατότητα ευκολότερης και ταχύτερης ανάπτυξης
- Βελτιωμένη διαχείριση υποδομής, απλοποιημένη και συλλογή λήψη αποφάσεων
- Αποτελεσματική επικοινωνία και επίλυση θεμάτων



Εικόνα 187. Το δένδρο της προτυποποίησης (ασύρματες επικοινωνίες 1990 - 2020) [51]

Χώρα	Νότια Κορέα	Η.Π.Α	Φινλανδία	Γαλλία	Ηνωμένο Βασίλειο	Βέλγιο	Αυστραλία
Δίκτυο	SafeNet PS-LTE, LTE-R, LTE-M	FirstNet	VIRVE 2.0	Réseau Radio du Futur (RRF)	Emergency Services Network (ESN)	-	NSW Telco Authority
Λόγοι Μετάβασης	Πλήθος δικτύων, Έλλειψη διασύνδεσης των Υπηρεσιών	Έλλειψη διασύνδεσης των Υπηρεσιών	Έλλειψη ευρυζωνικότητας	Έλλειψη Διαλειτουργικότητας και ευρυζωνικότητας	Πλήθος δικτύων, Έλλειψη διασύνδεσης των Υπηρεσιών	Έλλειψη ευρυζωνικότητας	Έλλειψη Διαλειτουργικότητας και ευρυζωνικότητας
Διαχειριστής δικτύου	Υπουργεία: Εσωτερικών, Ωκεανών και Αλιείας, Γης, Υποδομών και Μεταφορών	AT&T	Erillisverkot Group	Υπουργείο Εσωτερικών	Υπουργείο Εσωτερικών	Astrid	NSW Telco Authority
MNO	Korea Telecom, SK Telecom	AT&T	Elisa	Orange, Bouygues Telecom	EE	Proximus, Orange, BASE	NSW Telco Authority
Φάσμα	B28 2 x 10 MHz	B14 2 x 10 MHz	Μη καθορισμένη ζώνη συχνοτήτων	B28 2 x 3 MHz B68 2 x 5 MHz	Αέρος-Εδάφους B40 5 MHz	Μη καθορισμένη ζώνη συχνοτήτων	Μη καθορισμένη ζώνη συχνοτήτων
Κύριοι	Samsung	AT&T,	Ericsson	Airbus,	Motorola	Μ/Δ	Μ/Δ

Προμηθευτές τηλεπικοινωνιακού Υλικού		Motorola Solutions		Capgemini,ATOS,	Solutions, Samsung		
Χρήστες	285.000	3,5 εκ.	51.000	300.000	300.000	> 70.000	53.000
Γεωγραφική Κάλυψη Δικτύου	100%	28,6%	97% (2024)	Μ/Δ	99%	99,9%	44,5% (2022)
Πληθυσμιακή κάλυψη Δικτύου	100%	99%	99,98% (2024)	Μ/Δ	99%	99,9%	97% (2022)
4G	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι
5G	Ναι (2020 - 2027)	Ναι	Ναι (2023 - 2025)	Ναι (2024 - 2025)	Όχι	Δοκιμαστικό Στάδιο	Όχι (2028)
Αριθμός Σταθμών Βάσης	17.000	100,000	1400	Μ/Δ	19.500	Μ/Δ	675 (Ολοκλήρωση)
Επιχειρηματικό Μοντέλο - Χρηματοδοότηση	Κρατική	Κρατική και Σύμπραξη με Ιδιώτες	Κρατική	Κρατική	Κρατική	Κρατική	Κρατική
Τύπος Δικτύου	Αποκλειστικό	Κοινόχρηστο	Κοινόχρηστο	Κοινόχρηστο	Κοινόχρηστο	Κοινόχρηστο	Κοινόχρηστο
Έναρξης Λειτουργίας	2020	2012	2019	2024	2018 (σε εξέλιξη)	2011	2028 (5G)
Εκτιμώμενο Συνολικό κόστος Επένδυσης	1.5 billion(USD)	100 billion (USD)	1.2 billion (USD)	> 684 million (USD)	9.3 billion (GBP)	Μ/Δ	1.4 Billion (AUD)

Πίνακας 32. Χαρακτηριστικά των δικτύων δημόσιας ασφάλειας των χωρών: Νότιας Κορέας, Η.Π.Α., Φιλανδίας, Γαλλίας, Ηνωμένου Βασιλειου, Βελγίου και Αυστραλίας

7 *Επίλογος*

Η κοινότητα δημόσιας ασφάλειας έχει κάνει σημαντικά βήματα προς την ενίσχυση της ετοιμότητας και τη βελτίωση των δυνατοτήτων επικοινωνίας έκτακτης ανάγκης. Οι πρώτοι ανταποκριτές ωστόσο, εξακολουθούν να περιορίζονται από κατακερματισμένα δίκτυα και παρωχημένες τεχνολογίες. Η ανάπτυξη ενός οικονομικά αποδοτικού ασύρματου ευρυζωνικού δικτύου δημόσιας ασφάλειας θα παρέχει στους φορείς πρόσβαση προηγμένες υπηρεσίες, τεχνολογίες αιχμής και εφαρμογές που θα συνεισφέρουν σημαντικά στη βελτίωση της ανταπόκρισής τους στο πεδίο που επιχειρούν. Η μετάβαση αυτή από το LMR στην ευρυζωνική σύνδεση απαιτεί κατάλληλο συντονισμό και τη συνεργασία όλων των φορέων, κρατικών υπηρεσιών, οργανισμών, εταιριών και επιστημονικής κοινότητας, ώστε να αναπτυχθούν τα κατάλληλα πρότυπα και τεχνολογικές λύσεις που θα διασφαλίσουν τις απαιτήσεις των κρίσιμων επικοινωνιών [467].

Το πρώτο βήμα έγινε με τις εμπορικές αναπτύξεις ασύρματων υπηρεσιών LTE και τις λύσεις που η συγκεκριμένη τεχνολογία και το μεταγενέστερο 4G παρέχουν στα δίκτυα δημόσιας ασφάλειας. Η πορεία είναι αργή και απαιτεί κάθε στοιχείο που προσαρτάται και προσδιορίζεται ως λύση να έχει δοκιμαστεί σε ακραίες συνθήκες, με θετικά αποτελέσματα. Σε κάθε περίπτωση ο στόχος είναι η επιθυμητή σύγκλιση, από την τωρινή κατάσταση σε πρότυπα και λύσεις κοινά αποδεκτές, εφαρμόσιμες και αποδοτικές.

Το 2023 και τα επόμενα δύο χρόνια θα είναι μια περίοδος βαριάς ανάπτυξης του 5G, μετασχηματισμού στα άκρα και αυξημένης διασύνδεσης τεχνολογιών και συστημάτων δικτύου [468]. Ο ίδιος οδικός χάρτης της IEEE INGR μετάβασης από το 2022 στο 2032 επισημαίνει τις τάσεις, τις προκλήσεις και τις λύσεις στο τρέχον και βραχυπρόθεσμο τοπίο του δικτύου κινητής τηλεφωνίας και το μελλοντικό όραμα που καλλιεργείται μέσω των δραστηριοτήτων των Οργανισμών Ανάπτυξης Προτύπων (SDOs) σε όλο τον κόσμο. Συγκεκριμένα εστιάζει στους τομείς των δορυφορικών επικοινωνιών, της τεχνητής νοημοσύνης, της μηχανικής μάθησης, αλλά και το μείζον ζήτημα της ενεργειακής απόδοσης.

Η τεχνολογία των δικτύων 5G που αποτελούν σήμερα την ξεκάθαρη τάση, αποτέλεσαν αντικείμενο της έρευνας το 2020, ενώ το 2021 και το 2022 η στόχευση αφορούσε στη δημιουργία ενός διεπιστημονικού πλαισίου και ενός προγνωστικού μοντέλου για δίκτυα κινητής τηλεφωνίας. Τη συγκεκριμένη εξελικτική πορεία ακολουθούν πιστά και τα δίκτυα δημόσιας ασφάλειας, με δεδομένο μάλιστα ότι οι τεχνολογικές λύσεις που εφαρμόζονται στα δίκτυα κινητής τηλεφωνίας αποτελούν ένα έτοιμο εργαλείο για την υλοποίηση των PSNs.

Ευρισκόμενοι σ` αυτή τη χρονική συγκυρία, γίνεται σαφές ότι η κοινότητα της δημόσιας ασφάλειας έχει φτάσει στο κρίσιμο σημείο των αποφάσεων που θα ορίσουν τις μελλοντικές εξελίξεις που την αφορούν. Θα καταφέρουν οι φορείς της δημόσιας ασφάλειας να επωφεληθούν των ραγδαίων τεχνολογικών εξελίξεων και να καρπωθούν λύσεις που θα τους βελτιώσουν αισθητά τις επικοινωνίες στο πεδίο και σε όλες τις συνθήκες που καλούνται να αντιμετωπίσουν; Η απάντηση στο ερώτημα αυτό δεν αφορά μόνο στις δυνατότητες που παρέχει η τεχνολογία, καθώς ζητήματα πολιτικής βούλησης, δεκτικότητας στην καινοτομία, οικονομικά και διοικητικά καθορίζουν σημαντικά τις εξελίξεις.

Ωστόσο, η τεχνολογία είναι αυτή που θα πρέπει να δείξει τον ξεκάθαρο δρόμο, ώστε διατηρώντας τα κεκτημένα και κρατώντας από αυτά τις βέλτιστες πρακτικές, να μπορέσουμε να μεταβούμε στην επόμενη εποχή δικτύων δημόσιας ασφάλειας που συμβαδίζει με τις τεχνολογικές δυνατότητες των εμπορικών δικτύων. Καθίσταται οξύμωρο ο επαγγελματίας της δημόσιας ασφάλειας να χρησιμοποιεί στην καθημερινότητά του μια πληθώρα χρηστικών εφαρμογών που του βελτιώνουν τις συνθήκες διαβίωσης σε όλους τους τομείς και από την άλλη να μην είναι σε θέση να αξιοποιήσει αυτές τις δυνατότητες και υπηρεσίες όταν τις χρειάζεται περισσότερο, δηλαδή στην καθημερινή υπηρεσιακή του καθημερινότητα τόσο επ ωφελεία της δικής του ασφάλειας, όσο και των πολιτών. Το ίδιο οξύμωρο άλλωστε φαντάζει σε ένα τεχνολογικό μέλλον να εμπιστευόμαστε την τεχνολογία για απομακρυσμένη χειρουργική, αλλά όχι για τις κρίσιμες επικοινωνίες.

7.1 Σύνοψη και συμπεράσματα

Είναι γεγονός ότι οι κατασκευαστές του υλικού που προορίζεται για τα δίκτυα δημόσιας ασφάλειας και τις PMR δεν μπορούν να αντέξουν δαπάνες δισεκατομμυρίων ευρώ για έρευνα και ανάπτυξη τεχνολογιών επόμενης γενιάς. Η αγορά της δημόσιας ασφάλειας είναι μικρή και γίνεται ακόμη μικρότερη όταν αναζητά λύσεις ούσα κατακερματισμένη. Είναι χαρακτηριστικός δε ο παραλληλισμός οικονομικών μεγεθών που ανέφεραν οι [286], καθώς υποστήριξαν ότι εάν τη δεδομένη χρονική στιγμή (22-11-2011) ένας εμπορικός κατασκευαστής πουλούσε 40 εκατομμύρια κινητά σε διάστημα ενός τριμήνου, όσα δηλαδή

κατ` εκτίμηση ήταν σε παγκόσμιο επίπεδο συνολικά τα τερματικά δημόσιας ασφάλειας τότε, θα έπρεπε να υποβαθμιστεί από διεθνείς οίκους αξιολόγησης. Είναι τέτοια η διαφορά οικονομικών μεγεθών, ακόμη και σήμερα, που η όποια βελτίωση των επικοινωνιών δημόσιας ασφάλειας θα επιτευχθεί μέσα από δύο βασικούς πυλώνες. Την αποδοτική αξιοποίηση της τεχνολογίας και τη δημιουργία κουλτούρας συνεργασίας, τόσο σε επίπεδο κρατών, όσο και οργανισμών ή φορέων.

Για αυτό το μικρό εμπορικά, αλλά πολύ σημαντικό λειτουργικά κομμάτι της κοινωνίας μας, που υποστηρίζει τη διατήρηση της συνέχειας και συνοχής της, την ασφάλειά της και παρέχει αξιόλογες υπηρεσίες στους πολίτες, αξίζει να προσφέρουμε το καλύτερο τεχνολογικό κομμάτι. Για τον λόγο αυτό έγινε μια εκτεταμένη έρευνα και μελέτη των προτύπων επικοινωνίας δημόσιας ασφάλειας, μέσα από τη διαδρομή των τριάντα και πλέον ετών, δηλαδή από τη δεκαετία του 1990 έως και τις μέρες μας. Η αναλυτική μελέτη, ακόμη και των αρχικών προτύπων ήταν εσκεμμένη και πλήρως αιτιολογημένη, εάν συνυπολογίσουμε ότι ακόμη και σήμερα τα συγκεκριμένα πρότυπα βρίσκονται στην καθημερινότητα των πρώτων ανταποκριτών και υποστηρίζουν αυτούς στα καθήκοντά τους. Τα TETRA, P25, TETRAPOL, DMR και άλλα πρότυπα στενής ζώνης έχουν εξελιχθεί και πρωταγωνιστούν και σήμερα, κατά περίπτωση, προσπαθώντας να καλύψουν τις ανάγκες σε πολυμεσική επικοινωνία. Επιπλέον, κάποιες από τις εταιρίες και φορείς έχουν σχεδιάσει και υπολογίσει στη μετεξέλιξή τους και βελτίωσή τους, ώστε να καλύψουν τις αυξημένες πλέον απαιτήσεις των πρώτων ανταποκριτών τους.

Όλες αυτές οι εξελίξεις, την ίδια στιγμή που επιχειρείται η μετάβαση στην ευρυζωνικότητα, η οποία πατά πλέον στις σταθερές που έχει δημιουργήσει το LTE, κάποιες πολύ αξιόλογες εφαρμογές, οι οποίες μάλιστα συνοδεύονται από αντίστοιχες συσκευές και υποστηρίζονται επαρκώς από τα δίκτυα 4G και φιλοδοξεί να μεταβεί σε ένα υψηλότερο τεχνολογικό επίπεδο και να επιτύχει βέλτιστο επίπεδο ανταπόκρισης στο έδαφος του 5G. Παράλληλα, αναπτύξαμε λύσεις υποστήριξης των δικτύων αυτών για αντιμετώπιση ακραίων καταστάσεων και εξαιρετικά αφιλόξενα περιβάλλοντα, που δημιουργούν ανθρωπογενείς ή φυσικές καταστροφές, αλλά και τρομοκρατικές επιθέσεις, όπου αντιμετωπίζουμε απόλυτη ή μερική καταστροφή της υποδομής του δικτύου και των στοιχείων αυτής με ανάπτυξη εναλλακτικών κινητών συσκευών που προσαρμόζονται σε οχήματα, σε UAVs, σε κάθε άλλους κατασκευή που δύναται να προσεγγίσει έγκαιρα και με ασφάλεια την επίμαχη περιοχή, ή με κατάλληλη δορυφορική σύνδεση.

Παράλληλα, έγινε μια εποπτική αποτύπωση των οργανισμών, ενώσεων και πρωτοβουλιών που σχετίζονται με τη δημόσια ασφάλεια και μια προσεκτική αναφορά σε επιλεγμένες εταιρίες που οδηγούν τις εξελίξεις. Ταυτόχρονα, αναφερθήκαμε σε αξιόλογα έργα της επιστημονικής κοινότητας που εμφανίζουν σημαντικές προοπτικές, είτε για αυτοτελή

αξιοποίηση, είτε επειδή αντιμετωπίζουν αποδοτικά κάποιες από τις προκλήσεις της δημόσιας ασφάλειας.

Τέλος, καταγράψαμε, μελετήσαμε και συγκρίναμε τις πρακτικές που εφαρμόζει κάθε χώρα στο ζήτημα των δικτύων δημόσιας ασφάλειας και κρίσιμων επικοινωνιών. Ουσιαστικά χαρακτηριστικά παραδείγματα αυτών, από τα οποία συνάγονται ενδιαφέρουσες προσεγγίσεις και λύσεις που δοκιμάζονται καθημερινά στο πεδίο. Αναφερθήκαμε αναλυτικά σε περιπτώσεις χωρών που έχουν υλοποιήσει προγράμματα, για τα οποία πολλές εταιρίες του χώρου έχουν επιδείξει ιδιαίτερο ενδιαφέρον στην κατασκευή συσκευών για τους πρώτους ανταποκριτές και αντίστοιχης υποδομής για υποστήριξη των κέντρων διοίκησης και ελέγχου. Οι λύσεις που συναντούμε σε προηγμένες χώρες και οι οποίες ανταποκρίνονται αποδοτικά σε συμβάντα σεισμών, πλημμυρών, τυφώνων, μεγάλων καταστροφικών ή εγκληματικών γεγονότων, είναι λύσεις που με κατάλληλη τεχνολογική προσαρμογή και βούληση μπορούν να υποστηρίξουν και τις υπηρεσίες της χώρας μας. Μάλιστα, βρισκόμαστε στην κατάλληλη χρονική συγκυρία και οι συνθήκες είναι ώριμες, καθώς μόλις στο πρόσφατο παρελθόν έχουν απασχολήσει τη χώρα μας ακραία καταστροφικά γεγονότα, είτε με ανθρώπινα θύματα, είτε με ανυπολόγιστες υλικές ζημιές και καταστροφικές επιπτώσεις για το φυσικό πλούτο, ώστε να καταφύγουμε σε μια φιλόδοξη προσέγγιση και να σχεδιάσουμε τα δίκτυα δημόσιας ασφάλειας της χώρας μας με προοπτική δεκαετίας, παρέχοντας ιδανικά την απαιτούμενη διασύνδεση με το προσωπικό της Πολιτικής Προστασίας.

7.2 Μελλοντικές επεκτάσεις

Στην παρούσα εργασία έγινε μια βιβλιογραφική επισκόπηση των τεχνολογιών επικοινωνίας που εμπλέκονται στην υλοποίηση δικτύων δημόσιας ασφάλειας. Επιπλέον, μια μελέτη και περιγραφή των τάσεων της κοινότητας της δημόσιας ασφάλειας μέσα από την παρουσίαση των έργων που έχουν ολοκληρωθεί, ή είναι σε επίπεδο δοκιμών για την επικείμενη ένταξή τους στη διάθεση των επαγγελματιών της. Οι λύσεις είναι πολλές και σε κάποιες περιπτώσεις σημαντικά διαφορετικές. Κάθε μία εξ αυτών προσπαθεί να προσεγγίσει με βέλτιστο τρόπο ένα κενό ή κάποια δυσλειτουργία που εντόπισε στις υπάρχουσες και να συνεισφέρει στην εκπλήρωση κάποιων τεχνικών προδιαγραφών και απαιτήσεων. Τα πρότυπα είναι σύμμαχος της προσπάθειας αυτής, καθώς δημιουργούν ένα στέρεο τεχνολογικό περιβάλλον και την απαιτούμενη σταθερότητα για την περαιτέρω ανάπτυξη.

Ωστόσο, τα κενά και οι προβληματικές περιοχές που δημιουργούν τεχνολογικές προκλήσεις είναι ακόμη αρκετές. Για ν` αντιμετωπιστούν απαιτείται συνεργασία και αξιοποίηση των τεχνολογικών επιτευγμάτων στον τομέα των ασύρματων δικτύων επικοινωνίας, καθώς και

των υπολοίπων τεχνολογιών που μπορούν να συνδράμουν συμπληρωματικά και να βελτιώσουν τις εφαρμογές και υπηρεσίες. Παράλληλα, οι λύσεις αυτές θα πρέπει να είναι συμβατές με τις επικοινωνίες LMR, για μια πληθώρα λόγων, αλλά κύρια για να διασφαλίζεται η επιχειρησιακή συνέχεια καθώς η ταχύτητα ανάπτυξης των προηγμένων δικτύων είναι διαφορετική από χώρα σε χώρα.

Από την επισκόπηση που πραγματοποιήθηκε προέκυψε ότι μια αποδοτική λύση αποτελεί η υβριδική αρχιτεκτονική ενός δικτύου δημόσιας ασφάλειας, που υποστηρίζεται από ευρυζωνικές επικοινωνίες 5G και διαλειτουργεί με τα υπάρχοντα συστήματα, ώστε να καθίσταται συμβατό με τις λύσεις που έχουν αναπτυχθεί και εξυπηρετούν κάθε χώρα. Παράλληλα, η αρχιτεκτονική αυτή θα υποστηρίζεται στο πεδίο με υποδομή σε οχήματα, σε UAVs, ή δορυφορικά, για τις περιπτώσεις καταστροφής της υπάρχουσας.

Κάποιες από τις επεκτάσεις αυτής της εργασίας θα μπορούσαν να είναι:
α. Η εξαγωγή των αποτελεσμάτων της έρευνας, η οποία ξεκίνησε και δεν ολοκληρώθηκε, η εκτίμηση αυτών, παρά το γεγονός ότι θα λείπουν τα δεδομένα από την Ελληνική Αστυνομία και η αξιοποίησή τους σε μια πρόταση αρχιτεκτονικής για τα δίκτυα δημόσιας ασφάλειας που αφορά στη χώρα μας. Σ` αυτή την επέκταση θα μπορούσε να υπάρξει μια πλήρως κοστολογημένη πρόταση με στόχο να εισάγει την καινοτομία του 5G και ένα συγκεκριμένο αρχιτεκτονικό μοντέλο δικτύου που θα κάλυπτε το σύνολο της επικράτειας, το οποίο για να είναι ρεαλιστικό θα ήταν ωφέλιμο να ενταχθεί σε συγκεκριμένο Ευρωπαϊκό πρόγραμμα επιδότησης στο πλαίσιο των αντίστοιχων προγραμμάτων για την καινοτομία και τις ΤΠΕ της περιόδου 2021-2027.
β. Παραλλαγή αυτής της πρότασης θα μπορούσε να αποτελεί το μοντέλο που εφάρμοσε και λειτουργεί το Βέλγιο, όπου οι πρώτοι ανταποκριτές έχουν πρόσβαση στο δίκτυο κρίσιμων επικοινωνιών με τη χρήση κάρτας SIM σε συγκεκριμένες συσκευές και προκαθορισμένη εφαρμογή, διαμέσου της οποίας είναι εφικτή η απόλυτη διαλειτουργικότητα και επικοινωνία μεταξύ τους. Σ` αυτή την περίπτωση δε, θα μπορούσαν να προταθούν λύσεις συνεργασίας του δημοσίου τομέα με κάποιες εταιρείες, ή τηλεπικοινωνιακούς παρόχους, με όφελος για αμφότερες τις πλευρές, στη λογική που λειτουργεί το FirstNet στις Η.Π.Α..
γ. Η προγραμματιστική ανάπτυξη εφαρμογής και συγκεκριμένα πλατφόρμας μέσω ενός ενδοδικτύου (intranet) και θα υποστηριζόταν από το σύνολο των παρόχων δικτύων κινητής τηλεφωνίας που λειτουργούν στη χώρα μας, για κάλυψη σε όλο το διαθέσιμο εύρος κάλυψης από αυτούς και η οποία θα παρείχε τη δυνατότητα πιστοποιημένης εισόδου του συνόλου των πρώτων ανταποκριτών των αναφερόμενων Υπηρεσιών (Αστυνομία, Πυροσβεστική, Λιμενικό, ΕΚΑΒ) αλλά και του προσωπικού της Πολιτικής Προστασίας, με στόχο να παρέχει σ` αυτούς μια κοινή επιχειρησιακή εικόνα, αλλά και την απαιτούμενη αυτοτέλεια για εύκολο και γρήγορο συντονισμό των ενεργειών τους. Μάλιστα, η συγκεκριμένη πλατφόρμα θα

μπορούσε να καταστεί συμβατή με τις αντίστοιχες ηλεκτρονικές υπηρεσίες που έχουν αναπτυχθεί και λειτουργούν ήδη σε κάθε μια από τις Υπηρεσίες αυτές και να λειτουργήσει ως συνδετικός κρίκος, που θα ενεργοποιείται σε συγκεκριμένες περιπτώσεις αντιμετώπισης έκτακτων καταστάσεων.

Άλλωστε, η αυτοτέλεια των ενεργειών των υπηρεσιών είναι τόσο επιθυμητή, όσο και η κρίσιμη δυνατότητα να επικοινωνούν μεταξύ τους, όποτε και όπου απαιτείται, χωρίς να παρατηρούνται καθυστερήσεις και δυσλειτουργίες που αποβαίνουν σε βάρος των παρεχόμενων υπηρεσιών. Είναι γεγονός δε, ότι το καλύτερο πράγμα με τη διαλειτουργικότητα είναι ότι όλοι μπορούν να μιλούν με όλους, ενώ το χειρότερο χαρακτηριστικό της είναι ότι όλοι μπορούν να μιλούν με όλους.-

Βιβλιογραφία

[1] Γ. Μπαμπινιώτης, Λεξικό της Νέας Ελληνικής Γλώσσας, Αθήνα: Κέντρο Λεξικολογίας, 2005.

[2] A. H. Maslow, «A Theory of Human Motivation,» *Psychological Review,* p. 370–396, 1943.

[3] S. M. McLeod, «Maslow's Hierarchy of Needs,» *Simply Phsychology,* 2007.

[4] Τ. Καρατραντος, «kathimerini.gr,» 15 Αύγουστος 2021. [Ηλεκτρονικό]. Available: https://www.kathimerini.gr/opinion/561466438/i-epochi-ton-proton-antapokriton/. [Πρόσβαση Νοέμβριος 2022].

[5] Θ. Παπαθεοδώρου, Δημόσια ασφάλεια και Αντεγκληματική πολιτική. Συγκριτική προσέγγιση, Αθήνα: Νομική Βιβλιοθήκη, 2005.

[6] Α. Κωστάρας, Έννοιες και θεσμοί του ποινικού δικαίου, Αθήνα: Σάκκουλας, 2004.

[7] Ε. Λέκκας, Φυσικές και Τεχνολογικές καταστροφές, Αθήνα: Access PrePress, 2000.

[8] Κέντρο Μελετών Ασφαλείας (ΚΕ.ΜΕ.Α.), «ΕΚΠΑΙΔΕΥΣΕΙΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΥΠΟΔΟΜΩΝ ΖΩΤΙΚΗΣ ΣΗΜΑΣΙΑΣ - ΕΓΧΕΙΡΙΔΙΟ,» Ταμείο Εσωτερικής Ασφάλειας (ΕΕ), Αθήνα, 2018.

[9] United Nations Office for Disaster Risk Reduction, «Global Assessment Report on Disaster Risk Reduction 2022 (GAR2022),» 2022. [Ηλεκτρονικό]. Available: https://www.undrr.org/publication/global-assessment-report-disaster-risk-reduction-2022. [Πρόσβαση Οκτώβριος 2022].

[10] FirstNet Authority , «First Responder Network Authority Roadmap,» FirstNet Authority , 2020.

[11] United Nations Office for Disaster Risk Reduction, «UNDRR - UNISDR terminology on disaster risk reduction,» 2009. [Ηλεκτρονικό]. Available: https://www.undrr.org/publication/2009-unisdr-terminology-disaster-risk-reduction. [Πρόσβαση Οκτώβριος 2022].

[12] «Emergency Events Database (EM-DAT),» [Ηλεκτρονικό]. Available: https://www.emdat.be/.

[Πρόσβαση Οκτώβριος 2022].

[13] «Centre for Research on the Epidemiology of Disasters (CRED),» [Ηλεκτρονικό]. Available: https://www.cred.be/. [Πρόσβαση Οκτώβριος 2022].

[14] Centre for Research on the Epidemiology of Disasters - UNDRR, «Human cost of disasters - An overview of the last twenty years 2000 - 2019,» UNDRR - USAID - UCLouvain, Brussels - Geneva, 2019.

[15] Βικιπαίδεια ή Wikipedia, «Σεισμός Τουρκίας-Συρίας (2023),» Βικιπαίδεια ή Wikipedia, [Ηλεκτρονικό]. Available: https://el.wikipedia.org/wiki/Σεισμός_Τουρκίας-Συρίας_(2023). [Πρόσβαση 17 Φεβρουάριος 2023].

[16] UCLouvain, «Natural Hazards & Disasters - An overview of the first half of 2022,» Centre for Research on the Epidemiology of Disaster CRED, Brussels, 2022.

[17] UCLouvain, «Disasters1 Year in Review 2021,» Centre for Research on the Epidemiology of Disaster CRED, Brussels, 2022.

[18] H. Srinivas, «Environmental Vulnerability and Disaster Risk Reduction,» GLOBAL DEVELOPMENT RESEARCH CENTER, Kobe, Japan, 2022.

[19] Ε. Λεκκας, Ε. Ανδρεαδακης, Ε. Καπουρανη, Δ. Μινου - Μινοπουλου και Δεσποινα, «ΠΡΟΛΗΨΗ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΦΥΣΙΚΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΩΝ ΚΑΤΑΣΤΡΟΦΩΝ,» σε *ΠΡΟΓΡΑΜΜΑ ΣΥΜΠΛΗΡΩΜΑΤΙΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ ΕΞ' ΑΠΟΣΤΑΣΕΩΣ (E-LEARNING) ΤΟΥ ΕΚΠΑ*, 2007.

[20] «ethnos.gr,» 11 Μάρτιος 2022. [Ηλεκτρονικό]. Available: https://www.ethnos.gr/todayinhistory/article/198691/seismossthniaponiaxiliadesnekroiapotsoynamikaipyrhnikoatyxhmasthfoykoysima. [Πρόσβαση 2022].

[21] Κ. Σαπουντζακη και Μ. Δανδουλακη, Κίνδυνοι και καταστροφές, Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαικών Βιβλιοθηκών - Εθνικό Μετσόβιο Πολυτεχνείο, 2015.

[22] «Center for Disaster Philanthropy,» 2010. [Ηλεκτρονικό]. Available: https://disasterphilanthropy.org. [Πρόσβαση November 2022].

[23] Θ. Ντοκος, «Policy Paper - Προκλήσεις Εσωτερικής Ασφάλειας: Η αμάγκη μεταρρύθμισης του μηχαμισμού διαχείρισης εκτάκτωμ καταστάσεωμ,» Ελληνικό Ίδρυμα Ευρωπαϊκής και Εξωτερικής Πολιτικής (ΕΛΙΑΜΕΠ), Αθήνα, 2011.

[24] Θ. Ντοκος, «Ασύμμετρες Απειλές και Διεθνής Ασφάλεια,» σε *ΔΙΕΘΝΕΙΣ ΣΧΕΣΕΙΣ ΣΥΓΧΡΟΝΗ ΘΕΜΑΤΟΛΟΓΙΑ ΚΑΙ ΠΡΟΣΕΓΓΙΣΕΙΣ - ΑΦΙΕΡΩΜΑ ΣΤΟΝ ΘΕΟΔΩΡΟ ΚΟΥΛΟΥΜΠΗ*, Αθήνα, Παπαζήσης, 2008, p. 362.

[25] Κ. Αναγνωστόπουλος, «tovima.gr,» 22 Νοέμβριος 2008. [Ηλεκτρονικό]. Available:

https://www.tovima.gr/2008/11/24/opinions/o-seismos-poy-katedafise-ti-thriskolipsia/. [Πρόσβαση Νοέμβριος 2022].

[26] United Nations for Disaster Risk Reduction, United Nations for Disaster Risk Reduction, 28 May 2022. [Ηλεκτρονικό]. Available: https://www.preventionweb.net/news/seeds-wins-united-nations-sasakawa-award-2022-disaster-risk-reduction. [Πρόσβαση October 2022].

[27] International Decade for Natural Disaster Reduction, «Yokohama Strategy and Plan of Action for Safer World,» IDNDR, Yokohama, 1994.

[28] International Strategy for Disaster Reduction (LSDR), «Hyogo Framework for Action 2005-2015,» World Conference on Disaster Reduction , Kobe, Hyogo, 2005.

[29] United Nations Office for Disaster Risk Reduction (UNISDR) , «Sendai Framework for Disaster Risk Reduction 2015-2030,» United Nations Office for Disaster Risk Reduction (UNISDR), Sendai, 2015.

[30] United Nations Office for Disaster Risk Reduction (UNISDR), «UNISDR Strategic Framework 2016-2021,» United Nations Office for Disaster Risk Reduction (UNISDR), Geneva, 2016.

[31] United Nations for Disaster Risk Reduction (UNIDRR), «UNDRR STRATEGIC FRAMEWORK 2022 -2025,» United Nations for Disaster Risk Reduction (UNIDRR), Geneva, 2021.

[32] European Commission , «European Civil Protection and Humanitarian Aid Operations,» [Ηλεκτρονικό]. Available: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_en. [Πρόσβαση November 2022].

[33] European Union Law, «EUR-Lex,» 8 November 2007. [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32007D0779(01). [Πρόσβαση November 2022].

[34] European Commission , «COHESION OPEN DATA PLATFORM,» [Ηλεκτρονικό]. Available: https://cohesiondata.ec.europa.eu/themes/5/14-20. [Πρόσβαση 23 November 2022].

[35] A World Bank Group Flagship Report, «FINANCE FOR AN EQUITABLE RECOVERY - WORLD DEVELOPMENT REPORT 2022,» World Bank Group , Washington, 2022.

[36] Unated Nations s Development Programme, «New threats to human security in the Anthropocene - 2022 Special Report,» UNDP, New York, 2022.

[37] S. GHAFOOR, P. D. SUTTON, C. J. SREENAN και K. N. BROWN, «COGNITIVE RADIO FOR DISASTER RESPONSE NETWORKS: SURVEY, POTENTIAL, AND CHALLENGES,» *IEEE Wireless Communications,* October 2014.

[38] A. -. L. Muresan, E. Iafrate, A. Bonucci, M. Porfiri, M. Borgquist και M. Per, «Prioritised and Categorised Requirements Knowledgebase - Final - D3.3,» BroadMap - European Commission,

2018.

[39] Department of Homeland Security - USA, «Statement of requirements for Public Safety Wireless Communications and Interoperability,» Department of Homeland Security - USA, 2006.

[40] M. VOLK και J. STERLE, «5G Experimentation for Public Safety:Technologies, Facilities and Use Cases,» *IEEE Access,* pp. 41184 - 41217, 29 January 2021.

[41] G. Baldini, S. Karanasios, D. Allen και F. Vergari, «Survey of Wireless Communication Technologies for Public Safety,» *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* pp. 619 - 641, September 2013.

[42] C. Chung, D. Egan, A. Jain, N. Caruso, C. Misner και R. Wallace, «A Cloud-Based Mobile Computing Applications Platform for First Responders,» σε *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering*, Francisco, USA, 2013.

[43] A. Jarwan, A. Sabbah, M. Ibnkahla και O. Issa, «LTE-based Public Safety Networks: A Survey,» *IEEE Communications Surveys & Tutorials ·,* January 2019.

[44] K. Zeeshan, A. Ishtiaq και Q. D. Trung, Intelligent Unmanned Air Vehicles Communications for Public Safety Networks, Singapore: Springer, 2022.

[45] M. Roccetti, M. Gerla, C. E. Palazzi, S. Ferretti και G. Pau, «First Responders' Crystal Ball: How to Scry the Emergency from a Remote Vehicle,» σε *2007 IEEE International Performance, Computing, and Communications Conference*, Orleans, USA, 2007.

[46] Airbus Defence and Space, «The bridge to broadband,» Airbus , 2018.

[47] S. Dawkins, K. K. Greene και S. S. Prettyman, «Voices of First Responders—Nationwide Public Safety Communication Survey Findings: Mobile Devices, Applications, and Futuristic Technology Phase 2, Volume 2,» National Institude of Standards and Technology, 2020.

[48] A. Kumbhar και I. Guvenc, «A Comparative Study of Land Mobile Radio and LTE-based Public Safety Communications,» *ResearchGate,* 12 April 2015.

[49] Z. Kaleem, I. Ahmad και T. Q. Duong, Intelligent Unmanned Air Vehicles Communications for Public Safety Networks, Singapore: Springer, 2022.

[50] R. Shahzadi, M. Ali και M. Naeem, «UAV Placement and Resource Management in Public Safety Networks: An Overview,» σε *Intelligent Unmanned Air Vehicles Communications for Public Safety Networks*, Singapore, Springer, 2022, pp. 36-80.

[51] A. Yarali, Public Safety Networks from LTE to 5G, Murray: WILEY, 2020.

[52] F. PERVEZ, J. QADIR, M. KHALIL, T. YAQOOB, U. ASHRAF και S. YOUNIS, «Wireless Technologies for Emergency Response: A Comprehensive Review and Some,» *IEEE Access,* pp.

71814 - 71838, 23 November 2018.

[53] D. Câmara και N. Nikaein, Wireless Public Safety Networks 1 - Overview and Challenges, Elsevier Ltd, ISTE Press Ltd, 2015.

[54] M. Ulema, D. Zuckerman, P. Chatzimisios, F. Granelli, N. Mangra, E. Markakis, K. Namuduri, Y. Nikoloudakis, P. Rawat, M. Z. Shakir και T. Zhang, «Public Safety Technology Gaps and Opportunities - Public Safety Technology Task Force,» IEEE Future Directions Committee, 2021.

[55] A. U. Chaudhry και R. H. M. Hafez, «Review Article: LMR and LTE for Public Safety in 700 MHz Spectrum,» *Hindawi Wireless Communications and Mobile Computing,* p. 17, 2019.

[56] ITU-R, «Conventional digital land mobile radio Report ITU-R M.2474-0,» International Telecommunication Union Radiocommunication, Geneva, 2019.

[57] M. Ulema, Fundamentals of Public Safety Networks and Critical Communications Systems: Technologies, Deployment, and Management, New York: WILEY - IEEE PRESS, 2019.

[58] R. Liebhart, D. Chandramouli, C. Wong και J. Merkel, LTE FOR PUBLIC SAFETY, Wiley, 2015.

[59] Σ. Κωτσόπουλος, *ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ & ΠΡΩΤΟΚΟΛΛΑ ΔΙΚΤΥΩΝ ΙΙ,* 2012.

[60] A. Ahtianen, H. Kaaranen, S. Naghian, L. Laitinen και V. Niemi, UMTS Networks: Architecture, Mobility and Services, Helsinki, Finland: Wiley, 2005.

[61] Rohde & Schwarz, [Ηλεκτρονικό]. Available: https://www.rohde-schwarz.com/us/technologies/cellular/wcdma-hspa/wcdma-hspa-hspaplus-technology/wcdma-hspa-hspaplus_55946.html.

[62] Δ. Βουγιούκας, *Ασύρματα Δίκτυα Επικοινωνιών Δίκτυο LTE & LTE-Advanced.*

[63] R. Ferrús, O. Sallent, G. Baldini και L. Goratti, «LTE: The Technology Driver for Future Public Safety Communications,» *IEEE Communications Magazine,* pp. 154-161, October 2013.

[64] T. Doumi, M. F. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan και D. Flore, «LTE for Public Safety Networks,» *IEEE Communications Magazine,* pp. 106-112, February 2013.

[65] J. Noordhof, «Introduction to Broadband and Convergence- How to Choose the Right Communication Bearers,» Radio Academy - Tait Communications, [Ηλεκτρονικό]. Available: https://www.taitradioacademy.com/topic/pros-and-cons-of-lte/. [Πρόσβαση 02 01 2023].

[66] «THE FUTURE IS NOW: PUBLIC SAFETY LTE COMMUNICATIONS - WHITE PAPER,» Motorola Solutions , Schaumburg, Illinois, USA, 2012.

[67] Nokia Networks, «LTE-Advanced Pro Pushing LTE capabilities towards 5G,» ESPOO, Finland, 2015.

[68] S. M. Kerner, «4G (fourth-generation wireless),» TechTarget, [Ηλεκτρονικό]. Available: https://www.techtarget.com/searchmobilecomputing/definition/4G. [Πρόσβαση 02 01 2023].

[69] J. Li, K. K. Nagalapur, E. Stare, S. Dwivedi, S. A. Ashraf, P.-E. Eriksson, U. Engström, W.-H. Lee και T. Lohmar, «5G new radio for public safety mission critical communications,» 2021.

[70] K. Buchholz, «statista,» statista., 14 10 2022. [Ηλεκτρονικό]. Available: https://www.statista.com/chart/23194/5g-networks-deployment-world-map/. [Πρόσβαση 23 01 2023].

[71] «5G,» [Ηλεκτρονικό]. Available: https://5g.co.uk/guides/what-is-the-tactile-internet/. [Πρόσβαση 27 01 2023].

[72] «ITU,» ITU, 09 2015. [Ηλεκτρονικό]. Available: https://www.itu.int/rec/R-REC-M.2083-0-201509-I/en. [Πρόσβαση 28 01 2023].

[73] «ITU,» ITU, 02 2022. [Ηλεκτρονικό]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2150-1-202202-I!!PDF-E.pdf. [Πρόσβαση 28 01 2023].

[74] H. Remmert, «DIGI,» DIGI, 19 03 2021. [Ηλεκτρονικό]. Available: https://www.digi.com/blog/post/5g-network-architecture. [Πρόσβαση 28 01 2023].

[75] J. F. M. P. M. Afif Osseiran, «The 5G architecture,» σε *5G Mobile and Wireless Communications Technology*, New York, Cambridge University Press, 2016, p. 51.

[76] A. A. Gebremariam, M. Usman, R. Bassoli και F. Granelli, «SoftPSN: Software-defined resource slicing for low-latency reliable public safety networks,» *Wireless communications and mobile computing,* pp. 1-7, 2018.

[77] H. Holma, A. Toskala και T. Nakamura, 5G Technology: 3GPP New Radio, Standards Information Network, 2019.

[78] «3GPP,» 3GPP, [Ηλεκτρονικό]. Available: https://www.3gpp.org/specifications-technologies/releases/release-17. [Πρόσβαση 10 01 2023].

[79] «Qualcomm,» Qualcomm, 08 09 2022. [Ηλεκτρονικό]. Available: https://www.qualcomm.com/news/onq/2022/09/how-will-sidelink-bring-a-new-level-of-5g-versatility#:~:text=Sidelink%20is%20a%20core%20topology,and%20reception%20of%20data%20traffic.. [Πρόσβαση 27 01 2023].

[80] S. Kitanov και T. Janevski, «Energy efficiency of Fog Computing and Networking services in 5G networks,» σε *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, 2017.

[81] I. B. Sofi και A. Gupta, «A survey on energy efficient 5G green network with a planned multi-tier architecture,» *Journal of network and computer applications,* pp. 1-28.

[82] A. A. Esswie, «Power saving techniques in 3GPP 5G new radio: A comprehensive latency and reliability analysis,» 2022.

[83] I. P. Chochliouros, M.-A. Kourtis, A. S. Spiliopoulou, P. Lazaridis, Z. Zaharis, C. Zarakovitis και A. Kourtis, «Energy efficiency concerns and trends in future 5G network infrastructures,» *Energies,* αρ. 17, p. 5392, 2021.

[84] «Cloudfront.net,» 01 12 2022. [Ηλεκτρονικό]. Available: https://d86o2zu8ugzlg.cloudfront.net/mediatek-craft/documents/MediaTek_White-Paper-R17-5G.pdf. [Πρόσβαση 23 01 2023].

[85] «Devopedia,» [Ηλεκτρονικό]. Available: https://devopedia.org/images/article/300/4048.1609137100.png. [Πρόσβαση 27 01 2023].

[86] «ETSI,» ETSI, [Ηλεκτρονικό]. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/17.05.00_60/ts_133501v170500p.pdf. [Πρόσβαση 27 01 2023].

[87] «3GPP,» 01 04 2022. [Ηλεκτρονικό]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=623. [Πρόσβαση 28 01 2023].

[88] «3GPP,» 01 04 2022. [Ηλεκτρονικό]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3018. [Πρόσβαση 28 01 2023].

[89] «3GPP,» 01 04 2022. [Ηλεκτρονικό]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3019. [Πρόσβαση 28 01 2023].

[90] M. Pope, «3GPP,» 21 12 2021. [Ηλεκτρονικό]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144. [Πρόσβαση 28 01 2023].

[91] A. Jarwan, A. Sabbah, M. Ibnkahla και O. Issa, «LTE-based public safety networks: A survey,» *IEEE Communications Surveys & Tutorials,* τόμ. 21, αρ. 2, pp. 1165-1187, 2019.

[92] The Public Safety LTE & 5G Market: 2022 - 2030 - Opportunities, Challenges, Strategies & Forecasts.

[93] C. Appiakorang, «NIST,» 09 05 2022. [Ηλεκτρονικό]. Available: https://www.nist.gov/news-events/news/2022/05/firstnet-authority-nist-launch-immersive-virtual-experience-center-public. [Πρόσβαση 02 02 2023].

[94] «Denver7,» 03 08 2022. [Ηλεκτρονικό]. Available: https://www.denver7.com/news/national/immersive-virtual-reality-brings-first-responder-training-into-the-future. [Πρόσβαση 02 02 2023].

[95] «NIST,» [Ηλεκτρονικό]. Available: https://www.nist.gov/ctl/pscr/about/public-safety-immersive-test-center. [Πρόσβαση 02 02 2023].

[96] A. A. Abidi, «The Path to the Software-Defined Radio Receiver,» *IEEE Journal of Solid-State Circuits,* pp. 954 - 966, 23 April 2007.

[97] G. Youngblood, «A Software-Defined Radio for the Masses, Part 1, 2, 3 and 4,» ARRL's QEX, 2002 - 2003. [Ηλεκτρονικό]. Available: https://sites.google.com/site/thesdrinstitute/A-Software-Defined-Radio-for-the-Masses. [Πρόσβαση 03 01 2023].

[98] F. Frantz, «SDR for Public Safety,» L-3 Communications Government Services.

[99] SDR Forum, «Software Defined Radio Technology for Public Safety,» SDR Forum, 2006.

[100] M. Roomi, «5 Advantages and Disadvantages of SDN | Drawbacks & Benefits of SDN,» Hitechwhizz, 28 06 2021. [Ηλεκτρονικό]. Available: https://www.hitechwhizz.com/2021/06/5-advantages-and-disadvantages-drawbacks-benefits-of-sdn.html. [Πρόσβαση 03 01 2023].

[101] M. Dabbagh, B. Hamdaoui, M. Guizani και A. Rayes, «Software-Defined Networking Security: Pros and Cons,» *IEEE Communications Magazine,* June 2015.

[102] KnowledgeNile, «Software-Defined Networking Architecture: Prow and Cons of SDN,» KnowledgeNile, [Ηλεκτρονικό]. Available: https://www.knowledgenile.com/blogs/software-defined-networking-architecture-pros-and-cons-of-sdn/. [Πρόσβαση 04 01 2023].

[103] R. Awati, «cognitive radio (CR),» TechTarget, [Ηλεκτρονικό]. Available: https://www.techtarget.com/searchnetworking/definition/cognitive-radio. [Πρόσβαση January 2023].

[104] Z. Yu, S. Hoyos και B. M. Sadler, «MIXED-SIGNAL PARALLEL COMPRESSED SENSING AND RECEPTION FOR COGNITIVE RADIO,» σε *IEEE International Conference on Acoustics, Speech, and Signal*, Texas, USA, 2008.

[105] Wireless Innovation Forum, «Cognitive Radio Concept Architecture,» Wireless Innovation Forum, [Ηλεκτρονικό]. Available: https://www.wirelessinnovation.org/Cognitive_Radio_Architecture. [Πρόσβαση 03 01 2023].

[106] K. Gomez, S. Kandeepan, M. M. Vida, V. Boussemart, R. Ramos, R. Hermenier, T. Rasheed, L. Goratti, L. Reynaud, D. Grace, Q. Zhao, Y. Han, S. Rehan, N. Morozs, I. Bucaille, T. Wirth, R. Campo και T. Javornik, «Aerial Base Stations with Opportunistic Links for Next Generation Emergency Communications,» *IEEE Communications Magazine,* pp. 31-39, April 2016.

[107] European Commissions - CORDIS EU Research results, «COgnitive RAdio for SATellite Communications,» 30 09 2015. [Ηλεκτρονικό]. Available: https://cordis.europa.eu/docs/projects/cnect/9/316779/080/deliverables/001-CoRaSatDelD56r1v0.pdf. [Πρόσβαση 04 01 2023].

[108] S. Maleki, S. Chatzinotas, B. Evans, K. Liolis, J. G. Grotz, A. Vanelli-Coralli και N. Chuberre, «Cognitive Spectrum Utilization in Ka Band Multibeam Satellite Communications,» *IEEE Communications Magazine,* τόμ. 53, αρ. 3, pp. 24-29, March 2015.

[109] «System Reference document (SRdoc); Cognitive radio techniques for Satellite Communications operating in Ka band,» ETSI TR 103 263 , 2016.

[110] «CREW Project - Cognitive Radio Experimentation World,» European Commisssion, 2010. [Ηλεκτρονικό]. Available: http://www.crew-project.eu/. [Πρόσβαση 04 01 2023].

[111] G. Baldini, O. Picchi, M. Luise, T. A. Sturman, F. Vergari, C. Moy, T. Bräysy και R. Dopico, «The EULER Project: Application of Software Defined Radio in Joint Security Operations,» *IEEE Communications Magazine,* pp. 55-62, October 2011.

[112] G. Baldini, T. Sturman, A. Dalode, A. Kropp και C. Sacchi, «An emergency communication system based on software-defined radio,» *EURASIP Journal on Wireless Communications and Networking,* 01 10 2014.

[113] E. A. Yfantis, «A UAV with Autonomy, Pattern Recognition for Forest Fire Prevention, and AI for Providing Advice to Firefighters Fighting Forest Fires,» σε *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, USA, 2019.

[114] SAGEM DEFENSE SECURITE, «Digital and Innovative Technologies for Security and Efficiency of First Responders operation,» 31 12 2012. [Ηλεκτρονικό]. Available: https://cordis.europa.eu/docs/results/225/225404/final1-sp100-sds-ditsef-final-report-c00.pdf. [Πρόσβαση 04 01 2023].

[115] E. Del Re, S. Jayousi, S. Morosi, L. S. Ronga, M. De Sanctis, E. Cianca, M. Ruggieri, E. F. Falletti, A. Iera, G. Araniti και C. Sacchi, «SALICE Project: Satellite-Assisted Localization and Communication Systems for Emergency Services,» *IEEE A&E SYSTEMS MAGAZINE,* pp. 4-15, September 2013.

[116] Xavier Mestre, «Enhanced Multicarrier Techniques for Professional Ad-Hoc and Cell-Based Communications (EMPhAtiC),» 29 04 2015. [Ηλεκτρονικό]. Available: https://cordis.europa.eu/docs/projects/cnect/2/318362/080/deliverables/001-318362EMPHATICD15PROJECTFINALREPORTrenditionDownload.pdf. [Πρόσβαση 04 01 2023].

[117] NSF, «Enhancing Access to the Radio Spectrum (EARS),» National Science Foundation , 18 April 2014. [Ηλεκτρονικό]. Available: https://www.nsf.gov/pubs/2014/nsf14529/nsf14529.htm. [Πρόσβαση January 2023].

[118] NSF, «Robust and Secure Cognitive Radio Networks,» National Science Foundation, 30 08 2011. [Ηλεκτρονικό]. Available: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1147811. [Πρόσβαση 04 01 2023].

[119] 3GPP TR 22.803 Technical Report , «3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study for Proximity Services (ProSe) (Release 12),» 3GPP, Valbonne Franch , 2013.

[120] 3GPP TR23.703, «3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Study on architecture enchancements to support Proximity-based Services (ProSe)(Release 12),» 3GPP, Valbonne France, 2014.

[121] L. Goratti, K. M. Gomez, R. Fedrizzi και T. Rasheed, «A Novel Device-to-Device Communication Protocol for Public Safety Applications,» σε *2013 IEEE Globecom Workshops (GC Wkshps)*, Atlanta, USA, 2013.

[122] L. Goratti, G. Steri, K. M. Gomez και G. Baldini, «Connectivity and Security in a D2D Communication Protocol for Public Safety Applications,» σε *2014 11th International Symposium on Wireless Communications Systems (ISWCS)*, Barcelona, Spain, 2014.

[123] T. Ohtsuji, K. Muraoka, H. Aminaka, D. Kanetomo και Y. Matsunaga, «Device-to-Device Relay Selection based on Effective Path Throughput to Fill Coverage Hole in Public Safety LTE,» σε *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South), 2016.

[124] M. USMAN, A. A. GEBREMARIAM, U. RAZA και F. GRANELLI, «A Software-Defined Device-to-Device Communication Architecture for Public Safety Applications in 5G Networks,» *IEEE Access,* pp. 1649-1654, 1 October 2015.

[125] S. Gyawali, S. Xu, F. Ye, R. Q. Hu και Y. Qian, «A D2D based Clustering Scheme for Public Safety Communications,» σε *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, Porto, Portugal, 2018.

[126] W. YU, H. XU, J. NGUYEN, E. BLASCH, A. HEMATIAN και W. GAO, «Survey of Public Safety Communications: User-Side and Network-Side Solutions and Future Directions,» *IEEE Access,* pp. 70397-70425, 25 October 2018.

[127] G. FODOR, S. PARKVALL, S. SORRENTINO, P. WALLENTIN, Q. LU και N. BRAHMI, «Device-to-Device Communications for National Security and Public Safety,» *IEEE Access,* τόμ. 2,

pp. 1510-1520, 2014.

[128] O. HAYAT, R. NGAH, Z. KALEEM, S. Z. M. HASHIM και J. RODRIGUES, «A Survey on Security and Privacy Challenges in Device Discovery for Next-Generation Systems,» *IEEE Access,* pp. 84584-84603, 26 April 2020.

[129] CableFree 10+ Gigabit Wireless Networks, «LTE 3GPP releases Overview,» CableFree 10+ Gigabit Wireless Networks, 12 2015. [Ηλεκτρονικό]. Available: https://www.cablefree.net/wirelesstechnology/4glte/overview-of-lte-3gpp-releases/. [Πρόσβαση 04 01 2023].

[130] E. Webster, «MIMO (multiple input, multiple output),» TechTarget, [Ηλεκτρονικό]. Available: https://www.techtarget.com/searchmobilecomputing/definition/MIMO. [Πρόσβαση 04 01 2023].

[131] E. G. Larsson, O. Edfors, F. Tufvesson και T. L. Marzetta, «MASSIVE MIMO FOR NEXT GENERATION WIRELESS SYSTEMS,» *IEEE Communication Magazin,* τόμ. 52, αρ. 2, pp. 186 - 195, 23 January 2014.

[132] M. MEZZAVILLA, M. POLESE, A. ZANELLA, A. DHANANJAY, S. RANGAN, C. KESSLER, T. S. RAPPAPORT και M. ZORZI, «Public Safety Communications above 6 GHz: Challenges and Opportunities,» *IEEE Access,* pp. 316-329, 14 November 2017.

[133] N. Abbey, «5G mmWave Technology: What you need to know?,» STL, 03 08 2022. [Ηλεκτρονικό]. Available: https://www.stl.tech/blog/5g-mmwave-technology-what-you-need-to-know/. [Πρόσβαση 04 01 2023].

[134] GSM Association, «5G millimetre wave safety,» 10 2022. [Ηλεκτρονικό]. Available: https://www.gsma.com/publicpolicy/wp-content/uploads/2022/11/5G-millimetre-wave-safety-v2.pdf. [Πρόσβαση 04 01 2023].

[135] A. . I. Sulyman, A. T. Nassar, M. K. Samimi, G. R. MacCartney Jr, T. S. Rappaport και A. Alsanie, «Radio Propagation Path Loss Models for 5G Cellular Networks in the 28 GHz and 38 GHz Millimeter-Wave Bands,» *Communications Magazine, IEEE,* τόμ. 52, αρ. 9, pp. 78-86, 2014.

[136] K. Karipidis, R. Mate, D. Urban, R. Tinker και A. Wood, «5G mobile networks and health—a state-of-the-science review of the research into low-level RF fields above 6 GHz,» *Journal of Exposure Science & Environmental Epidemiology,* τόμ. 31, p. 585–605, 2021.

[137] Y. Niu, Y. Li, D. Jin, L. Su και A. . V. Vasilakos, «A Survey of Millimeter Wave (mmWave) Communications for 5G: Opportunities and Challenges,» *Wireless Network,* τόμ. 21, αρ. 8, p. 2657–2676, 2015.

[138] V. A. Thomas, M. El-Hajjar και L. Hanzo, «Millimeter-Wave Radio Over Fiber Optical Upconversion Techniques Relying on Link Nonlinearity,» *IEEE COMMUNICATION SURVEYS &*

TUTORIALS, τόμ. 28, αρ. 1, p. 29–53, 2015.

[139] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari και M. Ayyash, «Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,» *IEEE COMMUNICATION SURVEYS & TUTORIALS,* τόμ. 17, αρ. 4, pp. 2347-2376, 2015.

[140] P. Fraga-Lamas, T. M. Fernández-Caramés, M. Suárez-Albela, L. Castedo και M. González-López, «A Review on Internet of Things for Defense and Public Safety,» *Sensors,* 5 October 2016.

[141] P. PRATIM RAY, M. MUKHERJEE και L. SHU, «Internet of Things for Disaster Management: State-of-the-Art and Prospects,» *IEEE Access,* pp. 18818-18835, 12 October 2017.

[142] INTEL, «Emerging Public Safety Technology Leveraging IoT,» INTEL, [Ηλεκτρονικό]. Available: https://www.intel.com/content/www/us/en/internet-of-things/smart-cities-public-safety.html. [Πρόσβαση 04 01 2023].

[143] opentechdiary, «PART 2 : A WALK THROUGH INTERNET OF THINGS (IOT) BASICS,» opentechdiary, 16 07 2015. [Ηλεκτρονικό]. Available: https://opentechdiary.wordpress.com/2015/07/16/a-walk-through-internet-of-things-iot-basics-part-2/. [Πρόσβαση 04 01 2023].

[144] S. Kr, B. Pokric και F. Carrez, «Designing IoT Architecture(s) A European Perspective,» σε *2014 IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, Korea, 2014.

[145] CORDIS, «Internet of Things Architecture,» CORDIS, 30 11 2013. [Ηλεκτρονικό]. Available: https://cordis.europa.eu/project/id/257521. [Πρόσβαση 04 01 2023].

[146] L. Karagiannidis, «Challenges and opportunities in connecting IoT and public safety,» 06 2019. [Ηλεκτρονικό]. Available: https://aioti.eu/wp-content/uploads/2019/06/The-missing-link-between-IoT-and-public-safety_FINAL.pdf. [Πρόσβαση 04 01 2023].

[147] National Public Safety Telecommunications Council, «Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes,» 06 2019. [Ηλεκτρονικό]. Available: https://www.npstc.org/download.jsp?tableId=37&column=217&id=4195&file=NPSTC_PSIoT_Use_Cases_Report_190616.pdf. [Πρόσβαση 04 01 2023].

[148] A. Kumbhar, F. Koohifar, I. Güvenç και B. Mueller, «A Survey on Legacy and Emerging Technologies for Public Safety Communications,» *IEEE,* 2017.

[149] Ι. Καπουλας, Α. Καρυπιδης και Δ. Ντεντας, *Communications for Smart Cities,* Θεσσαλονίκη: Εργασία Φοιτητών ΜΠΣ στο μάθημα ΣΚΔΥ, 2022.

[150] Α. Καρυπίδης, *Communication protocols for First Responders and,* Θεσσαλονίκη: Εργασία Φοιτητή ΠΜΣ στο μάθημα Μεθοδολογίες Έρευνας, 2021.

[151] R. Want, «An Introduction to RFID Technology,» *ResearchGate,* pp. 25-33, February 2006.

[152] N. Chhabra, «Comparative Analysis of Different Wireless Technologies,» *Network Security and Communication,* pp. 13-17, 30 December 2013.

[153] C. Saad, B. Mostafa, E. A. Cheikh και H. Abderrahmane, «Comparative Performance Analysis of Wireless Communication Protocols for Intelligent Sensors and Their Applications,» *(IJACSA) International Journal of Advanced Computer Science and Applications,,* pp. 76-85, September 2014.

[154] H. Cao, V. Leung, C. Chow και H. Chan, «Enabling Technologies for Wireless Body Area Networks: A Survey and Outlook,» *IEEE Communications Magazine,* pp. 84-93, December 2009.

[155] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta και Y. Fun Hu, «Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards,» *Elsevier,* pp. 1656-1695, 29 December 2006.

[156] «Internet of Things-IOT: Definition, Characteristics, Architecture,Enabling Technologies, Application & Future Challenges,» *International Journal of Engineering Science and Computing (IJESC),* pp. 6122-6131, May 2016.

[157] K. K. Nair, A. M. Abu-Mahfouz και S. Lefophane, «Analysis of the Narrow Band Internet of Things (NB-IoT) Technology,» σε *2019 Conference on Information Communications Technology and Society (ICTAS)*, Durban, South Africa, 2019.

[158] I.-G. Lee, D. B. Kim, J. Choi, H. Park, S.-K. Lee, J. Cho και H. Yu, «WiFi HaLow for Long-Range and LowPower Internet of Things: System on Chip,» *IEEE Communications Magazine,* pp. 101-107, July 2021.

[159] IEEE 802.11, «IEEE 802.11 WIRELESS LOCAL AREA NETWORKS,» IEEE, [Ηλεκτρονικό]. Available: https://www.ieee802.org/11/. [Πρόσβαση 04 01 2023].

[160] «LoRa RF Interface and Physical Layer,» electronics notes, [Ηλεκτρονικό]. Available: https://www.electronics-notes.com/articles/connectivity/lora/radio-rf-interface-physical-layer.php. [Πρόσβαση 04 01 2023].

[161] J. d. C. Silva, J. J. P. C. Rodrigues, A. M. Alberti, P. Solic και A. L. L. Aquino, «LoRaWAN - A Low Power WAN Protocol for Internet of Things: a Review and Opportunities,» σε *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*, Split, Croatia, 2017.

[162] A. Lavric, A. I. Petrariu και V. Popa, «SigFox Communication Protocol: The New Era of IoT?,» σε *2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI)*, Lisbon, Portugal, 2019.

[163] Y. ZHANG, N. ANSARI και H. TSUNODA, «WIRELESS TELEMEDICINE SERVICES OVER INTEGRATED IEEE 802.11/WLAN AND IEEE 802.16/WIMAX NETWORKS,» *IEEE Wireless Communications,* pp. 30-36, February 2010.

[164] N. Tantitharanukul, K. Osathanunkul, K. Hantrakul, P. Pramokchon και P. Khoenkaw, «MQTT-Topic Naming Criteria of Open Data for Smart Cities,» σε *2016 International Computer Science and Engineering Conference (ICSEC)*, Chiang Mai, Thailand, 2016.

[165] A. Chaudhary, S. K. Peddoju και K. Kadarla, «Study of Internet-of-Things Messaging Protocols Used for Exchanging Data with External Sources,» σε *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, Orlando, USA, 2017.

[166] D. Glaroudis, A. Iossifides και P. Chatzimisios, «Survey, comparison and research challenges of IoT application protocols for smart farming,» *Elsevier Computer Networks,* 26 February 2020.

[167] RTInsights, «How Edge Computing and IoT Make Cities Safer,» Real Time Insights, 8 06 2020. [Ηλεκτρονικό]. Available: https://www.rtinsights.com/edge-iot-safe-city-infographic/. [Πρόσβαση 04 01 2023].

[168] W. Chai και S. J. Bigelow, «cloud computing,» TechTarget, [Ηλεκτρονικό]. Available: https://www.techtarget.com/searchcloudcomputing/definition/cloud-computing. [Πρόσβαση 04 01 2023].

[169] J. Bulano, «How Much Data Is Created Every Day in 2023?,» techjury, 07 02 2023. [Ηλεκτρονικό]. Available: https://techjury.net/blog/how-much-data-is-created-every-day/#gref. [Πρόσβαση 09 02 2023].

[170] IBM, «The Future of Public Safety How data and intelligence will transform law enforcement,» σε *IBM Government Cloud Virtual Summit Special Hybrid Cloud Edition*, 2019.

[171] O. Bekkouche, T. Taleb και M. Bagaa, «UAVs Traffic Control based on Multi-Access Edge Computing,» *ResearchGate,* December 2018.

[172] E. Maltezos, L. Karagiannidis, A. Dadoukis, K. Petousakis, F. Misichroni, E. Ouzounoglou, L. Gounaridis, D. Gounaridis, C. Kouloumentas και A. Amditis, «Public safety in smart cities under the edge computing concept,» σε *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, Athens, Greece, 2021.

[173] W. Shi, J. Cao, Q. Zhang, Y. i Li και L. Xu, «Edge Computing: Vision and Challenges,» *IEEE INTERNET OF THINGS JOURNAL,* pp. 637-646, October 2016.

[174] D. Nagothu, R. Xu, S. Y. Nikouei, X. Zhao και Y. Chen, «Smart Surveillance for Public Safety Enabled by,» σε *Edge Computing: Models, technologies and applications*, IET Digital Library,

2020, p. 447.

[175] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. Ahsan Kazmi, T. N. Dang και C. S. Hong, «Edge-Computing-Enabled Smart Cities: A Comprehensive Survey,» *IEEE Internet of Things Journal ,* pp. 10200 - 10232, 10 April 2020.

[176] M. G. SARWAR MURSHED, C. MURPHY, D. HOU, N. KHAN, G. ANANTHANARAYANAN και F. HUSSAIN, «Machine Learning at the Network Edge: A Survey,» *ResearchGate,* July 2021.

[177] M. Satyanarayanan, P. Bahl, R. Cáceres και N. Davies, «The Case for VM-Based Cloudlets in Mobile Computing,» *IEEE Pervasive Computing,* τόμ. 8, αρ. 4, pp. 14-23, 2009.

[178] T. Taleb και A. Ksentini, «Follow Me Cloud: Interworking Federated Clouds & Distributed Mobile Networks,» *IEEE Network,* 2013.

[179] A. Bahtovski και M. Gusev, «Cloudlet Challenges,» σε *24th DAAAM International Symposium on Intelligent Manufacturing and Automation, 2013*, 2013.

[180] M. Losavio, «Fog Computing, Edge Computing and a return to privacy and personal autonomy,» σε *Third International Conference on Computing and Network Communications (CoCoNet'19)*, 2019.

[181] B. Posey και S. Shea, «What is fog computing?,» TechTarget, [Ηλεκτρονικό]. Available: https://www.techtarget.com/iotagenda/definition/fog-computing-fogging. [Πρόσβαση 04 01 2023].

[182] OpenFog Consortium, «OpenFog Consortium Introduction and Overview at W3C Open Day,» 05 2017. [Ηλεκτρονικό]. Available: https://www.w3.org/2017/05/wot-f2f/slides/OpenFog-Overview-W3C-Open-Day-in-May-2017.pdf. [Πρόσβαση 05 01 2023].

[183] N. Mohamed, J. Al-Jaroodi, S. Lazarova-Molnar και I. Jawhar, «Applications of Integrated IoT-Fog-Cloud Systems to Smart Cities: A Survey,» *electronics,* τόμ. 10, αρ. 23, 2021.

[184] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam και M. Debbah, «A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems,» *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* pp. 2334-2360, 5 March 2019.

[185] L. Gupta, R. Jain και G. Vaszkun, «Survey of Important Issues in UAV Communication Networks,» *IEEE COMMUNICATIONS SURVEYS & TUTORIALS,* pp. 1123-1152, May 2016.

[186] S. SHAKOOR, Z. KALEEM, M. I. BAIG, O. CHUGHTAI, T. Q. DUONG και L. D. NGUYEN, «Role of UAVs in Public Safety Communications: Energy Efficiency Perspective,» *IEEE Access,* pp. 140665-140679, 18 September 2019.

[187] A. Sharma, P. Vanjani, N. Paliwal, C. M. Wijerathna Basnayaka, D. N. . K. Jayakody, H.-C. Wang και P. Muthuchidambaranathan, «Communication and Networking Technologies for UAVs: A Survey,» *Journal of Network and Computer Applications,* τόμ. 168, 2020.

[188] E. Kalantari, H. Yanikomeroglu και A. Yongacoglu, «On the Number and 3D Placement of Drone Base Stations in Wireless Cellular Networks,» σε *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*, Montréal, Canada, 2016.

[189] H. TENG, I. AHMAD, A. MSM και K. CHANG, «3D Optimal Surveillance Trajectory Planning for Multiple UAVs by Using Particle Swarm Optimization With Surveillance Area Priority,» *IEEE Access,* τόμ. 8, pp. 86316 - 86327, 2020.

[190] Y. Zheng, Y. Wang και F. Meng, «Modeling and Simulation of Pathloss and Fading for Air-Ground Link of HAPs within a Network Simulator,» σε *2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Washington, USA, 2013.

[191] J. Horwath, N. Perlot, M. Knapek και F. Moll, «Experimental verification of optical backhaul links for high- altitude platform networks: Atmospheric turbulence and downlink availability,» *INTERNATIONAL JOURNAL OF SATELLITE COMMUNICATIONS AND NETWORKING,* τόμ. 25, pp. 501-528, 2007.

[192] Y. Zeng και R. Zhang, «Energy-Efficient UAV Communication with Trajectory Optimization,» *IEEE Transactions on Wireless Communications,* τόμ. 16, αρ. 6, pp. 3747 - 3760, 2017.

[193] A. Y. Javaid, W. Sun, V. K. Devabhaktuni και M. Alam, «Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System,» σε *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, USA, 2012.

[194] A. . R. Ragab, M. S. Ale Isaac και M. A. Luna, «Unmanned Aerial Vehicle Swarming,» σε *7th International Conference on Engineering and Emerging Technologies (ICEET)*, Istanbul, Turkey, 2021.

[195] M. Khelifi και I. Butun, «Swarm Unmanned Aerial Vehicles (SUAVs): A Comprehensive Analysis of Localization, Recent Aspects, and Future Trends,» *Hindawi Journal of Sensors,* 14 February 2022.

[196] I. FRESNEL, «fresnel,» INSTITUT FRESNEL, [Ηλεκτρονικό]. Available: https://www.fresnel.fr/spip/spip.php?article1169&lang=fr. [Πρόσβαση 19 01 2023].

[197] A. Seas, B. Robinson, T. Shih, F. Khatri και M. Brumfield, «Optical communications systems for NASA's human space flight missions,» σε *International Conference on Space Optics — ICSO 2018*, 2018.

[198] «Taara - X, the moonshot factory,» X, the moonshot factory, [Ηλεκτρονικό]. Available: https://x.company/projects/taara/. [Πρόσβαση 19 01 2023].

[199] H. H. a. O. Wilfert, «An introduction to free-space optical communications,» *Radioengineering,* pp.

203-212, 2010.

[200] S. Kumar και N. Sharma, «Emerging military applications of Free Space Optical Communication technology: A detailed review,» *Journal of physics. Conference series,* τόμ. 1, 2022.

[201] Z. Zeng, S. Fu, H. Zhang, Y. Dong και J. Cheng, «A survey of underwater optical wireless communications,» *IEEE Communications Surveys & Tutorials,* τόμ. 19, αρ. 1, 2017.

[202] R. A. Motes, «Free-Space Laser Communication: An Introduction,» 2016.

[203] «NASA,» [Ηλεκτρονικό]. Available: https://www.nasa.gov/sites/default/files/llcdfactsheet.final_.web_.pdf. [Πρόσβαση 19 01 2023].

[204] S. Haque, «A broadband multi-hop network for earth-mars communication using multi-purpose interplanetary relay satellites and linear-circular commutating chain topology,» Reston, Virigina, 2011.

[205] J. T. :. Hq, «NASA,» [Ηλεκτρονικό]. Available: https://www.nasa.gov/directorates/spacetech/small_spacecraft/ocsd_project.html. [Πρόσβαση 19 01 2023].

[206] «Huawey,» Huawey, [Ηλεκτρονικό]. Available: https://www.huawei.com/en/huaweitech/inspiration-lab/optical-link-solution/fso-protype-innovation-live-demo. [Πρόσβαση 20 01 2023].

[207] «Aalyria,» Aalyria, [Ηλεκτρονικό]. Available: https://www.aalyria.com/#home. [Πρόσβαση 20 01 2023].

[208] Ευρωπαϊκή Επιτροπή, «Ραδιοφάσμα: η βάση των ασύρματων επικοινωνιών,» Ευρωπαϊκή Επιτροπή Shaping Europe`s digital future, [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/el/policies/radio-spectrum. [Πρόσβαση 31 01 2023].

[209] Γ. Καρίμαλης, «Ο Πρόεδρος της ΕΕΤΤ στην Προεδρία του BEREC για το 2023,» ΕΕΤΤ, 31 01 2023. [Ηλεκτρονικό]. Available: https://www.eett.gr/deltia_tipou/o-proedros-tis-eett-stin-proedria-toy-berec-gia-to-2023/. [Πρόσβαση 02 02 2023].

[210] Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, «ΑΠΟΦΑΣΗ αριθ. 243/2012/ΕΕ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ,» 14 03 2012. [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32012D0243&from=IT. [Πρόσβαση 31 01 2023].

[211] Επιτροπή Ευεωπαϊκών Κοινοτήτων, «Η παγκόσμια διάσκεψη ραδιοεπικοινωνιών 2007 της ITU,» 2 07 2007. [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52007DC0371&from=SK. [Πρόσβαση 07 01 2023].

[212] Β. Λογοθέτης και Ι. Νοεοκοσμίδης, «Κατά πόσο μπορεί η ανάγκη αλλαγής του τρόπου εκχώρησης

του φάσματος να αλλάξει τη δομή της τηλεπικοινωνιακής αγοράς;,» The Power Game, 27 01 2022. [Ηλεκτρονικό]. Available: https://www.powergame.gr/apopsis/192153/kata-poso-borei-i-anagki-allagis-tou-tropou-ekchorisis-tou-fasmatos-na-allaxei-ti-domitis-tilepikoinoniakis-agoras/. [Πρόσβαση 31 01 2023].

[213] FCC, «Public Safety Spectrum,» FCC, [Ηλεκτρονικό]. Available: https://www.fcc.gov/public-safety/public-safety-and-homeland-security/policy-and-licensing-division/public-safety-spectrum. [Πρόσβαση 31 01 2023].

[214] E. Hossain, D. Niyato και Z. Han, Dynamic Spectrum Access and Managment in Cognitive Radio Networks, New York: Cambridge University Press, 2009.

[215] R. Becker, *2021 4th IEEE 5G Workshop on First Responder and Tactical Networks,* Online: DHS / Office for Interoperability and Compatibility / Technology Centers Division, 2021.

[216] B. N. Silva, M. Khan και K. Han, «Internet of Things: A Comprehensive Review of Enabling Technologies, Architecture, and Challenges,» *Taylor and Francis Online,* pp. 205-220, 8 February 2017.

[217] R. Russell, *Edge Services, IAB, and ORAN for Tactical 5G Networks,* Online: Radisys , 2021.

[218] M. Ramteke, «What is an Force Sensing Resistor : Types and Applications,» Semiconductor, 09 09 2022. [Ηλεκτρονικό]. Available: https://www.semiconductorforu.com/what-is-an-force-sensing-resistor-types-and-applications/. [Πρόσβαση 02 02 2023].

[219] D. Sehrawat και N. S. Gill, «Smart Sensors: Analysis of Different Types of IoT Sensors,» σε *Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019)*, 2019.

[220] R. Pepito και A. Dutta, *Open Source 5G Security Testbed for Edge Computing - 4th IEEE 5G Workshop on First Responder and Tactical Networks,* Online: John Hopkins University Applied Physics Laboratory (JHU/APL), 2021.

[221] S. Chaudhry και M. Yuksel, «Engaging Communities in Public Safety via Social Media,» σε *2019 IEEE INFOCOM WKSHPS: HotSALSA 2019: Hot Topics in SociAL and mobile connected SmArt objects*, Paris, France, 2019.

[222] KEPIOS, «GLOBAL SOCIAL MEDIA STATISTICS,» DataReportal, 02 2023. [Ηλεκτρονικό]. Available: https://datareportal.com/social-media-users. [Πρόσβαση 18 02 2023].

[223] Μ. Άλγκρεν, «25+ ΣΤΑΤΙΣΤΙΚΆ ΜΈΣΑ ΚΟΙΝΩΝΙΚΉΣ ΔΙΚΤΥΩΣΗΣ, ΓΕΓΟΝΌΤΑ ΚΑΙ ΤΆΣΕΙΣ ΓΙΑ ΤΟ 2023,» WebSiteRating, 06 02 2023. [Ηλεκτρονικό]. Available: https://www.websiterating.com/el/research/social-media-statistics-facts/#social-media-statistics.

[Πρόσβαση 10 02 2023].

[224] S. Chaudhry και M. Yuksel, «Using Social Media for Crowd-Sourced Public Safety,» *IEEE COMSOC MMTC Communications - Frontiers,* τόμ. 14, αρ. 2, pp. 9-15, 2019.

[225] A. Amirkhanyan και C. Meinel, «Analysis of data from Twitter account of Berlin Police for public safety awareness,» σε *2017 IEEE 21st International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Wellington, New Zealand, 2017.

[226] engage, «Catalog of Solutions,» engage, [Ηλεκτρονικό]. Available: https://engageknowledgeplatform.eu/#/catalog-of-solutions. [Πρόσβαση 10 02 2023].

[227] N. Stolero, T. Simon, M. Bodas, K. Peleg και B. Adini , «Exploration of innovative use of communication and social media technologies,» Engage Society for Risk Awareness and Resilience, 2021.

[228] J. Glasco, «How crowdsourcing and incentives improve publ;ic safety,» bee smart city, 10 03 2019. [Ηλεκτρονικό]. Available: https://www.beesmart.city/en/solutions/smart-living/public-safety/how-crowdsourcing-and-incentives-improve-public-safety. [Πρόσβαση 12 02 2023].

[229] A. Goncalves, C. Silva, P. Morreale και J. Bonafide, «Crowdsourcing for public safety,» σε *2014 IEEE International Systems Conference Proceedings*, Ottawa, ON, Canada, 2014.

[230] «Vizsafe's Geoaware Network,» Vizsafe, [Ηλεκτρονικό]. Available: https://www.vizsafe.com/geoawarenetwork. [Πρόσβαση 12 02 2023].

[231] European Commission, «REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL,» European Commission, Brussels, 2022.

[232] EENA, «Public Safety Answering Points Global Edition,» EENA, 2023.

[233] Your Europe - gov.gr, «112 - Ευρωπαϊκός αριθμός κλήσης έκτακτης ανάγκης,» gov.gr, 4 08 2022. [Ηλεκτρονικό]. Available: https://www.gov.gr/sdg/healthcare/national-emergency-numbers/general/112. [Πρόσβαση 11 02 2023].

[234] Α. Κοκκαλάκης, «Ευρωπαϊκός Αριθμός Κλήσης Έκτακτης Ανάγκης "112",» *Αστυνομική Επιθεώρηση,* pp. 22-25, 08 2010.

[235] EENA, «Next Generation 112,» EENA, [Ηλεκτρονικό]. Available: https://eena.org/our-work/eena-special-focus/next-generation-112/. [Πρόσβαση 11 02 2023].

[236] ETSI, «2nd NG112 Emergency Services Plugtest - ETSI CTI Plugtests Report V1.0 (2017-04),» ETSI, Antipolis - Franch, 2017.

[237] ETSI, «3rd NG112 Emergency Services Plugtest - ETSI CTI Plugtests Report V1.0 (2019-01),» ETSI, Antipolis Franch, 2019.

[238] ETSI, «4th NG112 Emergency Services Plugtests - ETSI CTI PLUGTESTS Report V0.3 (2021-04),» ETSI, Antipolis Franch, 2021.

[239] M. Steves, M. F. Theofanos, Y.-Y. Choong, S. Dawkins, S. Furman, K. K. Greene και S. S. Prettyman, «Voices of First Responders – Examining Public Safety Communication from the Perspective of 9-1-1 Call Takers and Dispatchers,» National Institute of Standards and Technology /, 2020.

[240] MPLS911, «Minneapolis Emergency Communications Center,» 18 09 2019. [Ηλεκτρονικό]. Available: https://lims.minneapolismn.gov/Download/FileV2/21144/911-Call-Process-Presentation.pdf. [Πρόσβαση 11 02 2023].

[241] CISCO, «Cisco Annual Internet Report (2018 - 2023),» 2020.

[242] Daniels Electronics LTD, «P25 Radio Systems Training Guide,» Daniels Electronics LTD, Victoria Canada, 2007.

[243] www.taitradio.com, «www.p25bestpractice.com,» 2021. [Ηλεκτρονικό]. Available: www.p25bestpractice.com. [Πρόσβαση 04 01 2023].

[244] Cybersecurity and Infrastructure Security Agency (CISA), «Cybersecurity and Infrastructure Security Agency (CISA),» CISA, 2021. [Ηλεκτρονικό]. Available: https://www.youtube.com/watch?v=2GTAptVOpkE. [Πρόσβαση 04 01 2023].

[245] «www.project25.org,» 18 03 2022. [Ηλεκτρονικό]. Available: https://www.project25.org/index.php/documents/ptig-p25-system-case-studies?view=frontlist&catid[0]=10015. [Πρόσβαση 04 01 2023].

[246] TCCA, «TCCA,» [Ηλεκτρονικό]. Available: https://tcca.info/tetra/for-tetra-specialist/tetra-release-1/. [Πρόσβαση 17 11 2022].

[247] ETSI, «Terrestrial Trunked Radio (TETRA) - Voice plus Data (V+D),» [Ηλεκτρονικό]. Available: https://www.etsi.org/deliver/etsi_en/300300_300399/30039201/01.04.01_60/en_30039201v010401p.pdf. [Πρόσβαση 17 11 2022].

[248] TCCA, «TETRA Release 2,» [Ηλεκτρονικό]. Available: https://tcca.info/tetra/for-tetra-specialist/tetra-release-2/. [Πρόσβαση 17 11 2022].

[249] ETSI, «Study of the suitability of the GSM Adaptive Multi-Rate (AMR) speech codec for use in TETRA,» [Ηλεκτρονικό]. Available: https://www.etsi.org/deliver/etsi_tr/101900_101999/101977/01.01.01_60/tr_101977v010101p.pdf. [Πρόσβαση 17 11 2022].

[250] P. Stavroulakis, TErrestrial Trunked RAdio - TETRA "A Global Security Tool", Chania: Springer,

2007.

[251] A. K. Salkintzis, «Evolving Public Safety Communication Systems by Integrating WLAN and TETRA Networks,» *IEEE Communications Magazine,* pp. 38-46, 2006.

[252] K. Ammons, «www.powertrunk.com,» [Ηλεκτρονικό]. Available: https://www.powertrunk.com/docs/Pros_and_Cons_of_P25_vs_TETRA.pdf. [Πρόσβαση 04 01 2023].

[253] O. Arrhenius, «Ubiquitous Public Safety Communications,» EADS Defence and Security, 2009.

[254] Radio Resource Mission Critical Communications, «ETSI Releases New Algorithms to Secure TETRA Networks,» 8 November 2022. [Ηλεκτρονικό]. Available: https://www.rrmediagroup.com/News/NewsDetails/NewsID/21885. [Πρόσβαση November 2022].

[255] «ETSI - Mobile and Private Mobile Radio,» ETSI, [Ηλεκτρονικό]. Available: https://www.etsi.org/technologies/mobile-radio?jjj=1673108047189. [Πρόσβαση 04 01 2023].

[256] «dmrassociation.org,» Digital Mobile Radio Association, DMR, [Ηλεκτρονικό]. Available: https://www.dmrassociation.org/dmr-standards.html. [Πρόσβαση 07 01 2023].

[257] ETSI - TECHNICAL SPECIFICATION, «Electromagnetic compatibility and Radio spectrum Matters (ERM), Digital Mobile Radio (DMR) Systems, Part 4: DMR trunking protocol,» ETSI, Valbonne, 2021.

[258] Caltta Technologies (ZTE), «DMR Trunking Technology White Paper,» Caltta Technologies, 2021.

[259] «Understanding AIS – the DMR Application Interface Specification,» Catalist - Communications Technologies, 23 12 2016. [Ηλεκτρονικό]. Available: https://blog.catcomtec.com/2016/12/23/understanding-ais-the-dmr-application-interface-specification/. [Πρόσβαση 07 01 2023].

[260] SA Forum, «Service Availability Interface - SAI-Overview-B.05.03,» Service Availability Forum, 2011.

[261] DMR Association , «BENEFITS OF DMR White Paper,» DMR Association, 2010.

[262] «Product Showcase,» DMR Association, [Ηλεκτρονικό]. Available: https://www.dmrassociation.org/product-showcase.html. [Πρόσβαση 07 01 2023].

[263] D. Kuypers και M. Schinnenburg, «Traffic Performance Evaluation of Data Links in TETRA and TETRAPOL,» *11th European Wireless Conference 2005 - Next Generation wireless and Mobile Communications and Services,* April 2005.

[264] TETRAPOL, «Tetrapol / Markets and trends,» TETRAPOL, [Ηλεκτρονικό]. Available: https://www.tetrapol.com/markets_and_trends/references/. [Πρόσβαση 07 01 2023].

[265] P. Jacques, «Tetrapol technology underpins security at Brazil World Cup,» *Police Professional,* 23 July 2014.

[266] International Telecommunication Union , «Report ITU-R M.2014-3 - Digital land mobile systems for dispatch traffic,» ITU-Radiocommunication Sector , Geneva, 2017.

[267] NXDN Forum, «The history of NXDN™,» [Ηλεκτρονικό]. Available: http://www.nxdn-forum.com/what-is-nxdn/history/. [Πρόσβαση 07 01 2023].

[268] Mission Critical Communications, «ITU-R Accepts NXDN Common Air Interface,» Mission Critical Communications, 29 03 2017. [Ηλεκτρονικό]. Available: https://www.rrmediagroup.com/News/NewsDetails/NewsID/15362. [Πρόσβαση 07 01 2023].

[269] Icom Inc., «ICOM DIGITAL ADVANCED SYSTEM,» 2009. [Ηλεκτρονικό]. Available: http://www.icomcanada.com/idas/system/idas.pdf. [Πρόσβαση 07 01 2023].

[270] NXDN Forum, «Who are our members?,» [Ηλεκτρονικό]. Available: http://www.nxdn-forum.com/our-members/who-are-members/. [Πρόσβαση 07 01 2023].

[271] ETSI - TECHNICAL SPECIFICATION, «Digital Private Mobile Radio (dPMR) using FDMA with a channel spacing of 6,25 kHz,» 01 2019. [Ηλεκτρονικό]. Available: https://www.etsi.org/deliver/etsi_ts/102600_102699/102658/02.06.01_60/ts_102658v020601p.pdf. [Πρόσβαση 07 01 2023].

[272] ETSI - TECHNICAL SPECIFICATION, «TS 102 490 - Electromagnetic compatibility and Radio spectrum Matters (ERM), Peer-to-Peer Digital Private Mobile Radio using FDMA with a channel spacing of 6,25 kHz with e.r.p. of up to 500 mW,» 08 2016. [Ηλεκτρονικό]. Available: https://www.etsi.org/deliver/etsi_ts/102400_102499/102490/01.09.01_60/ts_102490v010901p.pdf. [Πρόσβαση 07 01 2023].

[273] dPMR Association, «dPMR Association,» [Ηλεκτρονικό]. Available: https://dpmrassociation.org/. [Πρόσβαση 07 01 2023].

[274] dPMR Association, «About Us,» dPMR Association, [Ηλεκτρονικό]. Available: https://dpmrassociation.org/about-dpmr-association.html. [Πρόσβαση 07 01 2023].

[275] dPMR Association, «Case Studies,» dPMR Association, [Ηλεκτρονικό]. Available: https://dpmrassociation.org/dpmr-case-studies-home.html. [Πρόσβαση 07 01 2023].

[276] I. Ozimek και G. Kandus, «Using TETRA for Remote Control, Supervision and Electricity Metering in an Electric Power Distribution System,» *ResearchGate,* pp. 289-299, April 2008.

[277] teltronic, «P25 and TETRA, comparative analysis of the two technologies that revolutionized critical communications,» teltronic, 19 11 2020. [Ηλεκτρονικό]. Available: https://www.teltronic.es/en/p25-

and-tetra-comparative-analysis-of-the-two-technologies-that-revolutionized-critical-communications/. [Πρόσβαση 07 01 2023].

[278] Mission Critical Communications, «A TETRA and DMR Comparison,» Mission Critical Communications, 01 04 2010. [Ηλεκτρονικό]. Available: https://www.rrmediagroup.com/Features/FeaturesDetails/FID/174. [Πρόσβαση 07 01 2023].

[279] tait Communications , «TECHNOLOGY COMPARISON - Comparing Voice Coverage: DMR and TETRA,» tait Communications , 2020.

[280] K. O. Olasupo, I. Kostanic, T. O. Olasupo και H. Alshamsi, «Investigation of the impact of heterogeneous traffic on performance of LTE-based mission critical communication networks,» σε *8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada, 2017.

[281] ETSI Technical Specification, «ETSI TS 100 392-2 - Terrestrial Trunked Radio (TETRA), Voice plus Data (V+D), Part 2: Air Interface (AI),» 10 2011. [Ηλεκτρονικό]. Available: https://www.etsi.org/deliver/etsi_ts/100300_100399/10039202/03.05.01_60/ts_10039202v030501p.pdf. [Πρόσβαση 07 01 2023].

[282] M. Nouri, V. Lottici, R. Reggiannini, D. Ball και M. Rayne, «TEDS: A High Speed Digital Mobile Communication Air Interface for Professional Users,» *IEEE Vehicular Technology Magazine,* τόμ. 1, αρ. 4, pp. 32 - 42, December 2006.

[283] M. Edwards, «TETRA Release 2.0 Overview,» Motorola CGISS European System Design Centre, 2003.

[284] Motorola Solutions, «Tetra Mission Critical Communications Solutions,» [Ηλεκτρονικό]. Available: https://www.motorolasolutions.com/content/dam/msi/docs/products/dimetra-tetra/brochures/tetra_mission_critical_communications_solutions_web.pdf. [Πρόσβαση January 2023].

[285] MOTOROLA SOLUTIONS / PUBLIC SAFETY, «SAFER AND TRUSTED CITIES,» Motorola Solutions, [Ηλεκτρονικό]. Available: https://video.motorolasolutions.com/detail/videos/public-safety/video/6274480244001/safer-and-trusted-cities?autoStart=true. [Πρόσβαση 07 01 2023].

[286] M. Steppler, P. Sievering, S. Kerkhoff και T. Gray, «Evolution of TETRA To a 4G All-IP Broadband Mission Critical Voice Plus Data Professional Mobile Radio Technology - WHITE PAPER,» P3 Communications GmbH, 2011.

[287] ETSI, «ETSI Technical Report 170 002 - Project MESA, Service Specification Group - Services and Applications, Definitions, symbols and abbreviations,» ETSI, 2002.

[288] ETSI, «ETSI Technical Specification 170 001 - Project MESA, Service Specification Group - Services and Applications,Statement of Requirements (SoR),» ETSI, 2006.

[289] ETSI, «ETSI Technical Specification 170 016 - Project MESA, Technical Specification Group - System, Functional Requirements Definition,» ETSI, 2009.

[290] ETSI & TIA, «Public Safety Partnership Project for Mobile Broadband Services MESA projectmesa,» 27 04 2001. [Ηλεκτρονικό]. Available: https://www.slideserve.com/pia/public-safety-partnership-project-for-mobile-broadband-services-mesa-projectmesa. [Πρόσβαση 07 01 2023].

[291] D. Thompson, «Project MESA - Broadband Mobility for Emergency and Safety Applications,» σε *2004 Wireless Broadband Forum*, Washington, USA, 2004.

[292] kbvresearch.com, «Global Terrestrial Trunked Radio (TETRA) System Market Size, Share & Industry Trends Analysis Report By Component (Hardware and Software), By Device, By Modes of Operation, By End User, By Regional Outlook and Forecast, 2021 - 2027,» 03 2022. [Ηλεκτρονικό]. Available: https://www.kbvresearch.com/terrestrial-trunked-radio-system-market/. [Πρόσβαση 07 01 2023].

[293] M. B. Simi, «Feasibility of Long Term Evolution (LTE) as Technology for Public Safety,» σε *20th Telecommunications FORUM TELFOR 2012*, Belgrade, Serbia, 2012.

[294] FirstNet Authority, «FirstNet: The History of our Nation's Public Safety Network,» FirstNet Authority, [Ηλεκτρονικό]. Available: https://www.firstnet.gov/about/history. [Πρόσβαση 07 01 2023].

[295] FirstNet Authority, «The 9/11 commission report,» 2004. [Ηλεκτρονικό]. Available: https://govinfo.library.unt.edu/911/report/911Report.pdf. [Πρόσβαση 07 01 2023].

[296] FirstNet Authority, «A Decade of Accomplishments - FISCAL YEAR 2021 ANNUAL REPORT TO CONGRESS,» FirstNet Authority, 2022.

[297] D. Jackson, «FirstNet Authority pursuing new CEO, Band 14 buildout, spectrum-license renewal,» IWCE's Urgent Communications Magazine, 16 11 2022. [Ηλεκτρονικό]. Available: https://urgentcomm.com/2022/11/16/firstnet-authority-pursuing-new-ceo-band-14-buildout-spectrum-license-renewal/. [Πρόσβαση 07 01 2023].

[298] D. Ramey, «FirstNet Authority Files Band 14 License Renewal Application,» *Mission Critical Communications,* 25 August 2022.

[299] S. Schwartz, «FirstNet & 5G: Reliably Connecting First Responders to Help Save Lives,» AT&T Blog, 31 08 2022. [Ηλεκτρονικό]. Available: https://about.att.com/blogs/2022/firstnet-schwartz.html. [Πρόσβαση 07 01 2023].

[300] J. I. Zahid, F. Hussain και A. Ferworn, «A Model of Computing and Communication for Public Safety Integrating FirstNet, Edge Computing, and Internet of Things,» *IEEE Xplore,* pp. 619 - 623, 4 July 2019.

[301] J. D. Kahn, «Process Document for the NIST List of Certified Devices,» National Institute of Standards and Technology (NIST), 09 01 2023. [Ηλεκτρονικό]. Available: https://www.nist.gov/ctl/pscr/process-document-nist-list-certified-devices. [Πρόσβαση 17 01 2023].

[302] FirstNet Authority, «Emergency Management,» FirstNet Authority, [Ηλεκτρονικό]. Available: https://www.firstnet.gov/public-safety/firstnet-for/emergency-management. [Πρόσβαση 07 01 2023].

[303] FirstNet Built with AT&T, «APPS CATALOG,» FirstNet Built with AT&T, [Ηλεκτρονικό]. Available: https://apps.firstnet.att.com/?auth=false. [Πρόσβαση 07 01 2023].

[304] FirstNet Authority, «EMERGENCY MANAGEMENT RESOURCE GUIDE,» FirstNet Authority, 2022.

[305] K. Nida, *FirstNet Authority Differentiators and Roadmap,* FirstNet Authority, 2019.

[306] IPLOOK Technologies Co., Limited, «IPLOOK EPC PRODUCT DESCRIPTION,» 01 February 2020. [Ηλεκτρονικό]. Available: https://www.iplook.com/products/evolved-packet-core?gclid=Cj0KCQiAq5meBhCyARIsAJrtdr7OUNzQQQP_-WJnK8_DUHErwHGePkdWyU_JKvflbbBUpBR6z3dkj4saAmVwEALw_wcB. [Πρόσβαση 07 01 2023].

[307] IPLOOK Technologies Co., Limited, «IPLOOK IMS PRODUCT DESCRIPTION,» 24 01 2022. [Ηλεκτρονικό]. Available: https://www.iplook.com/products/ip-multimedia-subsystem?gclid=Cj0KCQiAq5meBhCyARIsAJrtdr7SEa5TWzbF6NoxuJApgZQYO9btYdzJp-VDNPABbfwV61-RJXWrhckaAtErEALw_wcB. [Πρόσβαση 07 01 2023].

[308] «700 MHz Public Safety Spectrum,» Federal Communications Commission, 19 06 2020. [Ηλεκτρονικό]. Available: https://www.fcc.gov/700-mhz-public-safety-narrowband-spectrum. [Πρόσβαση 07 01 2023].

[309] FirstNet Authority, «FirstNet Deployable Fleet,» FirstNet Authority, [Ηλεκτρονικό]. Available: https://www.firstnet.gov/network/TT/deployables. [Πρόσβαση 07 01 2023].

[310] FirstNet Built with AT&T, «CRD for FirstNet,» FirstNet Built with AT&T, [Ηλεκτρονικό]. Available: https://www.firstnet.com/coverage/coverage-enhancements/compact-rapid-deployable.html. [Πρόσβαση 07 01 2023].

[311] A. Weissberger, «AT&T introduces 5G Flying COWs (Cell on Wings) drones,» IEEE Communication Society, 22 06 2022. [Ηλεκτρονικό]. Available: https://techblog.comsoc.org/2022/06/22/att-introduces-5g-flying-cows-cell-on-wings-drones/.

[Πρόσβαση 07 01 2023].

[312] FirtsNet Built with AT&T, *Press Release - FirstNet & 5G: An Experience Unlike Anything Else for America's First Responders,* DALLAS, USA: FirtsNet Built with AT&T, 2021.

[313] NOKIA, «5G spectrum bands explained — low, mid and high band,» NOKIA, [Ηλεκτρονικό]. Available: https://www.nokia.com/networks/insights/spectrum-bands-5g-world/. [Πρόσβαση 07 01 2023].

[314] A. Jasso, «AT&T 5G NETWORK: BANDS, COVERAGE, 5G VS 5G+, PLANS, AND MORE,» Wilson Amplifiers, 12 10 2022. [Ηλεκτρονικό]. Available: https://www.wilsonamplifiers.com/blog/att-5g-network-bands-coverage-5g-vs-5g-plans-and-more/. [Πρόσβαση 07 01 2023].

[315] FirstNetME, «FirstNet In Action,» FirstNetME, [Ηλεκτρονικό]. Available: https://firstnetme.gov/case-studies/index.html. [Πρόσβαση 07 01 2023].

[316] FirstNet, «10 WAYS FIRSTNET WILL HELP PUBLIC SAFETY SAVE LIVES AND SECURE COMMUNITIES,» [Ηλεκτρονικό]. Available: https://2014-2018.firstnet.gov/sites/default/files/Ten_Ways_FirstNet_Helps_180427.pdf. [Πρόσβαση 07 01 2023].

[317] L. G. Kruger, «The First Responder Network (FirstNet) and Next Generation Communications for Public Safety: Issues for Congress,» Congressional Research Service, 2017.

[318] T. Murdock, «Supporting Marshall Fire Responders with Priority Service and On-Demand Coverage,» FirstNet Authority, 02 03 2022. [Ηλεκτρονικό]. Available: https://www.firstnet.gov/newsroom/blog/supporting-marshall-fire-responders-priority-service-and-demand-coverage. [Πρόσβαση 07 01 2023].

[319] G. B. McCarraher, «No turbulence for FirstNet at Rhode Island airport exercise and drill,» FirstNet Authority, 06 02 2020. [Ηλεκτρονικό]. Available: https://www.firstnet.gov/newsroom/blog/no-turbulence-firstnet-rhode-island-airport-exercise-and-drill. [Πρόσβαση 07 01 2023].

[320] L3Harris Technologies, «CITY OF PARMA FirstNet CONNECTIVITY - Case Study,» L3Harris Technologies, Parma, Cleveland, USA, 2019.

[321] Broadmap, «About BroadMap,» [Ηλεκτρονικό]. Available: http://www.broadmap.eu/. [Πρόσβαση 10 01 2023].

[322] BroadWay, «BroadWay,» [Ηλεκτρονικό]. Available: https://www.broadway-info.eu. [Πρόσβαση 10 01 2023].

[323] BroadWay, «Consortium A Lead Contractor: Airbus DS,» 02 2020. [Ηλεκτρονικό]. Available:

https://www.broadway-info.eu/consortium-a-airbus-2/. [Πρόσβαση 10 01 2023].

[324] BroadWay, «Consortium B Lead Contractor: Frequentis,» 02 2020. [Ηλεκτρονικό]. Available: https://www.broadway-info.eu/consortium-b-frequentis-design/. [Πρόσβαση 10 01 2023].

[325] BroadWay, «Consortium C Lead Contractor: Leonardo,» 02 2020. [Ηλεκτρονικό]. Available: https://www.broadway-info.eu/consortium-c-leonardo-2/. [Πρόσβαση 10 01 2023].

[326] BroadWay, «Consortium D Lead Contractor: Rohill Technologies,» 02 2020. [Ηλεκτρονικό]. Available: https://www.broadway-info.eu/consortium-d-rohill/. [Πρόσβαση 10 01 2023].

[327] BroadWay, «BroadWay Pilot #1 - Ljubljana (Slovenia),» 08 06 2022. [Ηλεκτρονικό]. Available: https://www.broadway-info.eu/forest-fire-pilot-slovenia/. [Πρόσβαση 10 01 2023].

[328] BroadWay, «BroadWay Pilot #2 - Kerkrade (The Netherlands),» 30 06 2022. [Ηλεκτρονικό]. Available: https://www.broadway-info.eu/drug-smuggling-pilot-nl/. [Πρόσβαση 10 01 2023].

[329] BroadWay, «BroadWay Pilot #3 - Malaga (Spain),» 21 07 2022. [Ηλεκτρονικό]. Available: https://www.broadway-info.eu/ferry-fire-pilot-spain/. [Πρόσβαση 10 01 2023].

[330] BroadWay και D. Lund, «BroadWay to BroadNet The Full Story,» σε *PSCE Conference*, Salzburg, 2022.

[331] BroadWay, «SpiceNet Reference Architecture,» BroadWay, [Ηλεκτρονικό]. Available: https://www.broadway-info.eu/spicenet/. [Πρόσβαση 10 01 2023].

[332] T. Kourtis και M. Batistatos, «D2.2 System Specifications and Architecture,» Respond-A, 2021.

[333] J. Meseguer, D. Calduch και R. Company, «D2.3 Use Cases and Evaluation Strategy,» Respond-A, 2021.

[334] Respond-A, «Use Case 1- Forest Fires,» Respond-A, 19 10 2021. [Ηλεκτρονικό]. Available: https://respond-a-project.eu/use-case-1/. [Πρόσβαση 10 01 2023].

[335] Respond-A, «Use Case 2- Earthquake,» Respond-A, 22 09 2022. [Ηλεκτρονικό]. Available: https://respond-a-project.eu/use-case-2/. [Πρόσβαση 10 01 2023].

[336] K. Kanchanasut, A. Tunpan, M. A. Awal, D. K. Das, T. Wongsaardsakul και Y. Tsuchimoto, «A Multimedia Communication System for Collaborative Emergency Response Operation in Disaster-affected Areas,» *Internet Education and Research Laboratory (intERLab) Asian Institute of Technology (AIT),* January 2007.

[337] S. M. George, W. Zhou, H. Chenji, M. Won, Y. O. Lee, A. Pazarloglou και R. Stoleru, «DistressNet: A Wireless Ad Hoc and Sensor Network Architecture for Situation Management in Disaster Response,» *IEEE Communications Magazine,* pp. 128 - 136, March 2010.

[338] H. Chenji, W. Zhang, M. Won, R. Stoleru και C. Arnett, «A Wireless System for Reducing Response Time in Urban Search & Rescue,» σε *2012 IEEE 31st International Performance Computing and Communications Conference (IPCCC)*, Austin, USA, 2012.

[339] A. Meissner, Z. Wang, W. Putz και J. Grimmer, «MIKoBOS - A Mobile Information and Communication System for Emergency Response,» σε *3rd International ISCRAM Conference*, Newark, USA, 2006.

[340] N. Ahmed, K. Jamshaid και O. Z. Khan, «SAFIRE:A Self-OrganizingArchitecturefor InformationExchangebetween FirstResponders,» σε *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, San Diego, USA, 2007.

[341] G. Iapichino, C. Bonnet, O. del Rio Herrero, C. Baudoin και I. Buret, «Advanced Hybrid Satellite and Terrestrial System Architecture for Emergency Mobile Communications,» σε *26th International Communications Satellite Systems Conference (ICSSC)*, San Diego, USA, 2008.

[342] N. Li , M. Su, Z. Bi, Z. Su και C. Wang, «A new methodology to support group decision-making for IoT-based emergency response systems,» *Springer,* pp. 953-977, 26 January 2013.

[343] L. Lenert, T. C. Chan, W. Griswold, J. Killeen, D. Palmer, D. Kirsh, R. Mishra και R. Rao, «WiMesh: Leveraging Mesh Networking For Disaster Communication in Poor Regions of the World,» *Networking and Internet Architecture,* 3 January 2021.

[344] J. T. B. FAJARDO και C. M. OPPUS, «A Mobile Disaster Management System Using the Android Technology,» *WSEAS TRANSACTIONS on COMMUNICATIONS,* pp. 343-353, June 2010.

[345] L. Lenert, T. C. Chan, W. Griswold, J. Killee, D. Palmer, D. Kirsh, R. Mishr και R. Rao, «Wireless Internet Information System for Medical Response in Disasters (WIISARD),» σε *AMIA 2006 Symposium Proceedings*.

[346] R. E. Carella και S. P. McGrath, «ARTEMIS Personal Area Networks for Emergency Remote Triage and Information Management,» σε *3rd International ISCRAM Conference*, Newark, USA, 2006.

[347] J. KO, J. . H. LIM, Y. CHEN, R.˘ Z. MUSA˘ LOIU, A. TERZIS, G. M. MASSON, T. GAO, W. DESTLER, L. SELAVO και R. P. DUTTON, «MEDiSN: Medical Emergency Detection in Sensor Networks,» *ACM Transactions on Embedded Computing Systems,* τόμ. 10, αρ. 1, 2010.

[348] E. C. Kyriacou, C. S. Pattichis και M. S. Pattichis, «An Overview of Recent Health Care Support Systems for eEmergency and mHealth Applications,» σε *31st Annual International Conference of the IEEE EMBS*, Minneapolis, USA, 2009.

[349] T. Gao, T. Massey, L. Selavo, D. Crawford, B.-r. Chen, K. Lorincz, V. Shnayder, L. Hauenstein, F. Dabiri, J. Jeng, A. Chanmugam, D. White, M. Sarrafzadeh και M. Welsh, «The Advanced Health

and Disaster Aid Network: A Light-Weight Wireless Medical System for Triage,» *IEEE TRANSACTIONS ON BIOMEDICAL CIRCUITS AND SYSTEMS,* τόμ. 1, αρ. 3, pp. 203-216, 2007.

[350] T. Gao , C. Pesto , L. Selavo , Y. Chen, J. Ko, J. Lim, A. Terzis, A. Watt, J. Jeng, B. r. Chen, K. Lorincz και M. Welsh , «Wireless Medical Sensor Networks in Emergency Response: Implementation and PilotResults,» σε *2008 IEEE Conference on Technologies for Homeland Security*, Waltham, USA, 2008.

[351] T. C. Chan, J. Killeen, W. Griswold και L. Lenert, «Information Technology and Emergency Medical Care during Disasters,» *ACAD EMERG MED,* τόμ. 11, αρ. 11, pp. 1229-1235, 2004.

[352] T. Gao, D. Greenspan, M. Wels, R. R. Juang και A. Alm, «Vital Signs Monitoring and Patient Tracking Over a Wireless Network,» σε *Engineering in Medicine and Biology 27th Annual Conference*, Shanghai, China, 2005.

[353] Y. ZHANG, N. ANSARI και H. TSUNODA, «WIRELESS TELEMEDICINE SERVICES OVER INTEGRATED IEEE 802.11/WLAN AND IEEE 802.16/WIMAX NETWORKS,» *IEEE Wireless Communications,* pp. 30-36, 2010.

[354] E. A. Fry και L. A. Lenert, «MASCAL: RFID Tracking of Patients, Staff and Equipment to Enhance Hospital Response to Mass Casualty Events,» σε *AMIA 2005 Symposium*, 2005.

[355] P. Lukowicz, J. Ward, G. Tro¨ster, E. Hirt και C. Neufelt, «AMON: A Wearable Medical Computer for High Risk Patients,» σε *6th International Symposium on Wearable Computers (ISWCi02)*, 2002.

[356] S. Pavlopoulos, E. Kyriacou, A. Berler, S. Dembeyiotis και D. Koutsouris, «A NOVEL EMERGENCY TELEMEDICINE SYSTEM BASED ON WIRELESS COMMUNICATION TECHNOLOGY -“AMBULANCE”,» *IEEE Transactions on Information Technology in Biomedicine,* τόμ. 2, αρ. 4, 1998.

[357] P. Gardner-Stephen, «The Serval Project: Practical Wireless Ad-Hoc Mobile Telecommunications,» *ITU,* 22 July 2011.

[358] «ITU,» [Ηλεκτρονικό]. Available: https://www.itu.int/en/mediacentre/backgrounders/Pages/Non-geostationary-satellite-systems.aspx. [Πρόσβαση 28 12 2022].

[359] "Iridiumwhere.com. [Online]. Available: https://iridiumwhere.com/about/. [Accessed: 27-Dec-2022].," Iridium, [Online]. Available: https://iridiumwhere.com/about/. [Accessed 27 12 2022].

[360] «Microwave Journal,» [Ηλεκτρονικό]. Available: https://www.microwavejournal.com/articles/38970-the-globalstar-big-leo-satellite-system-for-near-global-satellite-communications. [Πρόσβαση 27 12 2022].

[361] «axessnet,» [Ηλεκτρονικό]. Available: https://axessnet.com/en/differences-between-bgan-and-vsat/.

[Πρόσβαση 27 12 2022].

[362] J. C. a. V. C. L.L. Dai, "``Communication satellites Technologies and systems"," *Encyclopedia of Life Support Systems,* 2007.

[363] T. Hatt, «gsmaintelligence,» 06 2021. [Ηλεκτρονικό]. Available: https://data.gsmaintelligence.com/research/research/research-2021/radar-connectivity-from-the-sky. [Πρόσβαση 28 12 2022].

[364] T.-M. newsroom, «T-Mobile,» T-Mobile - SpaceX, 25 08 2022. [Ηλεκτρονικό]. Available: https://www.t-mobile.com/news/un-carrier/t-mobile-takes-coverage-above-and-beyond-with-spacex. [Πρόσβαση 29 12 2022].

[365] A. support, «APPLE,» APPLE, [Ηλεκτρονικό]. Available: https://support.apple.com/en-us/HT213426. [Πρόσβαση 29 12 2022].

[366] F. A. D'Oliveira, F. C. L. d. Melo και T. C. Devezas, «High-altitude platforms - present situation and technology trends,» *Journal of Aerospace Technology and Management,* pp. 249-262, 2016.

[367] G. Karabulut Kurt, M. G. Khoshkholgh, S. Alfattani, A. Ibrahim, T. S. J. Darwish, M. S. Alam, H. Yanikomeroglu και A. Yongacoglu, «A vision and framework for the high altitude platform station (HAPS) networks of the future,» *IEEE Communications Surveys & Tutorials,* pp. 729-779, 2021.

[368] M. Y. Abdelsadek, A. U. Chaudhry, T. Darwish, E. Erdogan, G. Karabulut-Kurt, P. G. Madoery, O. B. Yahia και H. Yanikomeroglu, «Future space networks: Toward the next giant leap for humankind (invited paper),» *IEEE transactions on communications,* pp. 1-1, 2022.

[369] S. Alfattani, W. Jaafar, H. Yanikomeroglu και A. Yongacoglu, «Multi-mode high altitude platform stations (HAPS) for next generation wireless networks,» 2022.

[370] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas και H. Yanikomeroglu, «HAPS selection for hybrid RF/FSO satellite networks,» 2021.

[371] S. Euler, X. Lin, E. Tejedor και E. Obregon, «High-altitude platform stations as international mobile telecommunications base stations: A primer on HIBS,» *IEEE vehicular technology magazine, Volume 17, Issue 4,* pp. 92-100, 2022.

[372] ITU, «itu.int,» ITU, [Ηλεκτρονικό]. Available: https://www.itu.int/pub/R-REP-F.2438-2018. [Πρόσβαση 01 01 2023].

[373] 3. T. R. m. #94-3, «3GPP,» December 2021. [Ηλεκτρονικό]. Available: https://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_94e/Docs/RP-213691.zip. [Πρόσβαση 02 01 2023].

[374] ITU, «International Telecommunication Union,» ITU, 03 2021. [Ηλεκτρονικό]. Available:

https://www.itu.int/en/mediacentre/backgrounders/Pages/emergency-telecommunications.aspx. [Πρόσβαση 04 01 2023].

[375] X.Company, «X.COMPANY,» X.COMPANY - ALPHABET, 22 01 2021. [Ηλεκτρονικό]. Available: https://blog.x.company/loons-final-flight-e9d699123a96. [Πρόσβαση 04 01 2023].

[376] GSMA, «GSMA,» 9 02 2022. [Ηλεκτρονικό]. Available: https://www.gsma.com/futurenetworks/resources/high-altitude-platform-systems-towers-in-the-skies-version-2-0/. [Πρόσβαση 04 01 2023].

[377] P. Correa, «AIRBUS,» AIRBUS, 24 10 2022. [Ηλεκτρονικό]. Available: https://www.airbus.com/en/newsroom/press-releases/2022-10-airbus-and-salam-join-forces-for-high-altitude-platform-station. [Πρόσβαση 04 01 2023].

[378] «UAVISION,» Lockheed Martin, 18 02 2022. [Ηλεκτρονικό]. Available: https://www.uasvision.com/2022/04/12/lockheed-martin-stalker-vxe-uas-completes-a-world-record-39-hour-flight/. [Πρόσβαση 04 01 2023].

[379] «tao-group.de,» TAO GROUP, [Ηλεκτρονικό]. Available: https://www.tao-group.de/en_hap_fuer_telekommunikation.html. [Πρόσβαση 04 01 2023].

[380] «RosAeroSystems.com,» Augur RosAeroSystems, 2010. [Ηλεκτρονικό]. Available: http://rosaerosystems.com/projects/obj687. [Πρόσβαση 04 01 2023].

[381] «thalesgroup.com,» Thales Alenia Space, [Ηλεκτρονικό]. Available: https://www.thalesgroup.com/en/worldwide/space/press-release/thales-alenia-space-and-thales-sign-concept-study-contract-french. [Πρόσβαση 04 01 2023].

[382] H. S. A. W. H. Hariyanto, "Emergency broadband access network using low altitude platform," in *Proceedings of the International Conference on Instrumentation, Communications,Information Technology, and Biomedical Engineering (ICICI-BME)*, Bandung, Indonesia, 2009.

[383] B. E. Y. Belmekki και M.-S. Alouini, «Unleashing the potential of networked Tethered Flying Platforms for B5G/6G: Prospects, challenges, and applications,» 10 03 2020.

[384] «Windfair,» Altaeros, 12 11 2014. [Ηλεκτρονικό]. Available: https://w3.windfair.net/wind-energy/news/17116-what-s-new-in-the-windfair-world-the-altaeros-buoyant-airborne-wind-turbine. [Πρόσβαση 08 01 2023].

[385] P. Williams, B. Lansdorp και W. Ockesl, «Optimal crosswind towing and power generation with tethered kites,» *Journal of guidance, control, and dynamics: a publication of the American Institute of Aeronautics and Astronautics devoted to the technology of dynamics and control,* pp. 81-93, 2008.

[386] M. L. Loyd, «Crosswind kite power (for large-scale wind power production),» *Journal of energy,*

τόμ. 4, αρ. 3, pp. 106-111, 1980.

[387] «Allsopp,» Allsopp, [Ηλεκτρονικό]. Available: http://www.allsopp.co.uk/index.php?mod=page&id_pag=35. [Πρόσβαση 08 01 2023].

[388] «Hybrid Air vehicles,» Hybrid Air vehicles, [Ηλεκτρονικό]. Available: https://www.hybridairvehicles.com/our-aircraft/faq/#HAV1. [Πρόσβαση 08 01 2023].

[389] Y. K. K. M. S. Y. a. H. M. H. Suzuki, «"An Ad Hoc Network in the Sky, SKYMESH, for Large-Scale Disaster Recovery,",» Montreal, QC, Canada,, 2006.

[390] A. Qiantori, A. B. Sutiono, H. Hariyanto, H. Suwa και T. Ohta, «An emergency medical communications system by low altitude platform at the early stages of a natural disaster in Indonesia,» *Journal of medical systems,* pp. 41-52, 2012.

[391] «astynomia,» Υπουργείο Δημόσιας Τάξης, 2004. [Ηλεκτρονικό]. Available: https://www.astynomia.gr/images/stories/Attachment13839_OLYMPIC_SECURITY_EGL0408.pdf. [Πρόσβαση 15 01 2023].

[392] «Πολίτης,» 29 7 2019. [Ηλεκτρονικό]. Available: https://www.politischios.gr/politiki/samos-epitukhemene-dokime-tou-aeroploiou-gia-ten-epiterese-ton-sunoron. [Πρόσβαση 15 01 2023].

[393] «SVB24,» SVB, [Ηλεκτρονικό]. Available: https://www.svb24.com/en/guide/everything-there-is-to-know-about-ais.html#:~:text=AIS%20stands%20for%20Automatic%20Identification,traffic%20centres%20on%20the%20coast.. [Πρόσβαση 15 01 2023].

[394] Γ. Σουλιώτης, «Καθημερινή,» ΚΑΘΗΜΕΡΙΝΕΣ ΕΚΔΟΣΕΙΣ ΜΟΝΟΠΡΟΣΩΠΗ Α.Ε., 15 07 2021. [Ηλεκτρονικό]. Available: https://www.kathimerini.gr/society/561434116/ypersygchrona-zepelin-sta-synora/. [Πρόσβαση 15 01 2023].

[395] «ERDMAGAZINE,» ERD, 02 09 2021. [Ηλεκτρονικό]. Available: https://www.edrmagazine.eu/cnim-air-space-and-in-innovative-navigation-gmbh-have-deployed-two-maritime-airborne-surveillance-aerostat-systems-for-frontex-innovation-pilot-project-in-greece. [Πρόσβαση 15 01 2023].

[396] TCCA, «TCCA White Paper Mission-Critical Broadband Device Procurement,» TCCA, 2021.

[397] D. Stockton, «Best smartphones for public safety officers: 10 important factors,» Insights Samsung, 13 07 2021. [Ηλεκτρονικό]. Available: https://insights.samsung.com/2021/07/13/best-smartphones-for-public-safety-officers-10-important-factors/. [Πρόσβαση 11 02 2023].

[398] S. Saafi, J. Hosek και A. Kolackova, «Enabling Next-Generation Public Safety Operations with Mission-Critical Networks and Wearable Applications,» *sensors,* τόμ. 21, p. 16, 2021.

[399] D. Stockton, «9 ways wearables support smarter policing and officer safety,» 19 11 2019. [Ηλεκτρονικό]. Available: https://insights.samsung.com/2019/11/12/9-ways-wearables-support-smarter-policing-and-officer-safety-2/. [Πρόσβαση 11 02 2023].

[400] S. Scheurer, S. Tedesco, K. N. Brown και B. O'Flynn, «Human Activity Recognition for Emergency First Responders via Body-Worn Inertial Sensors,» σε *2017 IEEE 14th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, Eindhoven, Netherlands, 2017.

[401] D. Dias και J. P. . S. Cunha, «Wearable Health Devices—Vital Sign Monitoring, Systems and Technologies,» *sensors,* τόμ. 18, αρ. 8, p. 28, 2018.

[402] G. Appelboom, E. Camacho, M. E. Abraham, S. . S. Bruce, E. L. Dumont, B. E. Zacharia, R. D'Amico, J. Slomian, J. . Y. Reginster, O. Bruyère και S. Connolly Jr, «Smart wearable body sensors for patient self-assessment and monitoring,» *ARCHIVES OF PUBLIC HEALTH,* τόμ. 72, αρ. 28, p. 9, 2014.

[403] Motorola Solutions, «Police Body Cameras,» [Ηλεκτρονικό]. Available: https://www.motorolasolutions.com/en_us/video-security-access-control/body-worn-cameras/v300.html. [Πρόσβαση 11 02 2023].

[404] Samsung, «Public safety wearables,» [Ηλεκτρονικό]. Available: https://www.samsung.com/us/business/solutions/industries/public-safety/smartwatches-wearables/. [Πρόσβαση 11 02 2023].

[405] J. Careless, «5 ways a rugged smartphone keeps first responders connected and safe,» 19 04 2019. [Ηλεκτρονικό]. Available: https://www.police1.com/sponsored-article/articles/5-ways-a-rugged-smartphone-keeps-first-responders-connected-and-safe-r0bXSs5VqjbdSXZS/. [Πρόσβαση 11 02 2023].

[406] B. Tournier, «What is the Internet of Life Saving Things (IoLST)?,» Sierra Wireless, 03 12 2018. [Ηλεκτρονικό]. Available: https://www.sierrawireless.com/iot-blog/internet-of-life-saving-things/. [Πρόσβαση 12 02 2023].

[407] S. Chitturi, «Mission Critical Services Standards: Advancing Critical Communications Across Industries,» 31 08 2021. [Ηλεκτρονικό]. Available: https://www.samsung.com/global/business/networks/insights/blog/0831-mission-critical-services-standards-advancing-critical-communications-across-industries/. [Πρόσβαση 12 02 2023].

[408] ETSI, «Mission Critical Video over LTE - ETSI TS 122 281,» ETSI - TECHNICAL SPECIFICATION, 2017, Antipolis France .

[409] The Public Safety Network, «A Public Safety Agency Roadmap for Successful Mission Critical Push-to-Talk (MCPTT) Implementation,» 2020. [Ηλεκτρονικό]. Available:

https://www.publicsafety.network/wp-content/uploads/2021/01/MCPTT-White-Paper-PSN-Final.pdf. [Πρόσβαση 12 02 2023].

[410] H. Ludwig, «Reducing complexity & cost in future control room implementations,» 3GPP, 02 05 2022. [Ηλεκτρονικό]. Available: https://www.3gpp.org/technologies/reducing-complexity-cost-in-future-control-room-implementations. [Πρόσβαση 12 02 2023].

[411] K. Ali, H. X. Nguyen, Q.-T. Vien, P. Shah, M. Raza, V. V. Paranthaman, ,. B. Er-Rahmadi, M. Awais, S. Islam και j. J. P. C. Rodrigues, «Review and Implementation of Resilient Public Safety Networks: 5G, IoT, and Emerging Technologies,» *IEEE Network ,* pp. 18-25, March 2021.

[412] D. Lund, L. Claeys και M.-C. Bonnamour, «'Apps' for Public Protection and Disaster Relief (PPDR) - White Paper,» Public Safety Communication Europe, 2017.

[413] T. D. Raty, «Survey on Contemporary Remote Surveillance Systems for Public Safety,» *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews),* τόμ. 40, αρ. 5, pp. 493 - 515, 2010.

[414] R. Halili, F. Z. Yousaf, N. Slamnik-Krijestorac, G. M. Yilma, M. Liebsch, E. d. B. Silva, S. A. Hadiwardoyo, R. Berkvens και M. Weyn, «Leveraging MEC in a 5G System for Enhanced Back Situation Awareness,» σε *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, Sydney, NSW, Australia, 2020.

[415] K. C. Budka, T. Chu, T. L. Doumi, W. Brouwer, P. l Lamoureux και M. E. Palamara, «Public Safety Mission Critical Voice Services Over LTE,» *Bell Labs Technical Journal,* pp. 133-150, 2011.

[416] RedHat, «What is multi-access edge computing (MEC)?,» RedHat, 22 07 2022. [Ηλεκτρονικό]. Available: https://www.redhat.com/en/topics/edge-computing/what-is-multi-access-edge-computing. [Πρόσβαση 12 02 2023].

[417] F. Castanedo, «A Review of Data Fusion Techniques,» *Hindawi Publishing Corporation,* p. 16, 2013.

[418] T. Meng, X. Jing, Z. Yan και W. Pedrycz, «A Survey on Machine Learning for Data Fusion,» *Information Fusion,* τόμ. 5, pp. 115-129, 2020.

[419] I. Bouchrika, «20 Best Police Records Management System in 2023,» Research.com, 23 08 2022. [Ηλεκτρονικό]. Available: https://research.com/software/best-police-records-management-system. [Πρόσβαση 12 02 2023].

[420] FILECLOUD, «Record Management System | Document & Data Retention Software,» FILECLOUD, 11 03 2020. [Ηλεκτρονικό]. Available: https://www.filecloud.com/blog/2020/03/retention-in-record-management-software/#.Y-

51GC81vBI. [Πρόσβαση 12 02 2023].

[421] Z. Banach, «How to ensure REST API security,» Invicti, 11 03 2022. [Ηλεκτρονικό]. Available: https://www.invicti.com/blog/web-security/rest-api-web-service-security/. [Πρόσβαση 12 02 2023].

[422] M. Cobb, «12 API security best practices to protect your business,» TechTarget, 18 10 2022. [Ηλεκτρονικό]. Available: https://www.techtarget.com/searchapparchitecture/tip/10-API-security-guidelines-and-best-practices. [Πρόσβαση 12 02 2023].

[423] Cradlepoint, «Trend Report: The Value of Cellular Broadband for Mission-Critical Communication,» 24 03 2021. [Ηλεκτρονικό]. Available: https://resources.cradlepoint.com/white-papers/the-value-of-cellular-broadband-for-mission-critical-communication?_ga=2.47968293.343119316.1676485145-13755117.1676485145#page=1. [Πρόσβαση 12 02 2023].

[424] European Union Agency for Cybersecurity, ENISA, «ENISA THREAT LANDSCAPE 2021,» ENISA, Αθήνα, 2021.

[425] Χ. Μπουρας, *ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ ΚΑΙ ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ Ασφάλεια δικτύων,* Πάτρα: Πανεπιστήμιο Πατρών, 2017.

[426] C. KAUFMAN, R. PERLMAN και M. SPECINER, Network Security Private Communication in a Public World, Rearson, 2017.

[427] J. B. Perazzone, P. L. Yu, B. M. Sadler και R. S. Blum, «Cryptographic Side-Channel Signaling and Authentication via Fingerprint Embedding,» *IEEE Transactions on Information Forensics and Security,* τόμ. 13, αρ. 9, pp. 2216 - 2225, 2018.

[428] ITU-Telecommunication Standardization Sector Rec. X.805, «Security architecture for systems providing end-to-end communications,» INTERNATIONAL TELECOMMUNICATION UNION, 2003.

[429] Y. Huang, W. He, K. Nahrstedt και W. . C. Lee, «Requirements and System Architecture Design Consideration for First Responder Systems,» σε *2007 IEEE Conference on Technologies for Homeland Security*, Woburn, MA, USA, 2007.

[430] Κωνσταντ, Φ. Κωνσταντινου, Α. Κανατας και Γ. Παντος, Συστήματα Κινητών Επικοινωνιών, Αθήνα: Παπασωτηρίου, 2014.

[431] «Astrid.be,» [Ηλεκτρονικό]. Available: https://www.astrid.be/en/about-astrid/organisation. [Πρόσβαση 13 12 2022].

[432] «An update of public safety LTE deployment efforts around Europe,» [Ηλεκτρονικό]. Available: https://www.rrmediagroup.com/Features/FeaturesDetails/FID/1049. [Πρόσβαση 01 12 2022].

[433] «Service and support,» Astrid.be, [Ηλεκτρονικό]. Available: https://www.astrid.be/en/service-support. [Πρόσβαση 01 12 2022].

[434] «ASTRID to remain the partner of public safety sevices into the future,» [Ηλεκτρονικό]. Available: https://www.astrid.be/en/news/astrid-remain-partner-public-safety-services-future. [Πρόσβαση 01 12 2022].

[435] P. Clemons, «criticalcommunicationsreview.com,» 13 02 2015. [Ηλεκτρονικό]. Available: https://www.criticalcommunicationsreview.com/ccr/blogs/30005/the-end-of-airwave-and-the-truth-about-tetra-and-lte-for-uk-emergency-services-act-1. [Πρόσβαση 18 02 2023].

[436] «gov.uk,» 24 01 2023. [Ηλεκτρονικό]. Available: https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network. [Πρόσβαση 15 02 2023].

[437] «business.ee.co.uk,» [Ηλεκτρονικό]. Available: https://business.ee.co.uk/large-business/esn/temporary-coverage/. [Πρόσβαση 18 02 2023].

[438] BT, «newsroom.bt.com,» BT, 08 03 2022. [Ηλεκτρονικό]. Available: https://newsroom.bt.com/how-were-bringing-connectivity-to-more-of-britain-for-our-emergency-services/. [Πρόσβαση 18 02 2023].

[439] T. Savunen, H. Hämmäinen, K. Kilkki και P. Kekolahti, «The role of mobile network operators in next-generation public safety services,» *Telecommunications policy,* 2023.

[440] Z. Ghadialy, «blog.3g4g.co.uk,» DAS & SMALL CELLS, 21 11 2017. [Ηλεκτρονικό]. Available: https://blog.3g4g.co.uk/2017/11/a-practical-use-of-mocn-in-esn.html. [Πρόσβαση 18 02 2023].

[441] T. Savunen, H. Hämmäinen, K. Kilkki και P. Kekolahti, «The role of mobile network operators in next-generation public safety services,» *Telecommunications policy,* τόμ. 47, αρ. 3, 2023.

[442] «securelandcommunications,» AIRBUS, [Ηλεκτρονικό]. Available: https://www.securelandcommunications.com/customerstories/france-rubis-nationwide-network-for-gerdarmerie. [Πρόσβαση 14 02 2023].

[443] «Medium,» ESN, 24 09 2019. [Ηλεκτρονικό]. Available: https://medium.com/@ESNCommunicationsTeam/interview-with-radio-network-of-the-future-8908b9c0f50c#id_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IjU5NjJlN2EwNTljN2Y1YzBjMGQ1NmNiYWQ1MWZlNjRjZWVjYTY3YzYiLCJ0eXAiOiJKV1QifQ.eyJpc3MiOiJodHRwczovL2FjY291bnRzLmdvb2dsZS5jb. [Πρόσβαση 14 02 2023].

[444] «securelandcommunications,» AIRBUS, [Ηλεκτρονικό]. Available: https://www.securelandcommunications.com/customerstories/inpt-nationwide-public-safety-

network-in-france. [Πρόσβαση 14 02 2023].

[445] «Gouv.fr,» 13 10 2022. [Ηλεκτρονικό]. Available: https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2022-10/13-10-2022-cp-rrf.pdf. [Πρόσβαση 13 02 2023].

[446] «alloforfait,» 14 10 2022. [Ηλεκτρονικό]. Available: https://alloforfait.fr/mobile/news/109039-reseau-radio-futur-orange-bouygues-telecom-participer-construction.html. [Πρόσβαση 13 10 2023].

[447] K. Junttila, «Edrnap2021.hu,» 05 05 2022. [Ηλεκτρονικό]. Available: https://edrnap2021.hu/down/A-0040.pdf.

[448] Ericsson, «Ericsson,» 11 2022. [Ηλεκτρονικό]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2022. [Πρόσβαση 10 02 2023].

[449] «Erillisverkot.fi,» 04 2021. [Ηλεκτρονικό]. Available: https://www.erillisverkot.fi/uploads/2021/04/virve-mobile-stragegy-2021-version-1.1_03_2021web.pdf. [Πρόσβαση 10 02 2023].

[450] Ericsson, «Ericsson,» Ericsson, 09 04 2020. [Ηλεκτρονικό]. Available: https://www.ericsson.com/en/press-releases/2020/4/erillisverkot-finland-chooses-ericsson-5g-core-for-next-generation-public-safety-network. [Πρόσβαση 10 02 2023].

[451] Elisa, «Elisa.com,» Elisa, 09 04 2020. [Ηλεκτρονικό]. Available: https://elisa.com/corporate/news-room/press-releases/elisa-chosen-as-the-sole-radio-network-supplier-to-finland's-new-public-safety-network-for-10-years-due-to-quality-and-coverage/04606083990513/. [Πρόσβαση 10 02 2023].

[452] Erillisverkot, «Erillisverkot.fi,» 2021. [Ηλεκτρονικό]. Available: https://www.erillisverkot.fi/uploads/2021/04/virve-mobile-stragegy-2021-version-1.1_03_2021web.pdf. [Πρόσβαση 10 02 2023].

[453] «Gov.au,» [Ηλεκτρονικό]. Available: https://www.infrastructure.gov.au/department/media/news/life-saving-satellite-services-being-deployed-emergency-communications. [Πρόσβαση 01 12 2022].

[454] «Australian digital transformation of critical communications for public safety market 2017 0 2022,» Businesswire.comBusinesswire.com, [Ηλεκτρονικό]. Available: https://www.businesswire.com/news/home/20180103005530/en/Australian-Digital-Transformation-of-Critical-Communications-for-Public-Safety-Market-2017-2022-Digital-LMR-Continues-to-Dominate-the-Critical-Communications-Market-in-Australia---Research-and-Marke. [Πρόσβαση 01 12 2022].

[455] NSW Government, «Public Safety Network expanded across NSW,» NSW Government, 05 08 2022. [Ηλεκτρονικό]. Available: https://www.nsw.gov.au/news/public-safety-network-expanded-

across-nsw.. [Πρόσβαση 01 12 2022].

[456] «Terria map,» Gov.au, [Ηλεκτρονικό]. Available: https://nationalmap.gov.au/.. [Πρόσβαση 15 12 2022].

[457] «Australia public safety poised to advance with shared - network mobile broadband,» [Ηλεκτρονικό]. Available: https://www.criticalcomms.com.au/content/public-safety/sponsored/australia-s-public-safety-poised-to-advance-with-shared-network-mobile-broadband-491800103.. [Πρόσβαση 01 12 2022].

[458] NSW Government, «NSW Department of Customer Service,» NSW Government, [Ηλεκτρονικό]. Available: https://www.nsw.gov.au/telco-authority/public-safety-mobile-broadband.. [Πρόσβαση 01 12 2022].

[459] MA Exhibitions, «1200 Panel Disc B Held,» MA Exhibitions, 08 07 2022. [Ηλεκτρονικό]. Available: https://www.youtube.com/watch?v=pmFyPbMXB-I.. [Πρόσβαση 15 09 2022].

[460] N. Telco Authority, «NSW Telco Authority Annual Report,» [Ηλεκτρονικό]. Available: https://www.nsw.gov.au/sites/default/files/2022-11/nsw-telco-authority-annual-report-2021-2022.pdf. [Πρόσβαση 01 12 2022].

[461] «wikipedia.org,» [Ηλεκτρονικό]. Available: https://en.wikipedia.org/wiki/Sinking_of_MV_Sewol. [Πρόσβαση 15 02 2023].

[462] «Mois.go.kr,» [Ηλεκτρονικό]. Available: https://www.mois.go.kr/eng/bbs/type002/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000022&nttId=62037. [Πρόσβαση 15 02 2023].

[463] T. Savunen, H. Hämmäinen, K. Kilkki και P. Kekolahti, «The role of mobile network operators in next-generation public safety services,» *Telecommunications policy,* p. 102489, 2023.

[464] «Safenet.go.kr,» [Ηλεκτρονικό]. Available: https://www.safenet.go.kr/kor/contents/4. [Πρόσβαση 17 02 2023].

[465] American National Standards Institute, «Introduction,» American National Standards Institute, [Ηλεκτρονικό]. Available: https://www.ansi.org/about/introduction. [Πρόσβαση 13 02 2023].

[466] TCCA, «4G and 5G for Public Safety - Technology Options,» TCCA, 2017.

[467] SAFECOM, «Public Safety Communications Evolution,» Homeland Security SAFECOM, 2011.

[468] IEEE INGR, «Executive Summary - Roadmap from 2022 to 2032,» IEEE International Network Generations Roadmap , 2022.

[469] M. Ulema, FUNDAMENTALS OF PUBLIC SAFETY NETWORKS AND CRITICAL COMMUNICATIONS SYSTEMS, New York: WILEY, 2019.

[470] L. J. Ippolito Jr., Satellite Communications Systems Engineering: Atmospheric Effects, Satellite Link Design and System Performance, Wiley, 2008.

[471] «Australian digital transforn,» Businesswire.com, [Ηλεκτρονικό]. Available: https://www.businesswire.com/news/home/20180103005530/en/Australian-Digital-Transformation-of-Critical-Communications-for-Public-Safety-Market-2017-2022-Digital-LMR-Continues-to-Dominate-the-Critical-Communications-Market-in-Australia---Research-and-Marke. [Πρόσβαση 1 December 2022].

[472] gov.au, [Ηλεκτρονικό]. Available: https://www.nsw.gov.au/sites/default/files/noindex/2022-07/22-23telco-authority-corporate-plan.pdf. [Πρόσβαση 15 December 2022].

Παράρτημα

Παρατίθεται μια αναλυτική αποτύπωση του Ερωτηματολογίου

Πρώτη Ενότητα

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

Για τους ανθρώπους της δημόσιας ασφάλειας, πολιτικής προστασίας και πρώτους ανταποκριτές
Εικόνα θέματος από: https://www.civilprotection.gr/el/simantika-themata/epeteiaki-seira-grammatosimon-gia-ta-25-hronia-tis-politikis-prostasias-afieromeni

ntentasdim@gmail.com (δεν κοινοποιήθηκε)
Εναλλαγή λογαριασμού

Πρώτη ενότητα. Δημογραφικά στοιχεία

Περιλαμβάνει δημογραφικά στοιχεία που βοηθούν στην ομαδοποίηση των αποτελεσμάτων της έρευνας, ώστε να εξαχθούν εύστοχα και χρήσιμα συμπεράσματα. Σε καμία περίπτωση δεν δημοσιοποιούνται η ταυτότητα ή τυχόν στοιχεία του χρήστη

Φύλο *
- Γυναίκα
- Άνδρας

Ηλικία *
- έως 25
- 26 - 35
- 36 - 45
- 46 και πάνω

Επίπεδο σπουδών
- Δευτεροβάθμια εκπαίδευση
- Απόφοιτος ΙΕΚ
- Απόφοιτος ΑΕΙ/ΑΤΕΙ/ΤΕΙ
- Κάτοχος μεταπτυχιακού διπλώματος
- Κάτοχος διδακτορικού διπλώματος
- Άλλο:

Υπηρεσία *
- Ελληνική Αστυνομία
- Πυροσβεστική Υπηρεσία
- Λιμενικό Σώμα
- Εθνικό Σύστημα Υγείας
- Άλλο:

Εργάζομαι στην περιφερειακή ενότητα *
- Ανατολικής Μακεδονίας και Θράκης
- Κεντρικής Μακεδονίας
- Δυτικής Μακεδονίας
- Ηπείρου
- Θεσσαλίας
- Ιωνίων Νήσων
- Δυτικής Ελλάδας
- Στερεάς Ελλάδας
- Αττικής
- Πελλοποννήσου
- Βορείου Αιγαίου
- Νοτίου Αιγαίου
- Κρήτης

Έτη υπηρεσίας *
- έως 5
- 6-10
- 11-15
- 16-20
- 25 και πάνω

Κατά την άσκηση των καθηκόντων μου είμαι ένστολη/ος *
- Ναι
- Όχι

Τα κύρια καθήκοντά μου είναι *
- Μάχιμος (περιπολία, εξωτερική υπηρεσία)
- Υπηρεσία εντός Γραφείου (Διοικητικός, εσωτερικές υπηρεσίες)
- Σε σταθμό βάσης (τηλεφωνικό - επιχειρησιακό κέντρο συντονισμού)
- Υπηρεσία εντός γραφείου και μάχιμος
- Άλλο:

Αποτελεσματικότητα στη χρήση ηλεκτρονικού υπολογιστή
- Δεν χρησιμοποιώ υπολογιστή
- Ελάχιστα ικανή /ος
- Ικανή /ος
- Πολύ ικανή /ος
- Εξαιρετικά ικανή /ος

Δεύτερη Ενότητα (Α)

Δεύτερη ενότητα

Α.Χρήση της τεχνολογίας στην υπηρεσιακή καθημερινότητα
Είναι γνωστό ότι δεν υφίσταται η έννοια της "τυπικής - συνηθισμένης" ημέρας στο πλαίσιο άσκησης των υπηρεσιακών σου καθηκόντων. Παρόλα αυτά, οι ερωτήσεις που ακολουθούν και περιλαμβάνονται στην παρούσα υποενότητα εστιάζουν στο τεχνολογικό υλικό που χρησιμοποιείς σε μια συνηθισμένη ημέρα στη δουλειά.

Ποιες από τις συσκευές που αναφέρονται στη συνέχεια χρησιμοποιείς στην καθημερινή σου υπηρεσία *

	Χρησιμοποιώ πολύ	Χρησιμοποιώ περιστασιακά	Διαθέτω, αλλά δεν χρησιμοποιώ	Δεν διαθέτω
Ηλεκτρονικό υπολογιστή (desktop)	☐	☐	☐	☐
Ακουστικά (που προμηθεύτηκες ιδιωτικά)	☐	☐	☐	☐
Ενσύρματο μικρόφωνο	☐	☐	☐	☐
Προσωπικό έξυπνο τηλέφωνο (smartphone)	☐	☐	☐	☐

Η σημαντικότητα της ακρίβειας της πληροφορίας, κατά την άσκηση των καθηκόντων σου, είναι δεδομένη. Ποιες από τις αναφερόμενες περιπτώσεις και πόσο συχνά σε έχουν απασχολήσει - προβληματίσει;

	Πάντοτε	Τις περισσότερες φορές	Μερικές φορές	Σπάνια	Ποτέ	Δεν σχετίζεται/ με αφορά
Ανακριβείς ή ελλιπείς πληροφορίες από τους πολίτες	☐	☐	☐	☐	☐	☐
Αδυναμία εντοπισμού καλούντος / Αναγκαιότητα	☐	☐	☐	☐	☐	☐
Πολλαπλές κλήσεις την ίδια στιγμή / Υπερφόρτωση κέντρου (σταθμού βάσης)	☐	☐	☐	☐	☐	☐
Πολλές πληροφορίες την ίδια στιγμή / Υπερπληροφόρηση	☐	☐	☐	☐	☐	☐
Αδυναμία χρήσης χαρτών	☐	☐	☐	☐	☐	☐
Ασύρματα ακουστικά	☐	☐	☐	☐	☐	☐
Υπηρεσιακό κινητό τηλέφωνο	☐	☐	☐	☐	☐	☐
Υπηρεσιακό έξυπνο κινητό τηλέφωνο (smartphone)	☐	☐	☐	☐	☐	☐
Ασύρματο μικρόφωνο	☐	☐	☐	☐	☐	☐
Πομποδέκτης αυτοκινήτου	☐	☐	☐	☐	☐	☐
Φορητός πομποδέκτης	☐	☐	☐	☐	☐	☐
Προσωπικό έξυπνο τηλέφωνο	☐	☐	☐	☐	☐	☐
Tablet	☐	☐	☐	☐	☐	☐

Από τις παρακάτω συσκευές, επέλεξε τις πέντε (5) σημαντικότερες, για την καθημερινή άσκηση των καθηκόντων σου *

	1	2	3	4	5	ΟΧΙ
Φορητή κάμερα (σώματος)	☐	☐	☐	☐	☐	☐
Σταθερή κάμερα (κτήριο, όχημα, κ.λπ.)	☐	☐	☐	☐	☐	☐
Ηλεκτρονικός υπολογιστής (desktop)	☐	☐	☐	☐	☐	☐
Φορητός ηλεκτρονικός υπολογιστής (laptop)	☐	☐	☐	☐	☐	☐
Ακουστικά	☐	☐	☐	☐	☐	☐
Σαρωτής δακτυλικών αποτυπωμάτων	☐	☐	☐	☐	☐	☐
Ασύρματο τηλέφωνο	☐	☐	☐	☐	☐	☐

Πόσες διαφορετικού τύπου οθόνες χρησιμοποιείς παράλληλα στην καθημερινότητά σου, κατά την άσκηση των καθηκόντων σου (σταθερό Η/Υ, laptop, tablet, smartphone, smartwatch, κ.λπ.);

- ○ καμία
- ○ 1
- ○ 2
- ○ 3 και πάνω

Δεύτερη Ενότητα (Β)

Δεύτερη ενότητα

Β. Προβλήματα κατά τη χρήση της τεχνολογίας στην υπηρεσιακή καθημερινότητα
Οι ερωτήσεις που ακολουθούν εστιάζουν στα προβλήματα που αντιμετωπίζετε στη χρήση της τεχνολογίας και των συσκευών επικοινωνίας στην υπηρεσιακή σας καθημερινότητα

Κατά την επικοινωνία σας με το κέντρο (σταθμός βάσης), έχετε αντιμετωπίσει προβλήματα με

	Πάντοτε	Τις περισσότερες φορές	Μερικές φορές	Σπάνια	Ποτέ	Δεν σχετίζεται / με αφορά
Ποιότητα ήχου	☐	☐	☐	☐	☐	☐
Μπαταρία	☐	☐	☐	☐	☐	☐
Κανάλι επικοινωνίας	☐	☐	☐	☐	☐	☐
Καλωδίωση	☐	☐	☐	☐	☐	☐
Κάλυψη (νεκρές ζώνες)	☐	☐	☐	☐	☐	☐
Αντοχή	☐	☐	☐	☐	☐	☐
Διαλειτουργικότητα	☐	☐	☐	☐	☐	☐
Παλαιότητα	☐	☐	☐	☐	☐	☐
Παρεμβολές	☐	☐	☐	☐	☐	☐

Άλλο πρόβλημα με τον ασύρματο (εξειδίκευσε)

Η απάντησή σας

Παρεμβολές	☐	☐	☐	☐	☐	☐

Άλλο πρόβλημα με τον ασύρματο (εξειδίκευσε)

Η απάντησή σας

Αδυναμία χρήσης υπηρεσιακών βάσεων δεδομένων (διαθέσιμων υπηρεσιακών εφαρμογών)	☐	☐	☐	☐	☐	☐

Άλλο (εξειδίκευσε)

Η απάντησή σας

Συχνότητα χρήσης τεχνολογίας, συσκευών και τεχνολογικών δυνατοτήτων

	Χρησιμοποιώ πολύ	Περιστασιακή χρήση	Διαθέτω, αλλά δεν χρησιμοποιώ	Δεν διαθέτω
Υπηρεσιακός υπολογιστής συνδεδεμένος με το δίκτυο (car-pc, laptop, smartphone, etc)	☐	☐	☐	☐
Εγκληματολογική βάση δεδομένων	☐	☐	☐	☐
On line υπηρεσίες / Intranet	☐	☐	☐	☐
Γεωεντοπισμό σου / οχήματός σου	☐	☐	☐	☐
Μεταφραστή	☐	☐	☐	☐
GPS	☐	☐	☐	☐

Από τις παρακάτω εφαρμογές / λογισμικό, επέλεξε τις τρεις (3) σημαντικότερες, για την καθημερινή άσκηση των καθηκόντων σου *

	1	2	3	OXI
Υπηρεσιακός υπολογιστής συνδεδεμένος με το δίκτυο (car-pc, laptop, smartphone, etc)	☐	☐	☐	☐
On line υπηρεσίες / Intranet	☐	☐	☐	☐
Γεωεντοπισμός	☐	☐	☐	☐
GPS	☐	☐	☐	☐
Εφαρμογές πρόγνωσης καιρού	☐	☐	☐	☐
Σύστημα καταγραφής φωνής	☐	☐	☐	☐
Λογισμικό ηλεκτρονικής καταγραφής συμβάντων	☐	☐	☐	☐
Εφαρμογές κυκλοφοριακής συμφόρησης (live)	☐	☐	☐	☐
Εφαρμογές πρόγνωσης καιρού	☐	☐	☐	☐

Άλλο (εξειδίκευσε)

Η απάντησή σας

Άλλο (εξειδίκευσε)

Η απάντησή σας

Από τις παρακάτω εφαρμογές / λογισμικό, επέλεξε τις τρεις (3) σημαντικότερες, για την καθημερινή άσκηση των καθηκόντων σου *

	1	2	3	OXI
Υπηρεσιακός υπολογιστής συνδεδεμένος με το δίκτυο (car-pc, laptop, smartphone, etc)	☐	☐	☐	☐
On line υπηρεσίες / Intranet	☐	☐	☐	☐
Γεωεντοπισμός	☐	☐	☐	☐
GPS	☐	☐	☐	☐
Εφαρμογές πρόγνωσης καιρού	☐	☐	☐	☐

Άλλο (εξειδίκευσε)

Η απάντησή σας

Από τα παρακάτω αντικείμενα / συσκευές / εφαρμογές / λογισμικό, επέλεξε αυτά που θα μπορούσαν να σου φανούν χρήσιμα για την καθημερινή άσκηση των καθηκόντων σου

	Πάντοτε	Τις περισσότερες φορές	Μερικές φορές	Σπάνια	Ποτέ	Δεν σχετίζεται / με αφορά
Επαυξημένη πραγματικότητα	☐	☐	☐	☐	☐	☐
Εικονική πραγματικότητα	☐	☐	☐	☐	☐	☐
Drones	☐	☐	☐	☐	☐	☐
Αναγνώριση προσώπου	☐	☐	☐	☐	☐	☐
Γεωεντοπισμός / ακριβής εντοπισμός θέσης και καθ` ύψος (αλτίμετρο)	☐	☐	☐	☐	☐	☐
Προβολή πληροφοριών σε οδηγό (heads-up display - συστήματα υποβοήθησης οδηγού ADAS)	☐	☐	☐	☐	☐	☐
Σύστημα εντοπισμού θέσης εσωτερικού χώρου (Indoor mapping)	☐	☐	☐	☐	☐	☐
Κοινή είσοδο σε εφαρμογές (one login)	☐	☐	☐	☐	☐	☐

Γεωεντοπισμός / ακριβής εντοπισμός θέσης και καθ` ύψος (αλτίμετρο)	☐	☐	☐	☐	☐	☐
Προβολή πληροφοριών σε οδηγό (heads-up display - συστήματα υποβοήθησης οδηγού ADAS)	☐	☐	☐	☐	☐	☐
Σύστημα εντοπισμού θέσης εσωτερικού χώρου (Indoor mapping)	☐	☐	☐	☐	☐	☐
Κοινή είσοδο σε εφαρμογές (one login)	☐	☐	☐	☐	☐	☐
Βίντεο πραγματικού χρόνου (δυνατότητα ανάλυσης και εξαγωγής χρήσιμων στοιχείων από βιντεοληπτικό υλικό)	☐	☐	☐	☐	☐	☐
Ρομπότ	☐	☐	☐	☐	☐	☐
Αυτοκινούμενα οχήματα	☐	☐	☐	☐	☐	☐
Έξυπνες υποδομές (κτήρια)	☐	☐	☐	☐	☐	☐
Έξυπνα ρολόγια	☐	☐	☐	☐	☐	☐
Φωνητικές εντολές	☐	☐	☐	☐	☐	☐

Ποια άλλη, που τυχόν δεν αναφέρεται παραπάνω;

Η απάντησή σας

Έχεις ποτέ εμπλακεί, κατά τη διάρκεια της υπηρεσία σου, σε μεγάλα προγραμματισμένα γεγονότα; *

- ◯ Ναι
- ◯ Όχι

Άλλο (εξειδίκευσε)

Η απάντησή σας

Τρίτη Ενότητα

Τρίτη ενότητα

Χρήση της τεχνολογίας σε μεγάλες καταστροφές (φυσικές ή ανθρωπογενείς), καθώς και σε μεγάλα προγραμματισμένα γεγονότα.
Ειδικότερα, στη συγκεκριμένη ενότητα καλείσαι ν` απαντήσεις σε μια σειρά ερωτήσεων που αφορούν σε μεγάλες καταστροφές, αλλά και μεγάλα προγραμματισμένα γεγονότα.
Στον όρο **"μεγάλες καταστροφές"** περιλαμβάνονται κάθε ιδιαίτερο συμβάν που ξεφεύγει από τη συνηθισμένη ημέρα εργασίας και αφορά σε κρίση, μη δυνάμενη να προβλεφθεί (π.χ. π.χ. σεισμό μεγάλου μεγέθους, εξέγερση, περιστατικό πολλαπλών πυροβολισμών, πυρκαγιά μεγάλου μεγέθους, κ.λπ.)
Στον όρο **"μεγάλα προγραμματισμένα γεγονότα"** περιλαμβάνονται επιχειρήσεις που είναι προγραμματισμένες και έχουν ιδιαιτέρως αυξημένες απαιτήσεις σε θέματα δημόσιας ασφάλειας (*π.χ. Ολυμπιακοί Αγώνες, Διεθνείς Εκθέσεις - Συνέδρια, αθλητικές οργανώσεις Παγκοσμίου ή Πανευρωπαϊκού επιπέδου, παρελάσεις ή συναυλίες με εξαιρετικά μεγάλο επιχειρησιακό εύρος, κ.λπ.*)

Έχεις αντιμετωπίσει ποτέ, κατά τη διάκρεια της καριέρας σου, κάποια μεγάλη καταστροφή *

- ◯ Ναι
- ◯ Όχι

Σκέψου την τεχνολογία που χρησιμοποιείς σε μια κατάσταση μεγάλης καταστροφής. Διαφέρει σε σχέση μ` αυτή που χρησιμοποιείς σε μία συνηθισμένη ημέρα εργασίας; *

- ◯ Χρησιμοποιώ σχεδόν την ίδια τεχνολογία
- ◯ Χρησιμοποιώ την ίδια τεχνολογία, αλλά κάποιες εξειδικευμένες δυνατότητές της
- ◯ Χρησιμοποιώ πολύ διαφορετική τεχνολογία
- ◯ Δεν έχω αντιμετωπίσει κατάσταση μεγάλης καταστροφής

Ποιές από τις ακόλουθες τεχνολογίες και μέσα πιστεύεις ότι θα σε βοηθούσαν να αντιμετωπίσει αποδοτικότερα μια κατάσταση μεγάλης καταροφής;

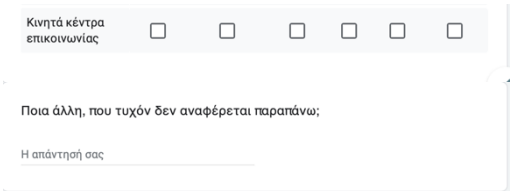
	Πάντοτε	Τις περισσότερες φορές	Μερικές φορές	Σπάνια	Ποτέ	Δεν σχετίζεται / με αφορά
Drones	☐	☐	☐	☐	☐	☐
Ελικόπτερα	☐	☐	☐	☐	☐	☐
Κινητά κέντρα ελέγχου	☐	☐	☐	☐	☐	☐
Ρομπότ	☐	☐	☐	☐	☐	☐
Κινητά κέντρα επικοινωνίας	☐	☐	☐	☐	☐	☐

Σκέψου την τεχνολογία που χρησιμοποιείς σε μεγάλα προγραμματισμένα γεγονότα. Διαφέρει σε σχέση μ` αυτή που χρησιμοποιείς σε μία συνηθισμένη ημέρα εργασίας; *

- ◯ Χρησιμοποιώ σχεδόν την ίδια τεχνολογία
- ◯ Χρησιμοποιώ την ίδια τεχνολογία, αλλά κάποιες εξειδικευμένες δυνατότητές της
- ◯ Χρησιμοποιώ πολύ διαφορετική τεχνολογία
- ◯ Δεν έχω αντιμετωπίσει κατάσταση μεγάλης καταστροφής

Ποιές από τις ακόλουθες τεχνολογίες και μέσα πιστεύεις ότι θα σε βοηθούσαν να αντιμετωπίσει αποδοτικότερα μεγάλα προγραμματισμένα γεγονότα; *

	Πάντοτε	Τις περισσότερες φορές	Μερικές φορές	Σπάνια	Ποτέ	Δεν σχετίζεται / με αφορά
Drones	☐	☐	☐	☐	☐	☐
Ελικόπτερα	☐	☐	☐	☐	☐	☐
Κινητά κέντρα ελέγχου	☐	☐	☐	☐	☐	☐
Δεδομένα από απομακρισμένους αισθητήρες (αεροπλάνα, δορυφόρους)	☐	☐	☐	☐	☐	☐
Ρομπότ	☐	☐	☐	☐	☐	☐



Τέταρτη Ενότητα

Τέταρτη Ενότητα

Ειδικότερα θέματα τεχνολογίας
Στην ενότητα αυτή ακολουθεί μια σειρά ερωτήσεων (εννιά -9- συνολικά) που αφορούν σε εξειδικευμένα τεχνολογικά ζητήματα και έργα που τρέχουν ήδη, ή βρίσκονται σε ερευνητικό επίπεδο ανά τον κόσμο και αφορούν στη δημόσια ασφάλεια και τους πρώτους ανταποκριτές

Πιστεύεις ότι η **εικονική πραγματικότητα (Virtual Reality)** μπορεί να συνεισφέρει στην εκπαίδευσής σου; *

- Ναι
- Όχι
- Δεν είμαι σίγουρος/η

Υπάρχει **δυνατότητα αποστολής γραπτών μηνυμάτων** στο τηλεφωνικό - επιχειρησιακό κέντρο της Υπηρεσία σου; *

- Ναι
- Όχι
- Δεν είμαι σίγουρος/η

Πιστεύεις ότι η **δυνατότητα αποστολής γραπτών μηνυμάτων** στο τηλεφωνικό - επιχειρησιακό κέντρο της Υπηρεσία σου θα λειτουργούσε θετικά; *

- Ναι
- Όχι
- Δεν είμαι σίγουρος/η

Υπάρχει **δυνατότητα αποστολής εικόνων ή βίντεο** στο τηλεφωνικό - επιχειρησιακό κέντρο της Υπηρεσία σου; *

- Ναι
- Όχι
- Δεν είμαι σίγουρος/η

Πιστεύεις ότι η **δυνατότητα αποστολής εικόνων ή βίντεο** στο τηλεφωνικό - επιχειρησιακό κέντρο της Υπηρεσία σου θα λειτουργούσε θετικά; *

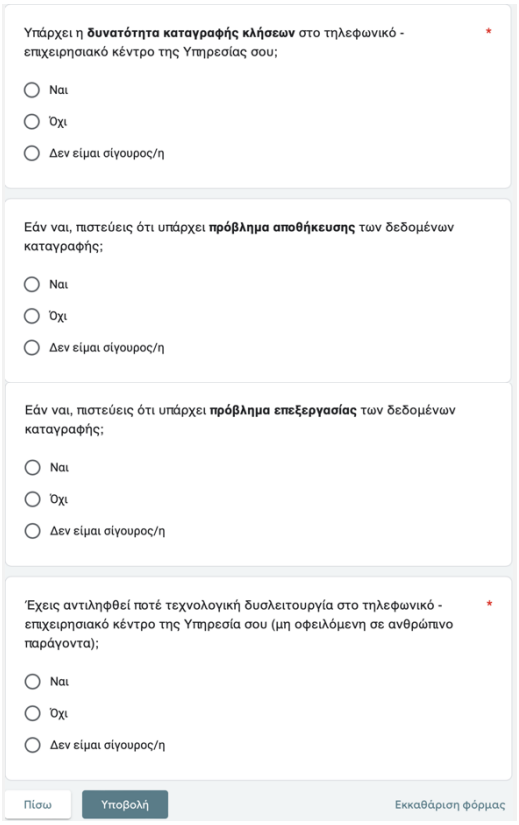
- Ναι
- Όχι
- Δεν είμαι σίγουρος/η

Υπάρχει η **δυνατότητα καταγραφής κλήσεων** στο τηλεφωνικό - επιχειρησιακό κέντρο της Υπηρεσίας σου; *

- Ναι
- Όχι
- Δεν είμαι σίγουρος/η

Εάν ναι, πιστεύεις ότι υπάρχει **πρόβλημα αποθήκευσης** των δεδομένων καταγραφής;

- Ναι
- Όχι
- Δεν είμαι σίγουρος/η



Εάν ναι, πιστεύεις ότι υπάρχει **πρόβλημα επεξεργασίας** των δεδομένων καταγραφής;

- Ναι
- Όχι
- Δεν είμαι σίγουρος/η

Έχεις αντιληφθεί ποτέ τεχνολογική δυσλειτουργία στο τηλεφωνικό - επιχειρησιακό κέντρο της Υπηρεσία σου (μη οφειλόμενη σε ανθρώπινο παράγοντα); *

- Ναι
- Όχι
- Δεν είμαι σίγουρος/η

Πίσω | Υποβολή | Εκκαθάριση φόρμας