ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

5G ΔΙΚΤΥΑ ΚΑΙ ΣΩΜΑΤΑ ΑΣΦΑΛΕΙΑΣ.

Η συνδρομή τους στην εξιχνίαση υποθέσεων των Αρχών Επιβολής του Νόμου.

Διπλωματική Εργασία

του

Τσινασλανίδη Λ. Ανέστη

Θεσσαλονίκη, Ιούνιος 2022

5G ΔΙΚΤΥΑ ΚΑΙ ΣΩΜΑΤΑ ΑΣΦΑΛΕΙΑΣ.
Η ΣΥΝΔΡΟΜΗ ΤΟΥΣ ΣΤΗΝ ΕΞΙΧΝΙΑΣΗ ΥΠΟΘΕΣΕΩΝ ΤΩΝ ΑΡΧΩΝ ΕΠΙΒΟΛΗΣ ΤΟΥ ΝΟΜΟΥ.

Τσινασλανίδης Λ. Ανέστης

Πτυχίο Οικονομικών Επιστημών, Δ.Π.Θ., 2011
Μ.Π.Σ. «Σπουδές στον Παρευξείνιο Χώρο», Δ.Π.Θ., 2008
Πτυχίο Γ.Φ.Π. Παρευξεινίων Χωρών, Δ.Π.Θ., 2006

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Ψάννης Κωνσταντίνος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 29/06/2022

ΨΑΝΝΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ	ΜΑΜΑΤΑΣ ΕΛΕΥΘΕΡΙΟΣ	ΠΕΤΡΙΔΟΥ ΣΟΦΙΑ
.....	.....	.....

ΤΣΙΝΑΣΛΑΝΙΔΗΣ Λ. Ανέστης

…….....

Περίληψη

Το εν λόγω θέμα επιλέχθηκε αφενός λόγω επαγγελματικής ιδιότητος του γράφοντος και αφετέρου αναγνωρίζοντας τις εξαιρετικές δυνατότητες εργαλειοποίησης των δικτύων 5G προς όφελος των Σωμάτων Ασφαλείας ως προς την επιτυχή εξιχνίαση υποθέσεων. Στη σύγχρονη κοινωνία η ταχεία ανάπτυξη της τεχνολογίας, καλύπτει όλο και περισσότερες πτυχές της καθημερινότητάς των πολιτών οι οποίες έχουν αυτοματοποιηθεί αναντίρρητα σε μεγάλο βαθμό προς όφελός τους. Αυτή η ανάπτυξη της τεχνολογίας έχει, δύο όψεις, όπου από τη μια έχουμε την χρήση της προς όφελος της κοινωνίας και από την άλλη την χρησιμοποίησή της προς εκμετάλλευση της κοινωνίας. Σε αυτό το πλαίσιο είναι αδύνατον να μην επηρεάσει και να μην επηρεαστεί -στην πράξη- η εφαρμογή της τεχνολογίας των δικτύων πέμπτης γενιάς- 5G από τα Σώματα Ασφαλείας, τα οποία καλούνται -σε ένα σύγχρονο περιβάλλον- να εξιχνιάζουν καθημερινώς μια σειρά από δυσεπίλυτες υποθέσεις που αλλιώς θα ήταν αδύνατον.

Στην παρούσα μελέτη, αρχικώς, αναφερόμαστε στα δίκτυα 4G- 5G και θα πραγματοποιηθεί μια σύντομη σύγκρισή τους αναφέροντας την βασική δομή τους. Έπειτα, θα αναφερθούμε στην εφαρμογή των 5G δικτύων εν γένει, το διαχωρισμό τους σε Standalone και Non Standalone δίκτυα αλλά και στα πλεονεκτήματα που δίδονται από τη χρήση τους από τα Σώματα Ασφαλείας. Τα δίκτυα 5G αποτελούν την γενιά δικτύων ασύρματης επικοινωνίας τα οποία ήδη κυριαρχούν στον τομέα των τηλεπικοινωνιών. Στην παρούσα διπλωματική πραγματοποιείται μια επισκόπηση των πλεονεκτημάτων από την λειτουργία των δικτύων 5G, καθώς και των βασικών προκλήσεων που πρέπει να ξεπεραστούν προκειμένου για να τεθούν σε πλήρη λειτουργία. Επίσης, αναλύεται μέρος της αρχιτεκτονικής των δικτύων 5G, τόσο όσον αφορά συγκεκριμένες τεχνολογίες, όσο και των προκλήσεων στην εφαρμογή τους που αυτές αντιμετωπίζουν. Τέλος μέρος της παρούσας διπλωματικής είναι αφιερωμένη στην ασφάλεια και τις προκλήσεις που αυτή αντιμετωπίζει από τα νέα χαρακτηριστικά των δικτύων 5G. Ακολούθως, προβαίνουμε στην ανάλυση όσο το δυνατόν μεγαλύτερου μέρους των δυνατοτήτων της πρακτικής εφαρμογής των δικτύων 5G.

Μέσω μελέτης υφιστάμενων άρθρων, εφαρμογών και επιστημονικών μελετών διαπιστώθηκε η απουσία προτάσεων μέγιστης αξιοποίησης των δικτύων πέμπτης γενιάς- 5G επί του πρακτέος από τα Σώματα Ασφαλείας. Προς τούτο, επιχειρήσαμε να αναδείξουμε τις δυνατότητες που παρέχονται από τη χρήση των εν λόγω δικτύων και να προτείνουμε πρακτικές εφαρμογές.

Λέξεις Κλειδιά:

Δίκτυα 5G, Αρχιτεκτονική 5G, Παράλληλη Καταγραφή Δεδομένων, Νόμιμη Καταγραφή Δεδομένων, Αρχές Επιβολής του Νόμου.

Abstract

This topic was partly chosen due to my professional occupation and partly due to the recognition of the extraordinary potential of 5G networks in order to benefit Law Enforcement Agencies (LEAs) in terms of successful case investigation.

In modern society, the rapid development of technology covers more and more aspects of citizens' daily lives, which have undoubtedly been automated, to a great extent, to their benefit. This development of technology has two aspects, where on the one hand we have its use for the benefit of society and on the other hand its use for the exploitation of society. In this context, it is impossible for the LEAs not to be influenced and affected - in practice - by the technology of fifth generation networks (5G), which are called upon - in a modern environment - to investigate a great number of difficult cases on a daily basis that would otherwise be impossible.

In this paper, we will firstly refer to 4G- 5G networks and make a brief comparison with reference to their basic structure. Then, we will refer to the implementation of 5G networks in general, their separation into Standalone and Non Standalone networks and the advantages of their use by the LEAs.

5G networks are the generation of wireless networks that already dominate the telecommunications sector. This thesis provides an overview of the advantages of operating 5G networks, as well as the key challenges that need to be overcome in order to make them fully operational. It also analyses part of the architecture of 5G networks, both in terms of the specific technologies and the implementation challenges they face. Furthermore, part of this thesis is devoted to security and the challenges faced by the new features of 5G networks. Then, we analyze as much as possible the practical application possibilities of 5G networks.

Through the study of existing articles, applications and scientific articles, we have identified the absence of proposals for the maximum possible implementation of the technology of fifth-generation (5G) networks by the LEAs. To this end, we tried to give prominence to the available possibilities of the use of 5G networks and propose practical utilizations.

Keywords:

5G networks, 5G architecture, Parallel Interception, Lawful Interception, Law Enforcement Agencies.

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο του Μεταπτυχιακού Προγράμματος Σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής, της Σχολής Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας. Η εισαγωγή και φοίτηση στο εν λόγω μεταπτυχιακό αποτέλεσε μια προσωπική πρόκληση καθόσον η θέληση για γνώση και η διαπίστωση ότι η επιστήμη της πληροφορική και δη η εις βάθος γνώση συγκεκριμένου αντικειμένου αυτής, αποτελεί απαραίτητο εφόδιο και εργαλείο για το μέλλον μιας σύγχρονης κοινωνία.

Σε αυτό το σημείο θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, κύριο Ψάννη Κωνσταντίνο, για την άριστη συνεργασία μας κατά τη διάρκεια εκπόνησης της παρούσης διπλωματικής εργασίας

Τέλος, χρίζει ιδιαίτερης μνείας η σημαίνουσα συνεισφορά της αγαπημένης μου οικογένειας και συγκεκριμένα της συζύγου μου και της κόρης μας που με υπομονή στέκονται αρωγοί σε κάθε μου βήμα.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Πίνακας συντμήσεων- Μετάφραση όρων.

-Αρχές Επιβολής του Νόμου- Law Enforcement Agencies (LEA)

-Νόμιμη καταγραφή δεδομένων- Lawful Interception (LI)

-Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων- Lawful Interception Provisioning Function (LIPF)

-Λειτουργία Ελέγχου Καταγραφής Δεδομένων (Lawful Interception Control Function (LICF)

-Πληροφορίες των Καταγεγραμμένων Δεδομένων- Intercepted Related Information (IRI)

-Δίκτυο Πρόσβασης Ραδιοσυχνοτήτων- Radio Access Network (RAN)

-Λειτουργία Αποθετηρίου Πληροφοριών Συστήματος- System Information Repository Function (SIRF)

-Λειτουργία Αποθετηρίου Δικτύου- Network Repository Function (NRF)

-Μόνιμο Αναγνωριστικό Συνδρομής- Subscription Permanent Identifier (SUPI)

-Κρυφό Αναγνωριστικό Συνδρομής- SUbscription Concealed Identifier (SUCI)

-Πύλη Σηματοδότησης- Signaling Gateway (SGW)

-Πύλη Δικτύου Πακέτου Δεδομένων- Packet Data Network Gateway (PGW)

-Εξοπλισμός Χρήστη- User Equipment (UE)

-Εξυπηρέτηση Κινητού Κέντρου Τοποθεσίας- Serving Mobile Location Center (SMLC)

-Λειτουργίας Επιπέδου Χρήστη- User Plane Function (UPF)

-Πολλαπλή Πρόσβαση Υπολογισμού Ακμών- Multi-access Edge Computing (MEC)

-Εξελιγμένο Πακέτο Πυρήνα- Evolved Packet Core (EPC)

-Οντότητα Διαχείρισης Κινητικότητας- Mobility Management Entity (MME)

-Σημεία Καταγραφής Δεδομένων- Points of Interception (POI)

-Λειτουργία Διαχείρισης Συνεδριών- Session Management Function (SMF)

-Λειτουργία Πρόσβασης Και Κινητικότητας- Access and Mobility Function (AMF)

-Λειτουργία Διαχείρισης- ADMinistration Function (ADMF)

-Περιεχόμενο Επικοινωνίας- Content of Communication (CC)

-Πάροχοι επικοινωνιών- Communications Service Providers (CSP)

-Κόμβος Επόμενης Γενιάς- Next Generation NodeB (gNB)

-Νόμιμη Πρόσβαση στις Υπηρεσίες Τοποθεσίας- Lawful Access Location Services (LALS)

-Υπηρεσία Παρακολούθησης Αρχών του Νόμου- Law Enforcement Monitoring Facility (LEMF)

-Λειτουργία Διαμεσολάβησης και Παράδοσης- Mediation and Delivery Function (MDF)

-Λειτουργίας Προσωρινής Αποθήκευσης Αναγνωριστικών- Identifier Caching Function (ICF)

-Λειτουργία Αναγνωριστικού Συμβάντος- Identifier Event Function (IEF)

-Λειτουργία Αναζήτησης Αναγνωριστικού- Identifier Query Function (IQF)

-Λειτουργία Εικονικού Δικτύου- Virtual Network Function (VNF)

-Στοιχείο Λειτουργίας Εικονικού Δικτύου- Virtual Network Function Component (VNFC)

-Μονάδα Πρωτοκόλλου δεδομένων- Protocol Data Unit (PDU)

-Δίκτυα Πέμπτης γενιάς – 5th Generation Networks (5G)

- Δίκτυα Τέταρτης γενιάς – 4th Generation Networks (4G)

- Δίκτυα Τρίτης γενιάς – 3rd Generation Networks (3G)

- Δίκτυα Δεύτερης γενιάς – 2nd Generation Networks (2G)

- Δίκτυα Πρώτης γενιάς –1st Generation Networks (1G)

-Πολλαπλή Πρόσβαση Διαίρεσης Συχνότητας– Frequency Division Multiple Access (FDMA)

-Τεχνητή Νοημοσύνη- Artificial Intelligence (AI)

-Λειτουργική Εικονοποίηση Δικτύου- Network Functional Virtualization (NFV)

-Τμηματοποίηση Δικτύου- Network slicing (NS)

-Διαχωρισμός της λειτουργίας ελέγχου και επιπέδου χρήστη- Control and User Plane Separation—(CUPS).

-Λειτουργία ελέγχου- Control Plane (CP)

-Λειτουργία επιπέδου χρήστη- User Plane (UP)

-Κυψελοειδές Διαδίκτυο των Πραγμάτων- Cellular Internet of Things (CIoT).

- Διεθνής Ταυτότητα Συνδρομητή Κινητής Τηλεφωνίας- International Mobile Subscriber Identity (IMSI)

-Διεθνής Ταυτότητα Εξοπλισμού Κινητής Συσκευής- International Mobile Equipment Identity (IMEI)

-Σταθμός Κινητής Τηλεφωνίας Ολοκληρωμένου Ψηφιακού Δικτύου Υπηρεσιών--Mobile Station Integrated Services Digital Network (MSISDN)

-Μονάδα Ταυτότητας Συνδρομητή- Subscriber Identity Module (SIM)

-Λειτουργία Ανίχνευσης Κυκλοφορίας- Traffic Detection Function (TDF)

-Λειτουργία Κανόνων Ελέγχου- Policy Control Rules Function (PCRF)

-Υπηρεσία Τοποθεσίας- Location Service (LCS)

- Μονάδες Μέτρησης Θέσης- Location Measurement Unit (LMU)

- Επίσκεψη στο Επίγειο Δημόσιο Δίκτυο Κινητής Τηλεφωνίας- Visiting Public Land Mobile Network (VPLMN)

-Λειτουργία Προσωρινής Αποθήκευσης Αναγνωριστικών- Identifier Caching Function (ICF)

1 Εισαγωγή

Στο πλαίσιο συγγραφής της παρούσης διπλωματικής εργασίας, πραγματοποιήθηκε έρευνα σε ένα ευρύ σύνολο επιστημονικών άρθρων σχετιζόμενων με τη λειτουργία των δικτύων 5G, την ασφάλεια στη χρήση τους, τη λογική πίσω από τη λειτουργία τους, τεχνικές και τρόπους βελτίωσης τους και τέλος τη χρησιμότητά τους και τη συνδρομή τους προς όφελος των Αρχών Επιβολής του Νόμου εν γένει.

Η μεθοδολογία που χρησιμοποιήθηκε προκειμένου να αναλυθεί το θέμα της εργασίας ώστε να καταλήξουμε σε ασφαλή συμπεράσματα ήταν η βιβλιογραφική επισκόπηση ενός συνόλου επιστημονικών άρθρων και μελετών. Συγκεκριμένα, επιχειρήθηκε η ανάλυση μέσω περιγραφής του περιεχομένου διαφόρων πηγών, η συγκριτική ανάλυση και η περιπτωσιολογική ανάλυση και μελέτη σχετικά με τα δίκτυα 5G και την ενδεχόμενη συνδρομή τους στα Σώματα Ασφαλείας.

Τα τεχνολογικά επιτεύγματα έχουν, ως φυσικό επακόλουθο, επίδραση στη καθημερινότητά μας, αλλά το 5G μπορεί να αποδειχθεί ιδιαίτερα σημαντικό. Είναι κοινώς αποδεκτό ότι η τεχνολογία δύναται να ενισχύσει τη δυναμική και τη δυνατότητα των Αρχών Επιβολής του Νόμου στην εξιχνίαση εγκλημάτων που αλλιώς θα ήταν αδύνατη. Παρόλα αυτά αξίζει να επισημανθεί ότι τη στιγμή που επευφημούμε τις δυνατότητες που μας παρέχει αυτή η τεχνολογία, όπως των υψηλών ταχυτήτων και της γρήγορης μεταφοράς δεδομένων, υπάρχει παράλληλα και μια ανησυχία επειδή αυτά ακριβώς τα πλεονεκτήματα μπορεί να χρησιμοποιηθούν για τον ακριβώς αντίθετο σκοπό από πλευράς κυβερνοασφάλειας.

Υπολογίζεται ότι τα δίκτυα 5G – στο αρχικό τους στάδιο- αγγίζουν ταχύτητες περί το 1 Gbps, ενώ αυτή η ταχύτητα δύναται να κυμανθεί μεταξύ των 5 και 10 Gbps. Αυτό όμως οδηγεί σε ακόμη μεγαλύτερες ποσότητες συλλογής, επεξεργασίας, αποθήκευσης και ανάλυσης δεδομένων.

Τα δίκτυα 5G αποτελούν μια τεχνολογία η οποία υποστηρίζει διαφορετικές τεχνολογίες συμπεριλαμβανομένων των Μη Αυτόνομων (Non-Standalone) και Αυτόνομων (Standalone) αρχιτεκτονικών. Ως προς τη Μη Αυτόνομη αρχιτεκτονική αναφέρεται ότι μπορεί να συνδυάζει στη σύνδεση Δικτύων Μακροπρόθεσμης Εξέλιξης (LTE) και 5G Radio στο Κυρίως Δίκτυο (single Packet Core/ EPC ή 5GC). Όλα αυτά

επιφέρουν επίπτωση στην διαδικασία της άρσης απορρήτου και της νόμιμης καταγραφής των επικοινωνιών.

Τα εν λόγω δίκτυα επίσης εισαγάγουν ένα σύνολο νέων πρωτοκόλλων καθώς και ένα νέο τύπο διεπαφών κατά τη διαδικασία της παράδοσης δεδομένων σε μια νόμιμη καταγραφή. Το γεγονός αυτό συνεπάγεται ότι τα Κέντρα Συλλογής Δεδομένων θα χρειασθεί να υιοθετήσουν και να βελτιώσουν την προσέγγισή τους στη διαδικασία συλλογής και επεξεργασίας δεδομένων.

Η παθητική και ενεργητική καταγραφή δεδομένων των χρηστών των δικτύων 5G, συμπεριλαμβανομένης και της καταγραφής της κυκλοφορίας (traffic) μεταξύ κεντρικών υπολογιστών, θα αμφισβητηθεί λόγω της εικονικοποίησης της λειτουργίας των δικτύων (NFV).

Αυτό που δεν θα πρέπει να μας διαφεύγει είναι η διαδικασία μετάβασης από την τεχνολογία των δικτύων τέταρτης γενιάς (4G) στην τεχνολογία των δικτύων πέμπτης γενιάς (5G). Το 4G μπορεί θεωρητικά να διαφαίνεται ότι βρίσκεται προς το τέλος της χρήσης του, όμως αυτό είναι κάτι το οποίο δεν ισχύει για όλες τις χώρες του κόσμου (συμπεριλαμβανομένης και της Ελλάδος) με τα δεδομένα να καταδεικνύουν την ταυτόχρονη χρήση των δικτύων 4G- 5G. Αυτή η μεταβατική περίοδος μπορεί να διαρκέσει και χρόνια, επομένως οι Αρχές θα πρέπει να είναι προετοιμασμένες να συλλέγουν δεδομένα μέσω και των δύο δικτύων ταυτόχρονα. Ενώ το 5G θα κατακλύζει τον κόσμο, οι Υπηρεσίες Ασφαλείας, οι Αρχές Επιβολής του Νόμου και οι Ρυθμιστικοί Φορείς θα πρέπει να βρουν τον καλύτερο και τρόπο για να ξεπεράσουν αυτή τη μεταβατική περίοδο.

Σύμφωνα με το ισχύον νομικό πλαίσιο στη χώρα μας, η άρση του απορρήτου των επικοινωνιών αποτελεί μια κατ' εξαίρεση επιτρεπόμενη διαδικασία, βάσει της οποίας τα στοιχεία της επικοινωνίας, τα οποία είναι καταρχήν απόρρητα, καθίστανται γνωστά σε συγκεκριμένες Αρχές και για συγκεκριμένους λόγους. Σύμφωνα με τη διάταξη του άρθρου 19 παρ. 1 του Συντάγματος, η άρση αυτή είναι δυνατόν να ισχύσει για τη δικαστική αρχή για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

Οι προαναφερθέντες λόγοι εξειδικεύονται με τις διατάξεις του ν. 2225/1994, όπως ισχύει, ο οποίος περιλαμβάνει και κατάλογο των εγκλημάτων για τη διακρίβωση των οποίων μπορεί να διαταχθεί με διάταξη του αρμόδιου δικαστικού συμβουλίου η άρση του απορρήτου. Τις διαδικασίες, τις τεχνικές και τις οργανωτικές ρυθμίσεις για την

άρση του απορρήτου των επικοινωνιών προβλέπουν, οι διατάξεις του ν. 2225/1994 και του ΠΔ 47/2005, όπως ισχύουν ("Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών," 2021).

Σύμφωνα με τους νόμους ν.2935/2001 και ν.2713/1999, εξειδικεύονται οι λόγοι για την άρση των επικοινωνιών για αδικήματα που αφορούν την καταπολέμηση της διαφθοράς στην Ελλάδα. Σημειώνεται ότι κάθε χώρα ανά τον κόσμο έχει θεσπίσει δικούς της κανόνες και πλαίσια που διέπουν τον τρόπο εφαρμογής της άρσης της επικοινωνίας των επικοινωνιών.

Η άρση ή αλλιώς η νόμιμη καταγραφή δεδομένων των χρηστών των δικτύων, αποτελεί ένα ισχυρό εργαλείο των Αρχών Επιβολής του Νόμου στην καταπολέμηση εγκλημάτων που προβλέπονται στις διατάξεις των νόμων που προαναφέρθηκαν. Αντιλαμβανόμενοι την ανωτέρω διαπίστωση είναι ακόλουθο το γεγονός ότι ακόμα και μια σύντομη διακοπή της εν λόγω υπηρεσίας θα μπορούσε να επιφέρει δυσάρεστες συνέπειες σε τυχόν εν εξελίξει έρευνες.

Όπως προαναφέρθηκε, προκειμένου να γίνει κατανοητό όσο το δυνατόν μεγαλύτερο φάσμα της χρησιμότητας των δικτύων 5G καθώς και της εφαρμογής αυτών στην εξιχνίαση εγκλημάτων από τις Αρχές επιβολής του Νόμου, μελετήθηκαν διάφορα άρθρα που αφορούν ακόμη και στη χρησιμότητά τους από στρατιωτικές υπηρεσίες, κυρίως ως προς τον τομέα της ασφάλειας της χρήσης τους. Επίσης, μελετήθηκαν άρθρα σχετιζόμενα με την τεχνολογία που χρησιμοποιείται από τα δίκτυα 5G.

Τέλος, για το σκοπό της έρευνας πραγματοποιήθηκε μελέτη (πέραν των επιστημονικών άρθρων) και πηγών σε διαδικτυακούς τόπους ιδιωτικών εταιρειών (white papers) οι οποίες δραστηριοποιούνται στην υλοποίηση εφαρμογών και στην ανάπτυξη τεχνολογιών σχετικά με τη χρήση των δικτύων 5G προς όφελος των Αρχών Επιβολής του Νόμου και δη της διαδικασίας υλοποίησης νόμιμων παράλληλων επισυνδέσεων-συνακροάσεων (parallel interception) των τηλεφωνικών επικοινωνιών χρηστών των δικτύων 5G, σε συνεργασία με εταιρείες παροχής τηλεπικοινωνιών.

2 Συνοπτική περιγραφή των δικτύων 5G και η διαφοροποίησή τους από τα δίκτυα 4G.

Προτού προχωρήσουμε σε μια σύντομη και συνοπτική περιγραφή των δικτύων 5G κρίνεται χρήσιμο να προβούμε σε μια -μερική- αναφορά της λειτουργίας των δικτύων 4ης γενιάς (4G). Καταρχήν να αναφέρουμε ότι το αγγλικό γράμμα "G" χρησιμοποιείται για να περιγράψει τις γενιές (generations) τεχνολογίας επικοινωνιών κυψελωτών συσκευών που έχουν εισαχθεί ή πρόκειται να εισαχθούν.

Το 4G αποτελεί την τέταρτη γενιά της τεχνολογίας ευρυζωνικών κυψελοειδών δικτύων, που διαδέχθηκε το δίκτυο 3G. Το πρότυπο (LTE) αποτελεί συντομογραφία του Long Term Evolution δηλαδή των Δικτύων Μακροπρόθεσμης Εξέλιξης, με το οποίο αναφερόμαστε στα δίκτυα 4G (Andrés, 2020), το οποίο αναπτύχθηκε εμπορικά στο Όσλο και τη Στοκχόλμη από το 2009. Ωστόσο, αποτελεί αντικείμενο συζήτησης μεταξύ των επιστημόνων εάν οι πρώτες εκδόσεις θα πρέπει να θεωρηθούν δίκτυα 4G.

Ο Διεθνής Τηλεπικοινωνιακός Σύνδεσμος (ITU) καθόρισε ένα σύνολο απαιτήσεων για τα πρότυπα 4G, με την αγγλική ονομασία «International Mobile Telecommunications- Advanced» (IMT- Advanced) (“ITU global standard for international mobile telecommunications ´IMT-Advanced´,” n.d.).

Σε αντίθεση με προηγούμενες γενιές, ένα σύστημα 4G δεν υποστηρίζει την παραδοσιακή υπηρεσία τηλεφωνίας με κυκλώματα μεταγωγής, αλλά επικοινωνία βασισμένη στο Πρωτόκολλο Διαδικτύου (IP), όπως η IP τηλεφωνία. Σημειώνεται ότι το Δίκτυο Μακροπρόθεσμης Εξέλιξης (LTE) είναι ένα σύστημα πλήρως βασισμένο σε IP.

Επίσης, επιλέχθηκε η μετάδοση πολλαπλών φορέων (Orthogonal Frequency Division Multiplexing/ OFDM) για τη διαδικασία του Downlink και η μετάδοση ενός φορέα Single Carrier-Frequency Division Multiple Access (SC-FDMA) για το Uplink, καθιστώντας δυνατή τη μεταφορά πολύ υψηλών ρυθμών μετάδοσης δεδομένων πολλαπλών διαδρομών (“3GPP - LTE,” 2008).

Η ασύρματη τεχνολογία 4ης γενιάς (4G) αποτέλεσε μια εξέχουσα τεχνολογία επικοινωνίας. Καθώς αυξάνονταν οι απαιτήσεις εύρους ζώνης δεδομένων, το 4G βελτίωνε το ρυθμό λήψης και αποστολής χρησιμοποιώντας υψηλότερες τεχνικές διαμόρφωσης.

Το Έργο Σύμπραξης Τρίτης Γενιάς (Third Generation Partnership Project -3GPP) προώθησε το Δίκτυο Μακροπρόθεσμης Εξέλιξης (Long Term Evolution/ LTE), προκειμένου να διασφαλιστεί η συνεχής αποτελεσματικότητα του Παγκόσμιου Συστήματος Κινητών Τηλεπικοινωνιών (Universal Mobile Telecommunications System/ UMTS) στο μέλλον. Το LTE μπορεί να παρέχει ταχύτητες λήψης περίπου εκατό (100) Mbps για πολλαπλές κεραίες (2x2), πολλαπλές εισόδους (MIMO) για τερματικούς σταθμούς ανώτερης κατηγορίας, ενώ για αυτούς τους τερματικούς σταθμούς ο ρυθμός αποστολής είναι περίπου 50 Mbps.

Επιπλέον, παρέχει καλύτερη φορητότητα, υψηλό επίπεδο ασφάλειας (συγκριτικά με τα παλαιότερης γενιάς δίκτυα), επεκτεινόμενη χρήση του ραδιοφάσματος, οικονομική υλοποίηση και διάφορα άλλα πλεονεκτήματα που καθιστούν το LTE πιο συνεπές και προσιτό στους χρήστες.

Ένα «μειονέκτημα» της αρχιτεκτονικής 4G το οποία απασχολεί, είναι ότι μπορεί να υποστηρίξει μέγιστο εύρος ζώνης ένα (1) Gigabit και καθώς το εύρος ζώνης που απαιτείται από τις συσκευές του Διαδικτύου των Πραγμάτων (IoT) αυξάνεται τα δίκτυα 4G τείνουν να αποτελέσουν σημείο συμφόρησης. Καθώς η ασφάλεια των δεδομένων και το εύρος ζώνης είναι σημαντικά δεδομένα για συσκευές IoT, το 4G οδεύει στο να μην αποτελεί την πιο κατάλληλη επιλογή.

Το 5G χρησιμοποιείται για την αναφορά των δικτύων τελευταίας γενιάς και δη των δικτύων "πέμπτης γενιάς", συστημάτων δηλαδή επικοινωνίας με κυψελοειδή μορφή. Το 5G κυμαίνεται σε υψηλό φάσμα συχνοτήτων ήτοι από 24 έως 100 GHz, το οποίο συνεπάγεται ότι τα δεδομένα μπορούν να μεταφερθούν πολύ γρηγορότερα από όσο μέχρι πρότινος.

Τα πρόσθετα βασικά στοιχεία της τεχνολογίας 5G σε σχέση με εκείνα των 4G, περιλαμβάνουν εκτεταμένη χρήση συστοιχιών κεραιών πολλαπλής εισόδου, πολλαπλής εξόδου (MIMO), εξελιγμένη εφαρμογή της τεχνολογίας διαμόρφωσης για τη μετάδοση σημάτων πιο άμεσα στους τελικούς χρήστες και «τμηματοποίηση» (slicing) δικτύου. Το ευρύ φάσμα τεχνολογικών αλλαγών και αλλαγών υποδομής που είναι εγγενείς στην υλοποίηση 5G δημιουργεί τεράστια οφέλη, καθώς και προκλήσεις τόσο σε απλούς χρήστες όσο και σε επιχειρήσεις αλλά και στους τηλεπικοινωνιακούς παρόχους.

Αν και τα δίκτυα 4G προσφέρουν -επί του παρόντος- σταθερές υπηρεσίες, αυτό δεν επαρκεί για τις μελλοντικές εφαρμογές και τις ασύρματες υπηρεσίες. Υπάρχουν

υψηλές προσδοκίες για τα 5G και αυτό αντικατοπτρίζεται στις εξαιρετικά υψηλές τιμές-στόχους που αναφέρονται.

Εν συντομία μπορούμε να αναφέρουμε ότι, συγκριτικά με τα δίκτυα 4G, η βελτίωση στα δίκτυα 5G αναμένονται να είναι πολύ μεγαλύτερη. Οι μέγιστοι ρυθμοί δεδομένων αναμένονται σε τιμές έως 20 Gbit/s, ενώ οι ρυθμοί δεδομένων που έχει ο χρήστης θα είναι περίπου 100 Mbit/s, με αύξηση 20 φορές και 10 φορές, αντίστοιχα. Η φορητότητα θα είναι έως 500 km/h, με βελτίωση 1,42, ο χρόνος αναμονής θα μειωθεί κατά 10x, η πυκνότητα σύνδεσης, δηλαδή ο μέγιστος αριθμός ταυτόχρονων συνδέσεων χρηστών σε μια περιοχή δεκαπλασιάζεται από 10^5 συσκευές/km^2 σε 10^6 συσκευές/km^2 και η χωρητικότητα κυκλοφορίας περιοχής θα αυξηθεί στα 10 Mbit/s/m^2 από 0,1 Mbit/s/m^2, με την βελτίωση να φτάνει τις 100 φορές παραπάνω (Barb and Otesteanu, 2020).

Key Requirements	4G (LTE)	5G
Peak Data Rate	1 Gbit/s	20 Gbit/s
User Experienced Data Rate	10 Mbit/s	100 Mbit/s
Mobility	350 Km/h	500 km/h
Latency	10 ms	<1 ms
Connection Density	10^5 devices/km^2	10^6 devices/km^2
Area Traffic Capacity	0.1 Mbit/s/m^2	10 Mbit/s/m^2

Πίνακας 1- Συγκριτικός πίνακας 4G και 5G δικτύων.
Ελήφθη από το άρθρο «4G/5G: A Comparative Study and Overview on What to Expect from 5G».

Κάθε νέα γενιά δικτύου χαρακτηρίζεται από τη διαφορά -σε σχέση με την προηγούμενη γενιά- στη ταχύτητα μεταφοράς των δεδομένων και στις μεθόδους κωδικοποίησης. Για παράδειγμα, το δίκτυο $4^{ης}$ γενιάς είναι πάνω από πεντακόσιες (500) φορές ταχύτερο από ότι το $3^{ης}$ γενιάς, ενώ (όπως αναφέρθηκε ήδη) το $5^{ης}$ γενιάς μπορεί να αγγίξει και τις εκατό (100) φορές πάνω την ταχύτητα των δικτύων της $4^{ης}$ γενιάς.

Σε αυτό το σημείο χρήζει ιδιαίτερης μνείας ο διαχωρισμός που υφίσταται ανάμεσα στα δίκτυα 5G. Συγκεκριμένα, αναφερόμαστε στον βασικότερο διαχωρισμό

τους ήτοι την δικτύωση της Μη Αυτόνομης Αρχιτεκτονικής (Non-Stand Alone/NSA) και της Αυτόνομης Αρχιτεκτονικής (Stand-Alone/SA).

Η κύρια διαφοροποίησή τους είναι ότι η Μη Αυτόνομη Αρχιτεκτονική προωθείται δια μέσω του ελέγχου των ραδιοδικτύων 5G στο κυρίως δίκτυο 4G, ενώ, η Αυτόνομη Αρχιτεκτονική συνδέει το ραδιοσύστημα 5G απευθείας στο κυρίως δίκτυο 5G και η σηματοδότηση ελέγχου δεν εξαρτάται καθόλου από το δίκτυο 4G.

Η Μη Αυτόνομη Αρχιτεκτονική, όπως υποδηλώνει η ονομασία της, είναι μια υπηρεσία 5G η οποία δεν είναι "αυτόνομη" αλλά έχει κατασκευαστεί πάνω από ένα υπάρχον δίκτυο 4G. Η Αυτόνομη Αρχιτεκτονική, από την άλλη πλευρά, επιτρέπει την πλήρως ανεξάρτητη λειτουργία μιας υπηρεσίας 5G χωρίς καμία αλληλεπίδραση με έναν πυρήνα 4G.

Το 5G New Radio (5G NR) είναι υπεύθυνο για τη σύνδεση συσκευών στο δίκτυο και περιλαμβάνει σταθμούς βάσης που, με τη σειρά τους, συνδέονται στο κεντρικό δίκτυο. Το 5G NR διατηρεί τα χαρακτηριστικά του 5G σε σχέση με το διαχωρισμό σηματοδότησης και τη μεταφορά (επίπεδα χρήστη και ελέγχου), ακόμη και στο σύστημα διευθυνσιοδότησης, επιτρέποντας έτσι την απλοποίηση των διεπαφών και προσφέροντας τη δυνατότητα δημιουργίας «τμημάτων» (slices) στο Radio Access Plane.

Η υποστήριξη της δυνατότητας κατάτμησης ή τμηματοποίησης ενός δικτύου αποτελεί την νεότερη λειτουργικότητα σε σύγκριση με τις λύσεις που υφίστανται ήδη στα δίκτυα 4G. Το 5G NR χρησιμοποιεί αυστηρούς μηχανισμούς ασφάλειας που βασίζονται στην κρυπτογράφηση (για την εξασφάλιση της εμπιστευτικότητας των δεδομένων) και την ακεραιότητα. Αξίζει να σημειωθεί ότι τα κλειδιά ασφαλείας του 5G NR είναι σαφώς διαχωρισμένα από τα κλειδιά του 5G.

Σύμφωνα με εταιρεία δημιουργίας δικτύων, έχει αποδειχθεί ότι η μέγιστη εμβέλειας σήματος του δικτύου 5G (αναφερόμενοι στο δίκτυο Αυτόνομης Αρχιτεκτονικής (SA)) έχει τα 1.500 πόδια (ft) ή περίπου τα 500 μέτρα (m) και αυτά χωρίς την ύπαρξη εμποδίων σε αυτή την ακτίνα (“How far does 5G reach?,” 2020a). Η αδυναμία των σημάτων των χιλιομετρικών κυμάτων (mmWave) να διεισδύσουν σε εμπόδια περιορίζει περαιτέρω το εύρος των δυνατοτήτων, διότι τα εμπόδια αυτά θα πρέπει να ενσωματωθούν σε σχέδια δικτύων για τους μετακινούμενους χρήστες. Έχοντας υπόψη αυτά τα προβλήματα εύρους τιμών, πιθανολογείται βάσιμα ότι η λειτουργία χρήσης υποδομής LTE ή 5 G χαμηλής ζώνης μπορεί να παραμείνει συστατικό στοιχείο

των δικτύων 5G, με μόνο τους χρήστες που βρίσκονται κοντά στις κεραίες να αποκομίζουν τα πλήρη οφέλη.

Κάποιες λύσεις που προτείνονται στην παγκόσμια επιστημονική βιβλιογραφία είναι η χρήση τεχνολογίας μικρών κυψελών αντί του παραδοσιακού πύργου κυψελών μπορούν να χρησιμοποιηθούν αποτελεσματικά για να καταστήσουν βιώσιμα τα αυτόνομα δίκτυα 5G, δηλαδή η χρήση μικρών κυψελών (cells) η οποία θα συμβάλει στην παροχή σήματος 5G αυξάνοντας άμεσα την κάλυψη και την ταχύτητα του δικτύου. Αυτό σημαίνει ότι θα αναπτυχθεί τεράστιος αριθμός μικρών κυψελών (cells) 5G παντού γύρω μας (Al-Turjman et al., 2019).

Comparison	2G	3G	4G	5G
Introduced in year	1993	2001	2009	2018
Technology	GSM	WCDMA	LTE, WiMAX	MIMO, mm Waves
Access system	TDMA, CDMA	CDMA	CDMA	OFDM, BDMA
Switching type	Circuit switching for voice and packet switching for data	Packet switching except for air interference	Packet switching	Packet switching
Internet service	Narrowband	Broadband	Ultra broadband	Wireless World Wide Web
Bandwidth	25 MHz	25 MHz	100 MHz	30 GHz to 300 GHz
Advantage	Multimedia features (SMS, MMS), internet access and SIM introduced	High security, international roaming	Speed, high speed handoffs, global mobility	Extremely high speeds, low latency
Applications	Voice calls, short messages	Video conferencing, mobile TV, GPS	High speed applications, mobile TV, wearable devices	High resolution video streaming, remote control of vehicles, robots, and medical procedures

Πίνακας 2- Συγκριτικός πίνακας 2G, 3G, 4 G και 5G δικτύων.
Ελήφθη από: https://rantcell.com/comparison-of-2g-3g-4g-5g.html

3 Εισαγωγή στα δίκτυα 5G.

Για τη λειτουργία των δικτύων 5G χρειαζόμαστε τόσο τα Δίκτυα Ραδιοπρόσβασης (5G Radio Access Network- RAN) όσο και τα Κυρίως Δίκτυα (5G Core Network) τα οποία συνδέονται με τα δίκτυα 5G RAN.

Συγκεκριμένα, ένα Δίκτυο Ραδιοπρόσβασης (RAN) αποτελεί ένα σημαντικό στοιχείο ασύρματου τηλεπικοινωνιακού συστήματος, το οποίο έχει ως βασική λειτουργία τη σύνδεση διαφόρων διαφορετικών συσκευών, με άλλα μέρη του δικτύου, μέσω ραδιοζεύξης (radio link). Με άλλα λόγια, τα εν λόγω δίκτυα ουσιαστικά συνδέουν τις διάφορες ηλεκτρονικές συσκευές όπως κινητά, υπολογιστές κ.ά μέσω οπτικής ίνας ή ασύρματου σύνδεσης με το Κυρίως Δίκτυο (5G Core Network), το οποίο διαχειρίζεται στις πληροφορίες των συνδρομητών, την τοποθεσία και διάφορα άλλα στοιχεία (“What is a Radio Access Network (RAN)?,” n.d.)

Η μεγάλη διαφοροποίηση πραγματοποιήθηκε την δεκαετία του 2000’ όπου εισήχθη η λειτουργία των δικτύων 4G- LTE και άλλαξε η διαδικασία της ραδιοπρόσβασης και του κυρίως δικτύου και αυτό διότι για πρώτη φορά η διασύνδεση πραγματοποιήθηκε βασισμένη στο Πρωτόκολλο Διαδικτύου (Internet Protocol/ IP), σε αντικατάσταση των προηγούμενων δικτύων που βασίζονταν σε κυκλώματα.

Σύμφωνα με τους συγγραφείς του άρθρου σχετικά με τον ορισμό του Δικτύου Ραδιοπρόσβασης (“What is a Radio Access Network (RAN)?,” n.d.), τα εν λόγω δίκτυα απαρτίζονται από τρία (03) βασικά δεδομένα:

α) το ότι οι κεραίες μετατρέπουν τα ηλεκτρικά σήματα σε ραδιοκύματα,

β) ότι μετασχηματίζουν ψηφιακές πληροφορίες σε σήματα και ακολούθως αυτές οι πληροφορίες αποστέλλονται ασύρματα, διασφαλίζοντας ότι οι μεταδόσεις γίνονται στις σωστές ζώνες συχνοτήτων και

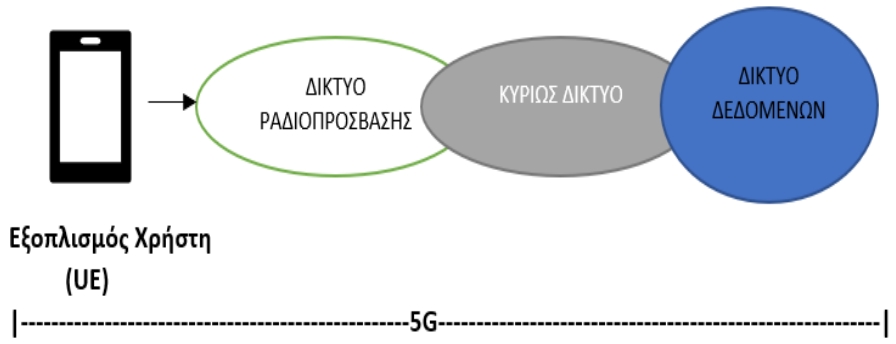
γ) ότι οι μονάδες βασικής ζώνης παρέχουν ένα σύνολο λειτουργιών επεξεργασίας σήματος με τέτοιο τρόπο ώστε να καθίσταται δυνατή η ασύρματη επικοινωνία.

Η διαφοροποίηση που πραγματοποιείται ουσιαστικά στην αρχιτεκτονική των εν λόγω δικτύων είναι ο διαχωρισμός του επιπέδου χρήστη (User Plane) και του επιπέδου ελέγχου (Control Plane). Με αυτή την αρχιτεκτονική επιτυγχάνεται η ανταλλαγή ενός συνόλου δεδομένων χρήστη μέσω λογισμικού δικτύωσης και παράλληλα ένα δεύτερο σύνολο μέσω διεπαφής ενός συστήματος ελέγχου. Όπως έχει ήδη αναφερθεί, με αυτόν τον τρόπο επιτυγχάνεται μεγαλύτερη ευελιξία, δίνοντας τη δυνατότητα εφαρμογής

τεχνολογιών όπως της «τμηματοποίησης δικτύου» (network slicing) και των υψηλών ρυθμών πολλαπλών εισόδων και εξόδων (MIMO), το οποίο αποτελεί μια μέθοδο για τον πολλαπλασιασμό της χωρητικότητας μιας ραδιοζεύξης με τη χρήση πολλαπλών κεραιών μετάδοσης και λήψης (Eye on Tech, 2019).

Μερικά από τα πλεονεκτήματα που απορρέουν από τη χρήση των δικτύων 5G, αποτελούν η υψηλή ταχύτητα, η υψηλή χωρητικότητα (πλήθος διασυνδεδεμένων συσκευών), η υψηλή αξιοπιστία, ο χαμηλός ρυθμός καθυστέρησης και η χαμηλή κατανάλωση ενέργειας (Liu et al., 2020). Τα προηγούμενα αναφερόμενα, έχουν ως συνέπεια την συνεχή και αδιάκοπη ροή υψηλής ποιότητας βίντεο, την επικοινωνία ανάμεσα στις συσκευές σε ένα περιβάλλον Διαδικτύου των Πραγμάτων (IoT), την μεγαλύτερη ακρίβεια στον γεωεντοπισμό, την χαμηλή καθυστέρηση στην επικοινωνία και την καλύτερη δυνατότητα ανάλυσης σε πραγματικό χρόνο (Dahiya, 2017). Επίσης, όπως έχει αναφερθεί, δίδεται η δυνατότητα με ένα μόνο δίκτυο 5G να δημιουργηθούν πολλά εικονικά δίκτυα (NFV) προσφέρει πολλαπλά οφέλη τόσο σε επιχειρήσεις όσο και στη λειτουργία για παράδειγμα αυτόνομων οχημάτων.

Από την άλλη έχουμε Κύρια Δίκτυα (5G Core Network) τα οποία συνδέονται, όπως αναφέρθηκε ανωτέρω, με τα δίκτυα 5G RAN. Τα δυο εν λόγω δίκτυα αποτελούν την νέα αρχιτεκτονική των δικτύων 5G. Μερικά από τα συστατικά μέρη της νέας αυτής αρχιτεκτονικής είναι οι Μονάδες Πρωτοκόλλου Δεδομένων (Protocol Data Unit/ PDU), οι ροές Ποιότητας Υπηρεσιών (Quality of Service/ QoS), οι Λειτουργίες Εικονικού Δικτύου (Network Functions Virtualization/NFV) και η «Τμηματοποίηση» Δικτύου (Network slicing/ NS).

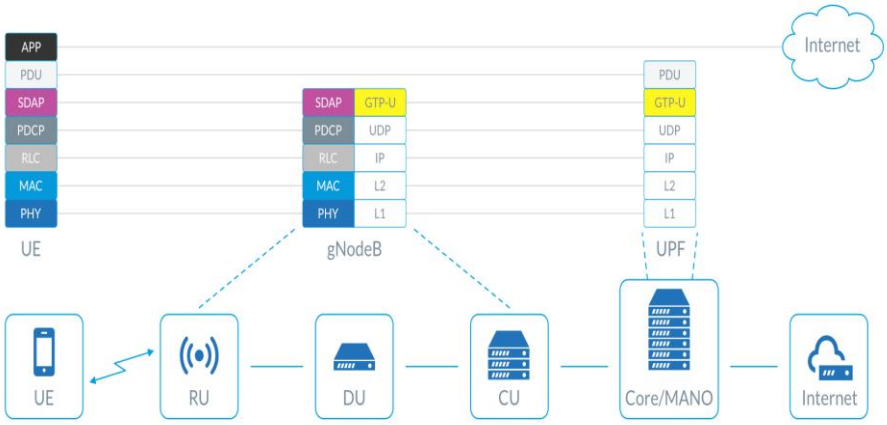


Εικόνα 1: Το δίκτυο 5G

πηγή: https://www.mpirical.com

Μια λεπτομερής απεικόνιση της αρχιτεκτονικής του Κυρίως (Core) Δικτύου 5G αποτελεί η εικόνα 2 σύμφωνα με την οποία παραθέτονται διάφορα στοιχεία του δικτύου συνδεδεμένα με διαφορετικά σημεία αναφοράς.

Αυτό που κυρίως παρατηρούμε στο εν λόγω διάγραμμα, είναι ότι η συνδεσιμότητα του αποκαλούμενου «User Plane» -το οποίο αποκαλείται PDU session δηλαδή η Μονάδα Πρωτοκόλλου Δεδομένων και παρουσιάζεται στην εικόνα 3 με την μπλε έντονη γραμμή- ξεκινάει από την συσκευή του χρήστη (User Equipment/ UE) και δια μέσω του gNB (Next Generation NodeB) (εικόνα 2) (το οποίο αποτέλεσε την αντικατάσταση του eNB στην αρχιτεκτονική των δικτύων 4G) περνάει στη UPF και εν τέλει στα Δεδομένα Δικτύου (Data Network).



Εικόνα 2: gNodeB 3GPP πρωτόκολλου για το User Plane.
Ελήφθη από: https://www.is-wireless.com/networks/software/gnodeb/

Με αυτόν τον τρόπο καμία άλλη συσκευή στο δίκτυο 5G δεν θα συνδέεται με το συγκεκριμένο PDU session, δηλαδή μια σύνδεση από άκρη σε άκρη (end-to-end) του user plane ανάμεσα στον εξοπλισμό του χρήστη (UE) και των Δεδομένων Δικτύου (Data Network) δια μέσω της Λειτουργίας Επιπέδου Χρήστη (UPF).

Προκειμένου να παρασχεθεί η λειτουργία της Ποιότητας Υπηρεσίας (QoS) μέσω του PDU session, έχουμε ροές QoS, δηλαδή ροές κυκλοφορίας του User Plane που θα λαμβάνει ένα συγκεκριμένο επίπεδο Ποιότητας Υπηρεσίας (QoS).

Λόγω του ότι υφίσταται η πιθανότητα να έχουμε κυκλοφορία διαφορετικών QoS τα οποία προκειμένου να τα διακρίνουμε, κάθε ροή έχει τη δική της ταυτότητα (ID). Για

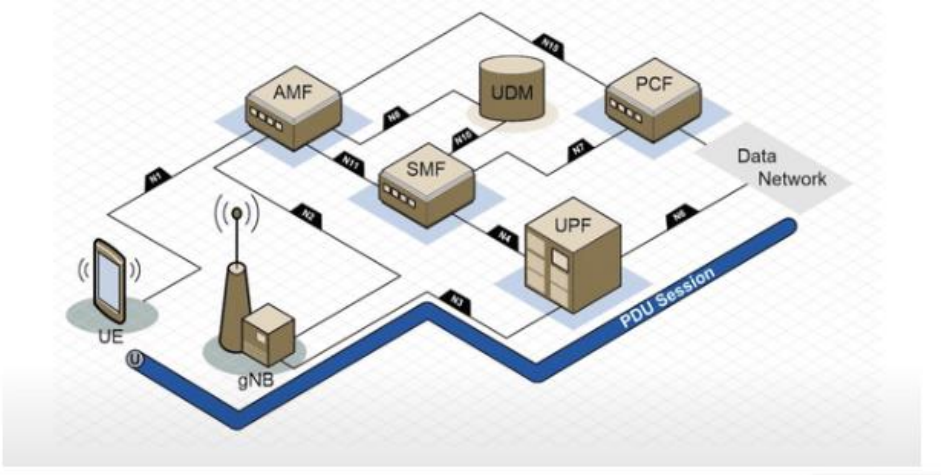
παράδειγμα, αν αναφερόμαστε στο πώς πραγματοποιείται η ανωτέρω διαδικασία με σύνδεση στο διαδίκτυο, τότε -θεωρητικώς- χρειαζόμαστε μόνο μια ροή QoS, η οποία θα μπορούσε να ήταν η προεπιλεγμένη ροή. Εάν από την άλλη αναφερόμασταν, για παράδειγμα, σε μια υπηρεσία ομιλίας μέσω 5G και τα δεδομένα δικτύου είναι το Διαδικτυακό Πρωτόκολλο Υποσυστήματος Πολυμέσων (IP Multimedia Subsystem/ IMS), δηλαδή η τεχνολογία που επιτρέπει στους παρόχους τηλεπικοινωνιακών υπηρεσιών να προσφέρουν μια νέα γενιά υπηρεσιών πολυμέσων, τότε μπορούμε να έχουμε μια ροή που μεταφέρει το σήμα το οποίο σχετίζεται με τη φωνή και έπειτα μια άλλη ροή η οποία μεταφέρει τα πραγματικά πακέτα φωνής.

Εν συνεχεία, έχουμε τη Λειτουργία Πρόσβασης Και Κινητικότητας η οποία αποτυπώνεται ως Access and Mobility Function/ AMF, η οποία παρουσιάζει ομοιότητες με την Οντότητα Διαχείρισης Κινητικότητας (Mobility Management Entity/ MME) στα δίκτυα 4G- LTE. Η εν λόγω λειτουργία έχει να κάνει με την κινητικότητα του χρήστη, την ασφάλεια και την εγγραφή του σε δίκτυο και έτσι είναι αυτή η λειτουργία η οποία πάντα γνωρίζει την περιοχή που βρίσκεται ο συνδρομητής ή το πιθανό κελί, κάτι το οποίο όμως πραγματικά εξαρτάται από το εάν ο συνδρομητής είναι αδρανής ή συνδεδεμένος. Επιπρόσθετα, το AMF παίζει σημαντικό ρόλο και στην ασφάλεια και στην εγγραφή ενός συνδρομητή στο δίκτυο, ουσιαστικά αναφερόμενοι στην αυθεντικοποίηση του συνδρομητή. Τέλος, η λειτουργία AMF, είναι αυτή που παρέχει μια προσωρινή ταυτότητα σε έναν συνδρομητή η οποία θα χρησιμοποιείται κάθε φορά που συνδέεται στο δίκτυο.

Ακολούθως, έχουμε τη Λειτουργία Διαχείρισης Συνεδριών (Session Management Function/ SMF), όπου έχουμε την ίδρυση και τροποποίηση των συνεδριών PDU (όπως αναφερθήκαμε ανωτέρω) η οποία εμπλέκεται άμεσα σε αυτό και ως μέρος του επικοινωνεί με τη Λειτουργία Ελέγχου (Policy Control Function/ PCF). Με αυτή τη διαδικασία προσδιορίζεται αν και πότε μια συγκεκριμένη συνεδρία δεδομένων του χρήστη επιτρέπεται να συνεχίσει.

Προσέτι δε, έχουμε τη Λειτουργία Ενοποιημένης Διαχείρισης Δεδομένων (Unified Data Management/ UDM), η οποία ουσιαστικά αποτελεί ένα κεντρικό αποθετήριο πληροφοριών του συνδρομητή, το οποίο συνδέεται άμεσα με την εξουσιοδότηση πρόσβασης διότι περιλαμβάνει τα κλειδιά ασφαλείας και το προφίλ των Δεδομένων Δικτύου. Κατ’ επέκταση αυτό που κάνει η Ενοποιημένη Διαχείριση

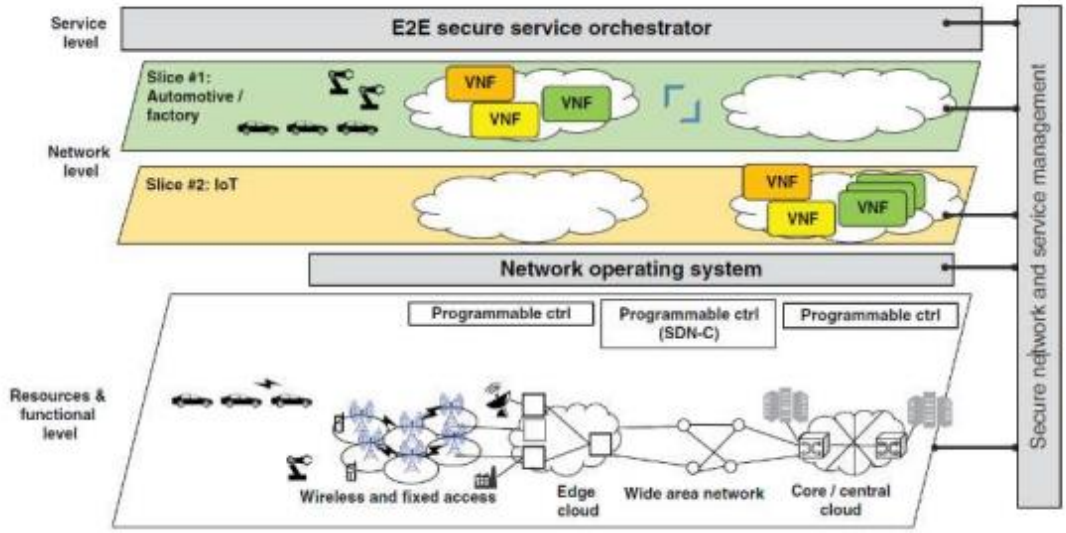
Δεδομένων είναι να αναφέρει στις λειτουργίες AMF και SMF τι επιτρέπεται και τι όχι να κάνει ένας συνδρομητής (Mpirical, 2019).



Εικόνα 3: Απεικόνιση αρχιτεκτονικής συστήματος δικτύου 5G.
Ελήφθη από: https://www.mpirical.com/

Σύμφωνα με την εικόνα 4, η αρχιτεκτονική του δικτύου πέμπτης γενιάς (5G) χωρίζεται σε τρία επίπεδα:

1) Επίπεδο Πόρων και Λειτουργιών (Resource & Functional Level),
2) Λειτουργικό σύστημα δικτύου και επίπεδο δικτύου (Network Operating System & Network level),
3) Επίπεδο Υπηρεσιών (Service Level).



Εικόνα 4: Γενική απεικόνιση της αρχιτεκτονικής του δικτύου 5G.
Πηγή: (https://www.academia.edu/ "A Review Of 5G Technology: Architecture, Security and wide Applications")

Η αρχιτεκτονική του 5G περιλαμβάνει μακρό ή μικροκύτταρα (macro-microcells), έτσι ώστε να επιτρέπεται η κάλυψη και η αύξηση της παραγωγικότητας όπως επίσης και η παροχή ομοιόμορφης συνδεσιμότητας του τελικού χρηστή. Οι κεραίες κατανεμημένες σε μεγάλες συστοιχίες αναλαμβάνουν το ρολό των σημείων πρόσβασης μικρών κελίων υποστηρίζοντας πολλαπλά πρωτοκολλά (RAN) για ένα ευρύ φάσμα. Στο εξωτερικό περιβάλλον οι χρηστές συνεργάζονται για τη δημιουργία εικονικών μεγάλων συστοιχιών κεραίας. Όλα αυτά μαζί καθόρισαν τη κατασκευή εικονικών massive MIMO συνδέσεων στα μικρά κελιά. Τα σημεία πρόσβασης μικρών κελίων συνδέονται blackhaul μέσω οπτικών ινών με το βασικό σταθμό βάσης (Base Stations/BS).

4 Επίπεδο, τύπος κρυπτογράφησης και ασφάλεια των δικτύων 4G- 5G.

Προκειμένου να αντιληφθούμε αρτιότερα τη λειτουργία των δικτύων 5G μελετήθηκαν άρθρα σχετικά με την ασφάλεια που παρέχεται στους χρήστες τόσο των δικτύων 4G όσο και των δικτύων 5G. Με αυτόν τον τρόπο μας δίδεται η δυνατότητα να κατανοήσουμε την διαφορά και την αναβάθμιση στο επίπεδο ασφάλειας που έχει συντελεστεί από τη μετάβαση από το 4G στο 5G δίκτυο.

Σύμφωνα με επιστημονικό άρθρο (Sullivan et al., 2021), τα δίκτυα 4G βελτίωσαν το τότε υπάρχων δίκτυο συμπεριλαμβάνοντας αξιόπιστες λύσεις οι οποίες στηρίζοντας εξ ολοκλήρου στο Πρωτόκολλο Διαδικτύου (IP). Οι υψηλότεροι ρυθμοί δεδομένων συγκριτικά με το παρελθόν έδωσαν τη δυνατότητα διαμοιρασμοί δεδομένων με συνεχόμενη ροή στο δίκτυο.

Οι νέες τεχνολογίες που εισήγαγε το 4G ήταν το Multimedia Messaging Service (MMS), η ψηφιακή μετάδοση βίντεο (DVB), η συνομιλία μέσω βίντεο, η υψηλής ανάλυσης περιεχομένου τηλεόραση και η κινητή τηλεόραση. Σύμφωνα με το εν λόγω άρθρο, τα δίκτυα 4G παρέχουν τα χαρακτηριστικά ασφαλείας που χρειάζονται για να μετριαστούν όλες οι επιθέσεις που έχουν αναγνωριστεί στα προηγούμενης γενιάς δίκτυα, με νέους κρυπτογραφικούς αλγόριθμους βελτιωμένων βασικών δομών (Dutta and Hammad, 2020).

Οι βασικοί κρυπτογραφικοί αλγόριθμοι που χρησιμοποιήθηκαν σε αυτά τα δίκτυα ήταν οι EPS Encryption Algorithms (EEA) και EPS Integrity Algorithms (EIA), ενώ χρησιμοποιήθηκαν κλειδιά μήκους 256-bits (το διπλάσιο δηλαδή μέγεθος αυτών που χρησιμοποιήθηκαν στα δίκτυα 3G) (Zou et al., 2016) (Piqueras Jover and Marojevic, 2019).

Μια άλλη βασική διαφορά των δικτύων 4G σε σύγκριση με τα παλαιότερα είναι ότι η κίνηση δεδομένων (traffic) του control και user plane εκμεταλλεύονται διαφορετικούς αλγόριθμους και μήκη κλειδιών. Επίσης, η αυθεντικοποίηση παρέχεται από το πρωτόκολλο Authentication and Key Agreement (AKA), όπου η ακεραιότητα και η προστασία από επαναλαμβανόμενες επιθέσεις εγγυόταν μέσω των πρωτοκόλλων-σημάτων NAS (Non-Access Stratum) και RRC (Radio Resource Control).

Το Internet Protocol Security (IPSec), δηλαδή η ασφαλής «σουίτα» πρωτοκόλλου δικτύου που πιστοποιεί και κρυπτογραφεί τα πακέτα δεδομένων για να παρέχει ασφαλή κρυπτογραφημένη επικοινωνία μεταξύ δύο υπολογιστών μέσω δικτύου πρωτοκόλλου Internet, χρησιμοποιούνταν στην κρυπτογράφηση της κίνησης του «πίσω μέρους» (backhaul) (Rommer et al., 2020). Παρόλα αυτά, λόγω της σύνδεσης του δικτύου κινητής τηλεφωνίας με το διαδίκτυο, εξαιτίας του πλαισίου IP από άκρη σε άκρη (end-to-end), ενώ επίσης τα δίκτυα 4G έχουν καταστεί πλέον ευάλωτα και έχουν εκτεθεί σε μεγάλο αριθμό επιθέσεων που προέρχονται από το διαδίκτυο (Idrissi et al., 2012), (Liyanage and Gurtov, 2012).

Όλοι οι φορείς επιθέσεων που στόχευαν στη βασική λειτουργία του πρωτοκόλλου IP αποτελούν τώρα επιλογές επίθεσης για τα δίκτυα κινητής τηλεφωνίας. Τέτοιου είδους παραδείγματα αποτελούν οι επιθέσεις τύπου address spoofing, TCP SYN flood, TCP RST και hijack, Denial of Service (DoS), κλοπή του ID χρήστη και επιθέσεις εισβολής (intrusion attacks) (Liyanage et al., 2013).

Η υψηλότερη υπολογιστική ισχύς των κινητών συσκευών δημιουργεί επίσης νέες επιλογές επιθέσεων, οι οποίες μπορούν να δημιουργηθούν από τις συσκευές στο δίκτυο κινητής τηλεφωνίας. Επιπλέον, από τη στιγμή που υποστηρίζουν 4G τεχνολογίες όπως το Wi-Fi και το WIMAX, «κληρονομούν» και όλα τα ζητήματα ασφάλειας αυτών των τεχνολογιών (Ferrag et al., 2018).

Ο διαχωρισμός ανάμεσα στα δίκτυα 5G σε RAN και CORE είναι σημαντικός για την εξέλιξή τους, λόγω του ότι το gNB (Next Generation NodeB), ουσιαστικά τερματίζει την κρυπτογράφηση των δεδομένων του χρήστη, εκτός και αν κρυπτογραφείται εξωτερικά και είναι εκτός του ελέγχου ενός διαχειριστή δικτύου 5G. Μέχρι στιγμής δεν υφίσταται ένας συγκεκριμένος κανόνας ή οδηγία σχετικά με το διαχωρισμό των λειτουργιών των δικτύων 5G RAN και CORE.

Επίσης, οι τεχνικές εξέλιξης όπως το κατανεμημένο RAN, το διαχωρισμένο RAN, το O- RAN κ.ά, κατακερματίζουν και διανέμουν την ανάπτυξη των λειτουργιών RAN, γεγονός το οποίο έχει αντίκτυπο στον τομέα της ασφάλειας. Για τον λόγο αυτό εξετάζεται και η ασφάλεια στον διαχωρισμό του gNB (“Whitepaper on security in 5G RAN and core deployment,” 2019).

Σύμφωνα με το ανωτέρω αναφερόμενο άρθρο (“Whitepaper on security in 5G RAN and core deployment,” 2019), τα τηλεπικοινωνιακά δίκτυα, όπως τα γνωρίζουμε, αποτελούνται από τέσσερα διακριτά μέρη: το RAN, το δίκτυο πυρήνα (core), ένα δίκτυο

μεταφοράς και ένα δίκτυο διασύνδεσης. Τα εν λόγω δίκτυα μεταφέρουν τρεις διαφορετικούς τύπους κίνησης, που συνήθως αναφέρονται ως επίπεδα. Το επίπεδο ελέγχου (control plane) μεταφέρει την κίνηση σηματοδότησης, το επίπεδο χρήστη (user plane) τα δεδομένα χρήστη (που είναι το περιεχόμενο των επικοινωνιών) και το επίπεδο διαχείρισης (management plane). Το τελευταίο, περιέχει εντολές διαμόρφωσης και ελέγχου για τις λειτουργίες RAN και Core. Η ασφάλεια του δικτύου είναι ζωτικής σημασίας για αυτά τα επίπεδα, καθώς και τα τρία είναι επιρρεπή σε διαφορετικούς τύπους απειλών.

Όπως είναι γνωστό, για τα δίκτυα 5G αποτελεί ζωτικής σημασίας η διασφάλιση συνδεσιμότητας και επικοινωνίας συσκευής με συσκευή M2M (machine-to-machine). Ορισμένες μελέτες, όπως αυτή που αναφέρεται στο άρθρο «The Facts on 5G» (Kennedy, 2019), υποστηρίζουν ότι το RAN αποτελεί σε μεγάλο βαθμό ασήμαντο μέρος ενός δικτύου 5G καθώς και ότι δεν δύναται να επηρεάσει την ακεραιότητα και την εμπιστευτικότητα του δικτύου. Την εν λόγω άποψη δεν ενστερνίζονται οι Karl Norrman και Patrik Teppo, συγγραφείς του άρθρου «Security in 5G RAN and core deployments» (“Whitepaper on security in 5G RAN and core deployment,” 2019), οι οποίοι υποστηρίζουν ότι από τεχνικής πλευράς είναι λάθος μια τέτοια θεώρηση καθώς το gNB αποτελεί το σημείο τερματισμού για την κρυπογράφηση και ενδεχομένως, το επίπεδο χρήστη (user plane) να προσπελαστεί σε αποκρυπτογραφημένο κείμενο στην περίπτωση που δε χρησιμοποιείται κρυπτογράφηση από άκρη-σε-άκρη (end-to-end).

Όπως αναφέραμε και παραπάνω, ο διαχωρισμός ενός δικτύου 5G σε διαφορετικά μέρη και δη ανάμεσα σε λειτουργίες RAN και Core θεωρείται ότι εξασφαλίζει την ασφάλεια του δικτύου. Παρόλα αυτά όμως ο ορισμός αυτών των λειτουργιών, όπως αναφέρονται και περιγράφονται στο 3GPP, λαμβάνουν ως δεδομένο ότι οι εν λόγω λειτουργίες έχουν εκ των προτέρων αναπτυχθεί με ασφάλεια. Θα πρέπει όμως να επισημανθεί ότι στην περίπτωση που αυτή η υπόθεση αποτύχει, τότε δεν θα έχει επιτευχθεί η ζητούμενη ασφάλεια.

Σύμφωνα με τα πρότυπα της 3GPP, η ασφάλεια στα δίκτυα 5G πραγματοποιείται με τρόπο «hop-by-hop», κατά την οποία τα δεδομένα του χρήστη κρυπτογραφούνται και αποκρυπτογραφούνται σε διαφορετικά επίπεδα λειτουργιών του δικτύου. Κατά πλειοψηφία, σύμφωνα με τους συγγραφείς του άρθρου, τα δεδομένα που μεταφέρονται δια μέσω του δικτύου είναι κρυπτογραφημένα, όμως σε πολλές περιπτώσεις μετατρέπονται σε κείμενο (cleartext).

Η ακεραιότητα της διαδικασίας μεταφοράς των δεδομένων μεταξύ μια συσκευής που χρησιμοποιεί το δίκτυο και ενός σταθμού βάσης (gNB), προστατεύεται και κρυπτογραφείται. Ακολούθως, η ίδια διαδικασία ασφαλείας πραγματοποιείται και κατά τη μεταφορά των δεδομένων από το σταθμό βάσης (gNB), μέσω του «backhaul» δικτύου και του κυρίως δικτύου. Με αυτή τη διαδικασία επιτυγχάνεται η ακεραιότητα και η εμπιστευτικότητα του επιπέδου χρήστη (user plane) και του επιπέδου ελέγχου (control plane), μεταξύ της συνδεδεμένης συσκευής στο δίκτυο, του σταθμού βάσης (gNB) και του κυρίως δικτύου. Επίσης, στα δίκτυα 5G, αλλά και στα 4G, το αποκαλούμενο «NAS» (Non-Access Stratum) (δηλαδή ένα σύνολο πρωτοκόλλων ασύρματων τηλεπικοινωνιών μεταξύ του κεντρικού δικτύου και του εξοπλισμού του χρήστη (“NAS,” n.d.)) κρυπτογραφείται.

Η μετάβαση στα δίκτυα 5G επιφέρει βελτιώσεις σε πολλαπλά επίπεδα, αφ ης στιγμής τα εν λόγω δίκτυα συνδυάζουν τη χρήση του 5G New Radio και ενός Δικτύου Μακροπρόθεσμης Εξέλιξης (LTE). Παρόλα αυτά όμως λόγω ακριβώς αυτού του συνδυασμού κληρονομούν και όλες τις ευπάθειες που εντοπίζονται στα δίκτυα LTE. Έτσι τα Μη Αυτόνομα Δίκτυα 5G θεωρούνται δίκτυα τα οποία είναι ευάλωτα σε επιθέσεις τύπου Denial Of Service (DoS).

Σύμφωνα με το κείμενο «5G SECURITY ISSUES» (“5G-Research_A4.pdf,” n.d.) η υποκλοπή εντός των δικτύων 5G είναι εφικτή όσο εφικτή είναι και στο διαδίκτυο και αυτό λόγω του ότι τα δίκτυα 5G χρησιμοποιούν -κατά κόρον- τα API πρωτόκολλα HTTP (HyperText Transfer Protocol) και REST (Representational State Transfer), τα οποία είναι ευρέως διαδεδομένα στο διαδίκτυο.

Με μια απλή στατιστική ανάλυση σύμφωνα με την οποία αναμένεται να έχουμε πάνω από είκοσι (20) δισεκατομμύρια συσκευές Διαδικτύου των Πραγμάτων (IoTs), καταλήγουμε ευλόγως στο συμπέρασμα ότι θα αυξηθούν δραματικά και οι επιθέσεις σε αυτές τις συσκευές, των οποίων η προστασία είναι σχετικώς φτωχή και η προσβολή τους από κακόβουλο λογισμικό σε έξαρση.

Από την άλλη πλευρά, η ασφάλεια που παρέχουν τα Αυτόνομα 5G δίκτυα (Standalone) δίδουν τη δυνατότητα για ακόμη μεγαλύτερο αριθμό διασυνδέσεων στο δίκτυο όπου συσκευές με διαφορετικές δυνατότητες και περιορισμούς στις ανάγκες περί ποιότητας υπηρεσιών (Ghosh et al., 2019). Ως εκ τούτου, το 5G αντιμετωπίζει επίσης τη συνεχώς αυξανόμενη ζήτηση των χρηστών για σύνδεση. Σε σύγκριση με τις προηγούμενες γενιές δικτύων, το 5G επιλύει έξι προκλήσεις, αυτή της υψηλότερης

χωρητικότητας, του υψηλότερου ρυθμό διακίνησης δεδομένων, μικρότερο χρόνο καθυστέρησης, μαζική συνδεσιμότητα συσκευών, μειωμένο κόστος και ποιότητα υπηρεσιών. Ταυτόχρονα, αυξήθηκαν και οι δυνατότητες των επιτιθέμενων σε σύγκριση με τις προηγούμενες γενιές δικτύων. Στην πραγματικότητα, η υπολογιστική ισχύς των σημερινών κινητών συσκευών επιτρέπει την έναρξη περίπλοκων επιθέσεων μέσα στο δίκτυο κινητής τηλεφωνίας.

5 Νόμιμη καταγραφή δεδομένων χρηστών των δικτύων 5G.

Προτού ξεκινήσουμε την αναφορά μας σχετικά με τη δράση των ιδιωτικών εταιρειών ανάπτυξης λογισμικού με το οποίο καταγράφονται τα δεδομένα των χρηστών των δικτύων 5G, θα προβούμε σε μια μικρή εισαγωγή σχετικά με τον τρόπο λειτουργίας και την διαδικασία που πραγματοποιείται η άρση του απορρήτου των επικοινωνιών των χρηστών- στόχων των δικτύων 5G.

Για οποιονδήποτε πάροχο τηλεπικοινωνιών, η νόμιμη καταγραφή δεδομένων (Lawful Interception /LI) πρέπει να ικανοποιεί αρκετά απαιτητικούς κανόνες και να πληρούνται όλες οι νομικές υποχρεώσεις. Η νόμιμη καταγραφή επιτρέπει στις αρμόδιες Αρχές να καταγράφουν το σύνολο των επικοινωνιών των συγκεκριμένων χρηστών-στόχων στο πρότυπο του 3GPP.

Σύμφωνα με έναν ορισμό που έχει δοθεί ως προς το τι είναι η καταγραφή επικοινωνιών των χρηστών, νόμιμη καταγραφή έχουμε όταν: «Οι νόμοι μεμονωμένων εθνών και περιφερειακών ιδρυμάτων, και μερικές φορές οι συνθήκες αδειοδότησης και λειτουργίας, ορίζουν την ανάγκη παρακολούθησης στοχευμένων επικοινωνιών και των σχετικών πληροφοριών στα συστήματα επικοινωνίας». Η νόμιμη παρακολούθηση εφαρμόζεται σύμφωνα με την ισχύουσα εθνική ή περιφερειακή νομοθεσία και συγκεκριμένους τεχνικούς κανονισμούς» (“Lawful Intercept (LI) in 5G System - Techplayon - 5G Network Architectures,” n.d.).

Προκειμένου να πραγματοποιηθεί η οποιαδήποτε διαδικασία καταγραφής δεδομένων χρηστών θα πρέπει να ικανοποιούνται μια σειρά από απαιτήσεις όπως οι κάτωθι:

1) Να επιτρέπεται στις Αρχές να λαμβάνουν τις απαραίτητες πληροφορίες από τα δίκτυα 5G μέσω νομικών διαδικασιών, σύμφωνα με συγκεκριμένες απαιτήσεις ασφαλείας, χωρίς διακοπή του τρόπου λειτουργίας και χωρίς να τίθεται σε κίνδυνο το απόρρητο των επικοινωνιών ώστε να μην υποκλαπούν,

2) Η διαδικασία της νόμιμης παρακολούθησης να επιτρέπει στις Αρμόδιες Αρχές να πραγματοποιούν καταγραφή των επικοινωνιών για συγκεκριμένους χρήστες συμπεριλαμβανομένου του πότε θα πραγματοποιείται η έναρξη και πότε η λήξη μιας καταγραφής δεδομένων καθώς και τον τρόπο που απαιτείται για τη διαδικασία της επισύνδεσης,

3) Όλες οι διαδικασίες να διέπονται και να περιλαμβάνονται σε αντίστοιχα Βουλεύματα του εκάστοτε Συμβουλίου Πλημμελειοδικών.

5.1 ETSI (European Telecommunications Standards Institute)

Όλες οι εταιρείες και οργανισμοί που παρέχουν, σε συνεργασία με τους παρόχους τηλεπικοινωνιών, τη δυνατότητα στις Αρχές Επιβολής του Νόμου να λαμβάνουν τα δεδομένα της νόμιμης καταγραφής, διέπονται από κανόνες και στάνταρτ τα οποία ρυθμίζονται από το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Δεδομένων ETSI (European Telecommunications Standards Institute) (“ETSI - Welcome to the World of Standards!,” n.d.).

Η Ευρωπαϊκή Ένωση, επισήμως αναγνωρίζει την ETSI ως τον επίσημο ευρωπαϊκό οργανισμό. Η ETSI αποτελεί έναν οργανισμό που έχει μέλη συνεργαζόμενα μέλη σε όλες τις ηπείρους ανά την υφήλιο. Η ETSI διαδραμάτισε σημαντικό ρόλο ως προς τις προδιαγραφές και την κατεύθυνση που θα έπρεπε να ακολουθήσουν τα νομίμως υποκλαπέντα δεδομένα. Το 3rd Generation Partnership Project (3GPP) αποτελεί ένα έργο συνεργασίας της ETSI το οποίο οργανώθηκε ως κοινοπραξία επτά (7) παγκόσμιων οργανισμών τηλεπικοινωνιακών προτύπων που προωθούν τη συνεργασία μεταξύ Ευρώπης, Βόρειας Αμερικής, Ιαπωνίας, Ινδίας, Κίνας και Νότιας Κορέας. Ουσιαστικά το 3GPP οριοθέτησε όλα τα πρότυπα που σχετίζονται με τα δίκτυα κινητής τηλεφωνίας και τις υπηρεσίες κινητής επικοινωνίας από 2G έως 5G.

5.2 Τεχνολογία, αρχιτεκτονική και διαδικασία της νόμιμης καταγραφή χρηστών δικτύων 5G.

Το 3GPP παρέχει λεπτομέρειες και εξειδικεύσεις σχετικά με τους κανονισμούς και τις διαδικασίες που διέπουν τη νόμιμη καταγραφή δεδομένων στα δίκτυα 5G.

Σύμφωνα με την επίσημη ιστοσελίδα του 3GPP σχετικά με τον ορισμό και το ρόλο που διαδραματίζει αυτή η παγκόσμια συνεργασία, το εν λόγω το ακρωνύμιο ορίζεται από τα αρχικά των λέξεων 3rd Generation Partnership Project (“About 3GPP Home,” n.d.). Ενώνει επτά (7) οργανισμούς ανάπτυξης τηλεπικοινωνιακών προτύπων (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), γνωστούς ως «Organizational Partners»

και παρέχει στα μέλη τους ένα σταθερό περιβάλλον για την παραγωγή των Αναφορών και των Προδιαγραφών που ορίζουν τις τεχνολογίες 3GPP. Το έργο καλύπτει τεχνολογίες κυψελωτών τηλεπικοινωνιών, συμπεριλαμβανομένης της ραδιοπρόσβασης, του βασικού δικτύου και των δυνατοτήτων υπηρεσιών, οι οποίες παρέχουν μια πλήρη περιγραφή του συστήματος για τις κινητές τηλεπικοινωνίες. Οι προδιαγραφές 3GPP παρέχουν επίσης άγκιστρα για μη ραδιοφωνική πρόσβαση στο κεντρικό δίκτυο και για διασύνδεση με δίκτυα εκτός 3GPP.

Ο αρχικός σκοπός του 3GPP το έτος 1998 ήταν η παραγωγή Τεχνικών Προδιαγραφών και Τεχνικών Αναφορών για ένα Κινητό Σύστημα 3G που βασίζεται σε εξελιγμένα δίκτυα πυρήνα GSM και στις τεχνολογίες ραδιοπρόσβασης που υποστηρίζουν. Το πεδίο εφαρμογής τροποποιήθηκε στη συνέχεια για να συμπεριλάβει τη συντήρηση και την ανάπτυξη των Τεχνικών Προδιαγραφών και των Τεχνικών Αναφορών για τις εξελιγμένες τεχνολογίες 3GPP, πέρα από το 3G.

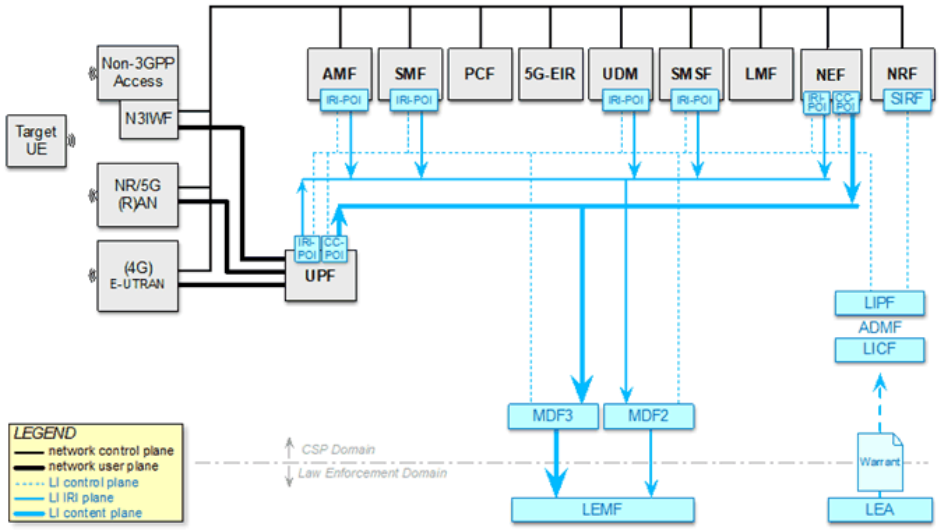
Η παραγωγή προδιαγραφών και μελετών του 3GPP βασίζεται στη συνεισφορά, από εταιρείες-μέλη, σε ομάδες εργασίας και σε επίπεδο Ομάδας Τεχνικών Προδιαγραφών (Technical Specification Group / TSG). Η κύρια εστίαση σε όλες τις εκδόσεις 3GPP είναι να γίνει το σύστημα συμβατό, για να διασφαλιστεί ότι η λειτουργία του εξοπλισμού χρήστη είναι αδιάλειπτη. Για το 5G, πολλοί πάροχοι ξεκινούν με διπλή συνδεσιμότητα μεταξύ του εξοπλισμού LTE και 5G NR - χρησιμοποιώντας την τεχνολογία των «Non-Standalone» δικτύων 5G.

Η λειτουργία του 3GPP για τα δίκτυα 5G αποτελείται από τρία μέρη:

α) σε αυτό σχετικά με τις τεχνικές απαιτήσεις και διέπεται από τον κανονισμό ETSI TS 133 126 V16.2.0 (2020-11),

β) σε αυτό σχετικά με την αρχιτεκτονική και τις λειτουργίες και διέπεται από τον κανονισμό ETSI TS 133 127 V16.6.0 (2021-01) και

γ) σε αυτή σχετικά με τα πρωτόκολλα και τις διαδικασίες και διέπεται από τον κανονισμό ETSI TS 133 128 V16.5.0 (2021-01).



Εικόνα 5: Απεικόνιση της αρχιτεκτονικής του δικτύου 5G κατά τη διαδικασία της νόμιμης καταγραφής δεδομένων.

πηγή: https://www.etsi.org ETSI TS 133 127 V16.6.0 (2021-01)

Στην παραπάνω εικόνα παρατηρούμε την αρχιτεκτονική του δικτύου 5G κατά τη διαδικασία της νόμιμης καταγραφής δεδομένων όπου οι λειτουργίες του δικτύου απεικονίζονται με γκρι χρώμα, ενώ τα στοιχεία της νόμιμης καταγραφής, τα οποία θα καταλήξουν στις Αρχές Επιβολής του Νόμου, με μπλε χρώμα.

Επισημαίνεται ότι αναφερόμαστε στα StandAlone (SA) 5G δίκτυα όπου έχουμε τη λειτουργία ελέγχου (Control Plane/ CP), δηλαδή τις βασικές λειτουργίες του δικτύου, ήτοι τις λειτουργίες Access and Mobility Functions (AMF), Session Management Functions (SMF), Policy Control Functions (PCF), Network Slice Session Functions (NSSF), 5G Equipment Id Register (5G-EIR), Unified Data Management (UDM), SMS Functions (SMSF), Location Management Functions (LMF) και Network Repository Functions (NRF), τα οποία ενεργοποιούνται και χρησιμοποιούνται σε κάθε συνεδρία.

Από την πλευρά της λειτουργίας χρήστη (User Plane/ UP) έχουμε τη λειτουργία του User Plane Function (UPF) και πέρα από αυτό υφίσταται και ένα Δίκτυο Δεδομένων (Data Network/ DN) το οποίο δε απαιτείται από τις Αρχές Επιβολής του Νόμου.

Στην αριστερή πλευρά της παραπάνω εικόνας έχουμε το 5G New Radio ή αλλιώς gNB ή θα μπορούσε να υπάρξει σύνδεση ακόμη και LTE στο δίκτυο του 5G Core το οποίο αναγράφεται και ως eLTE. Επιπρόσθετα, αναφέρεται ότι θα μπορούσε να υπάρξει

μια Non- 3GPP σύνδεση- πρόσβαση στο δίκτυο του 5G Core, ενώ επίσης σημειώνεται ότι θα μπορούσε να υπάρξει οποιαδήποτε σύνδεση στο δίκτυο 5G.

Από πλευράς των συστατικών μερών που απαρτίζουν τη λειτουργία της νόμιμης καταγραφής δεδομένων για τις Αρχές Επιβολής του Νόμου, τα «Σημεία Καταγραφής Δεδομένων» (Points of Interception/POI), δηλαδή η λειτουργία δικτύου που υποστηρίζει την καταγραφή δεδομένων, έχουμε δυο (2) ειδών:

α) τις «Πληροφορίες σχετικά με τα Καταγεγραμμένα Δεδομένα» (Intercepted Related Information/IRI) οι οποίες παρέχονται στο MDF2 και

β) την «Λειτουργία Περιεχομένου Συνομιλίας» (Call Content/CC) οι οποίες παρέχονται στο MDF3.

Τα «Σημεία Καταγραφής Δεδομένων» μπορούν να έχουν τους εξής συνδυασμούς: POI- CC, POI-IRI, IRI-CC, κάτι το οποίο εξαρτάται από το εάν βρίσκεται στη λειτουργία Control Plane (CP) ή User Plane (UP). Τόσο οι συνδυασμοί POI- CC όσο και POI-IRI είτε μπορούν να παρασχεθούν άμεσα είτε να πυροδοτηθούν.

Για παράδειγμα, το Access and Mobility Function (AMF) θα γνωρίζει την τοποθεσία μιας συγκεκριμένης συσκευής ή ενός πελάτη- χρήστη που διερευνάται, στοιχεία τα οποία υφίστανται και λαμβάνονται από το συνδυασμό POI-IRI.

Παρόμοια λειτουργία έχουμε και στο Session Management Function (SMF), όπου παραγγέλλει στο User Plane Function (UPF) να δημιουργήσει μια συνεδρία δεδομένων (Data Session) ή να τροποποιήσει μια συνεδρία δεδομένων ή να τερματίσει μια συνεδρία δεδομένων, λαμβάνοντας στοιχεία τα οποία παρέχονται από τον συνδυασμό POI-IRI.

Ακολούθως, παρόμοια λειτουργία έχουμε και από στο Unified Data Management (UDM) στο οποίο υφίσταται το προφίλ των πελατών- χρηστών, πληροφορίες οι οποίες παρέχονται από το IRI, ενώ, τέλος η ίδια λειτουργία με αντίστοιχα στοιχεία δεδομένων που δίδεται από τον συνδυασμό POI-IRI έχουμε και από το SMS Functions (SMSF).

Σημειώνεται ότι το «Περιεχόμενο Συνομιλιών» (Call Content/CC) θα βρίσκεται πάντα στο User Plane (UP) στο οποίο, όπως παρατηρείται και στην εικόνα 13, υφίσταται ο συνδυασμός CC- POI, το οποίο μπορεί να έχει επίσης και κάποια Μεταδεδομένα (Metadata) και για αυτό το λόγο εντός της λειτουργίας User Plane (UP) υφίσταται και ο συνδυασμός POI-IRI. Ο συνδυασμός POI-IRI μπορεί να αποτελεί μέρος τόσο της ίδιας συνεδρίας όσο και διαφορετικής συνδεδεμένη μεμονωμένα για παράδειγμα στη λειτουργία AMF.

Στη δεξιά πλευρά της παραπάνω εικόνας κάτω από την διακεκομμένη γραμμή έχουμε τον τομέα των Αρχών Επιβολής του Νόμου και πάνω από αυτή (τη γραμμή) έχουμε τον τομέα των Παρόχων Τηλεπικοινωνιών (Communication Service Provider/CSP). Στον τομέα των Παρόχων Τηλεπικοινωνιών έχουμε τη λειτουργία του Administration Function (ADMF). Η λειτουργία αυτή αποτελείται από δυο (2) συστατικά μέρη, το ένα είναι η «Λειτουργία Ελέγχου Καταγραφής Δεδομένων» (Lawful Interception Control Function/ LICF) και το άλλο η «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF).

Η εν λόγω λειτουργία (ADMF) λαμβάνει το Βούλευμα του Δικαστικού Συμβουλίου είτε εγγράφως, είτε μέσω κρυπτογραφημένου ηλεκτρονικού μηνύματος ή με οποιονδήποτε άλλο τρόπο. Ακολούθως, η «Λειτουργία Ελέγχου Καταγραφής» (Lawful Interception Control Function/LICF) καταγράφει όλους του στόχους δημιουργώντας μια λίστα, αναπτύσσει νέες λειτουργίες με δυνατότητες καταγραφής και τέλος υλοποιεί τις υποδομές καταγραφής δεδομένων των δοθέντων στόχων. Από την άλλη, η «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF) παρέχει λειτουργίες ούτως ώστε να δύναται να πραγματοποιηθεί η καταγραφή δεδομένων. Όταν αναφερόμαστε στη «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων», ουσιαστικά αναφερόμαστε στην παροχή ενός ιδιαίτερου «Σημείου Καταγραφής Δεδομένων» (Point of Interception/POI). Η «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF) λαμβάνει «εντολή» να προβεί στην οποιαδήποτε παροχή δεδομένων από τη «Λειτουργία Ελέγχου Καταγραφής» (Lawful Interception Control Function/LICF) και έτσι ακολούθως ενεργοποιούνται και παρέχονται τα δεδομένα IRI, CC ή και τα δυο ταυτόχρονα τα οποία μεταφέρονται για αξιοποίηση στις Αρχές Επιβολής του Νόμου.

Όπως αναφέρθηκε και παραπάνω, η παράδοση των δεδομένων που ζητήθηκαν και παρασχέθηκαν γίνεται προς τη «Λειτουργία Διαμεσολάβησης και Παράδοσης» (Mediation/ Delivery Function/ MDF), η οποία διαχωρίζεται σε MDF2 η οποία περιέχει όλα τις πληροφορίες δεδομένων του IRI- xIRI και MDF3 η οποία περιέχει όλα τα δεδομένα των φωνητικών κλήσεων (φωνητικού περιεχομένου) CC- xCC. Από αυτή τη λειτουργία παραδίδονται τα δεδομένα στη «Λειτουργία Παρακολούθησης Δεδομένων» (Law Enforcement Monitoring Function/ LEMF) των Αρχών του Νόμου. Παράλληλα, μεταφέρονται και ειδικά μεταδεδομένα όπως η ταυτότητα δικτύου (network id),

χρονοσφραγίδα (timestamp), νόμιμη καταγραφή ταυτότητας (lawful Intercept Id) και άλλες σχετιζόμενες πληροφορίες.

Σύμφωνα και με την εικόνα 4, απεικονίζεται η αρχιτεκτονική και ο τρόπος λειτουργίας της καταγραφής δεδομένων των χρηστών των δικτύων 5G, όπου η έντονη μπλε γραμμή αποτελεί τη μεταφορά των δεδομένων των φωνητικών κλήσεων (Call Content), ενώ η πιο λεπτή γραμμή αποτελεί τη μεταφορά όλων των λοιπών δεδομένων.

Με αυτή τη διαδικασία παρέχονται όλα τα «Σημεία Καταγραφής» οποιουδήποτε στόχου στις Αρχές Επιβολής του Νόμου, είτε ο στόχος προβεί στην πραγματοποίηση φωνητικής κλήσης, είτε κλήσης δεδομένων, είτε συνδεθεί στο διαδίκτυο.

Όσον αφορά τα «Σημεία Καταγραφών Δεδομένων» (Points of Interception/ POI) συγκεντρωτικά αναφέρουμε ότι πραγματοποιούν τις εξής λειτουργίες α) είναι αυτά που αναγνωρίζουν τον στόχο του οποίου οι επικοινωνίες θα καταγραφούν, β) διοχετεύει όλες τις πληροφορίες των καταγεγραμμένων δεδομένων (IRI) του χρήστη- στόχου, γ) διοχετεύει όλες τις πληροφορίες του περιεχομένου των επικοινωνιών (CC)του χρήστη-στόχου, δ) διοχετεύει όλα τα στοιχεία που συλλέχθηκα από το σημείο καταγραφής δεδομένων (POI), το οποίο αναφέρεται ως xIRI, στο MDF2 και ως xCC στο MDF3, ε) το αποτέλεσμα του σημείου καταγραφής δεδομένων καθορίζεται από τον τύπο της λειτουργίας δικτύου που σχετίζεται με αυτό το σημείο, στ) ένα σημείο καταγραφής δεδομένων μπορεί να είναι ενσωματωμένο σε μια λειτουργία δικτύου ή να είναι ξέχωρα από τη λειτουργία δικτύου με την οποία σχετίζεται και τέλος ζ) πολλαπλά σημεία καταγραφής δεδομένων μπορεί να χρειαστεί να εμπλακούν στην εκτέλεση ενός Βουλεύματος.

Επιπρόσθετα, σημειώνεται ότι ένας ακόμη διαχωρισμός των POIs πραγματοποιείται:

α) σε αυτά που παρέχονται απευθείας από τη «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF), όπου τα άμεσα παρεχόμενα POI αναγνωρίζουν τις επικοινωνίες του στόχου που πρέπει να καταγραφούν και παρέχουν τις σχετικές πληροφορίες που κατεγράφησαν ή το περιεχόμενο της επικοινωνίας τους από το στόχο και

β) σε αυτά που χρειάζεται να πυροδοτηθούν πρώτα από μια αντίστοιχη λειτουργία πυροδότησης. Τα πυροδοτημένα POI αναγνωρίζουν τις επικοινωνίες του στόχου στηριζόμενα στην πυροδότηση που έλαβαν από μια σχετιζόμενη λειτουργία

πυροδότησης και έπειτα αποστέλλουν τα στοιχεία IRI ή CC των εν λόγω επικοινωνιών αναλόγως του τύπου του σημείου POI.

5.3 Καταγραφή δεδομένων στα δίκτυα 4G. Αρχιτεκτονική του 5G EPC «Εξελιγμένου Πακέτου Πυρήνα» (Evolved Packet Core).

Προκειμένου να κατανοήσουμε αρτιότερα την αρχιτεκτονική και τον τρόπο λειτουργίας της καταγραφής δεδομένων στα δίκτυα 5G, θα προβούμε σε μια σύντομη περιγραφή της εν λόγω διαδικασίας που υφίσταντο στα δίκτυα πριν του 5G, δηλαδή του 4G.

Σύμφωνα με το άρθρο «Towards 5G cellular network forensics» του Filipo Sharevski (Sharevski, 2018), αναφέρονται μηχανισμοί της ψηφιακής εγκληματολογίας ως προς την καταγραφή δεδομένων και τον γεω-εντοπισμό χρηστών μέσω των δικτύων LTE και LTE-Advanced, ενώ, παράλληλα αναφέρονται και τα σχετικά εργαλεία που χρησιμοποιούνται για εγκληματολογική ανάλυση.

Οι καταγραφές που πραγματοποιούνται σε δεδομένα ενός δικτύου κινητών τηλεφώνων δύναται να διαχωριστούν σε πραγματικό χρόνο (real time) και μη πραγματικό χρόνο (non-real-time). Οι real time έρευνες πραγματοποιούνται με στοιχεία τα οποία μεταφέρονται μέσω του δικτύου «εν τω πράττεσθαι», αναφερόμενοι στη ζωντανή παρακολούθηση μιας κλήσης, ενός browsing sessions ή στον γεωεντοπισμό ενός χρήστη. Οι non-real-time έρευνες αναφέρονται σε στοιχεία που προκύπτουν σε σχέση με αντίστοιχη παρελθοντική δραστηριότητα του ερευνώμενου χρήστη. Οι επιχειρήσεις αυτές πραγματοποιούνται με δυο μηχανισμούς, με την αναφερόμενη στην ξενόγλωσση βιβλιογραφία ως Lawful Interception (LI), δηλαδή την νόμιμη επισύνδεση χρηστών και την Lawful Access Location Services (LALS), δηλαδή την νόμιμη πρόσβαση στην υπηρεσία τοποθεσίας (Sharevski, 2018).

Όσον αφορά την νόμιμη καταγραφή δεδομένων χρηστών των δικτύων 4G, επισημαίνεται ότι η ταυτότητα του χρήστη (ID) συγκεκριμενοποιείται είτε με τον αριθμό MSISDN, είτε με τον IMSI, είτε με τον IMEI ή με συνδυασμό αυτών. Ακολούθως, οι πάροχοι μπορούν να καταγράφουν δυο τύπους δεδομένων των χρηστών των κινητών

τηλεφώνων, την κίνηση του χρήστη (user traffic) και την κίνηση του του σήματός του (signaling traffic).

Τα καταγεγραμμένα δεδομένα της κίνησης του χρήστη (user traffic), αναφέρονται ως Content of Communication (CC) και παραδίδονται πάνω από το HI3 σε μια προκαθορισμένη μορφή στην υπηρεσία καταγραφής δεδομένων των Αρχών Επιβολής του Νόμου (LEMF), όπως π.χ. ήχος ή αρχεία δεδομένων τα οποία χρησιμοποιούνται.

Τα δεδομένα της κίνησης του σήματος (signaling traffic), αναφέρονται ως Interception-Related Information (IRI) και παραδίδονται μέσω του HI2 με διαφόρους τύπους. Οι τύποι των εν λόγω δεδομένων μπορεί να καταγράφουν την ώρα και την ημέρα (LocalTimeStamp attribute) όπου η ταυτότητα του «στόχου» εγγράφηκε, την αποσύνδεση από το δίκτυο την απενεργοποίηση του κινητού τηλεφώνου, εάν ο στόχος βγάλει την κάρτα SIM, πληροφορίες τοποθεσίας, κ.ά.

Επίσης, τα δεδομένα τα οποία καταγράφονται γενικώς είναι τα εξής: η Διεθνής Ταυτότητα Συνδρομητή Κινητής Τηλεφωνίας- International Mobile Subscriber Identity (IMSI), η Διεθνής Ταυτότητα Εξοπλισμού Κινητής Συσκευής- International Mobile Equipment Identity (IMEI), ο Σταθμός Κινητής Τηλεφωνίας Ολοκληρωμένου Ψηφιακού Δικτύου Υπηρεσιών- -Mobile Station Integrated Services Digital Network (MSISDN), η διεύθυνση IP πηγής και προορισμού, θύρες πηγής και προορισμού, APNs, οι τηλεφωνικοί αριθμοί των καλούντων και καλουμένων, τα κελία που ενεργοποιούνται, τις περιοχές που καταγράφονται, αποστολείς και λήπτες SMS, περιεχόμενο των SMS, καθώς και ημερομηνία, ώρα και διάρκεια των καταγεγραμμένων δεδομένων.

Σχετικά με το IRI, αναφέρεται ότι αυτός απαρτίζεται από τα κάτωθι:

• IRI-BEGIN- Το πρώτο γεγονός μιας προσπάθειας αναγνώρισης της ταυτότητας στόχου.

• IRI-END- Το τέλος μιας προσπάθειας επικοινωνίας. κλείσιμο της συναλλαγής IRI.

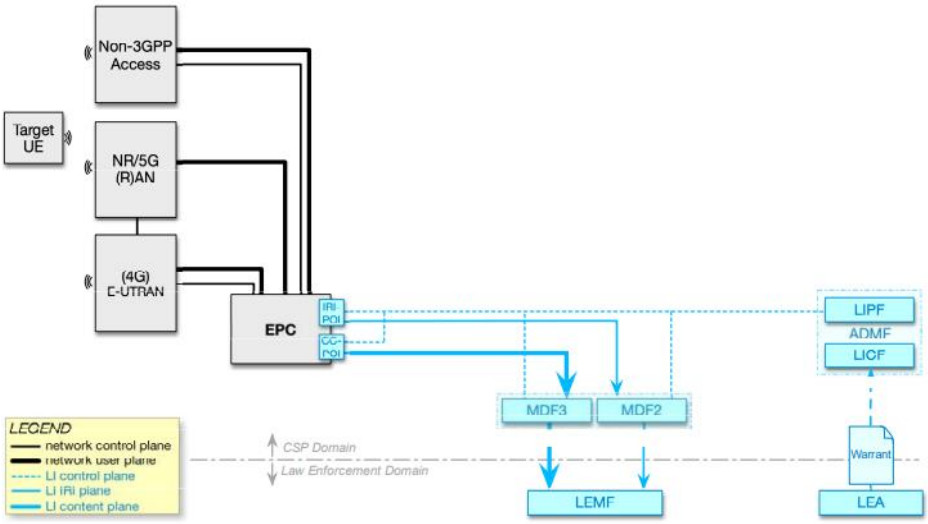
• IRI-CONTINUE- Καταγραφή διαμεσολαβητή ανά πάσα στιγμή κατά τη διάρκεια μιας επικοινωνίας στο πλαίσιο της

συναλλαγής IRI.

• IRI-REPORT εγγραφή- Χρησιμοποιείται για συμβάντα που δεν σχετίζονται με την επικοινωνία, για παράδειγμα, αιτήματα σύνδεσης δικτύου.

Όσον αφορά την νόμιμη πρόσβαση στην υπηρεσία τοποθεσίας (Lawful Access Location Services (LALS)), είναι μια ενέργεια που εκτελείται από έναν φορέα

εκμετάλλευσης δικτύου κινητής τηλεφωνίας για τη διάθεση πληροφοριών τοποθεσίας. Τα δίκτυα κινητής τηλεφωνίας παρέχουν Υπηρεσίες τοποθεσίας (LCS) που χρησιμοποιούν τη γεωγραφική θέση του χρήστη. Για το σκοπό αυτό, τα κυψελωτά δίκτυα εφαρμόζουν μια αρχιτεκτονική υπηρεσίας τοποθεσίας LCS με LMU (Location Measurement Unit) στο ραδιοδίκτυο για την εκτέλεση της μέτρησης εντοπισμού και η Εξυπηρέτηση Κινητού Κέντρου Τοποθεσίας- Serving Mobile Location Center (SMLC) στο κεντρικό δίκτυο για να επικοινωνούν τις πληροφορίες τοποθεσίας με τους πελάτες LCS. Τα SMLC διακινούν τα αιτήματα εντοπισμού χρησιμοποιώντας το πρωτόκολλο LPP στα LMU, τα οποία με τη σειρά τους συντονίζονται με τις ταυτότητες στόχων για να υπολογίσουν την τρέχουσα θέση τους. Η τοποθεσία του χρήστη υπολογίζεται χρησιμοποιώντας οποιαδήποτε από αυτές τις μεθόδους εντοπισμού.



Εικόνα 6: Απεικόνιση αρχιτεκτονικής του 4G EPC (Evolved Packet Core) «Εξελιγμένου Πακέτου Πυρήνα».

πηγή: https://www.etsi.org ETSI TS 133 127 V16.6.0 (2021-01)

Το δίκτυο 5G αποτελεί ένα δίκτυο στο οποίο δύναται να πραγματοποιούνται όλων των ειδών οι συνδέσεις δικτύου. Για παράδειγμα έχουμε το δίκτυο 4G Core συνδεδεμένο στην πλευρά του Radio ακόμα και του 5G Radio. Η αρχιτεκτονική που

ακολουθείται για τη διαδικασία της νόμιμης καταγραφής δεδομένων και εδώ είναι παρόμοια με την αρχιτεκτονική που περιγράφηκε παραπάνω για τα δίκτυα 5G.

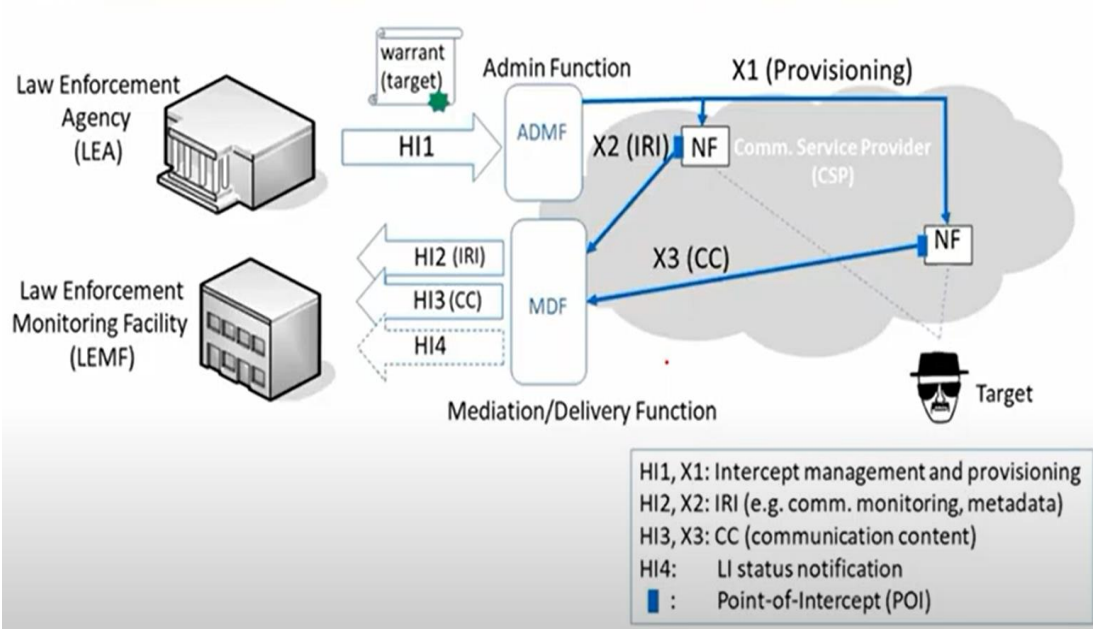
Συγκεκριμένα, έχουμε τη λειτουργία Administration Function (ADMF), η οποία και εδώ αποτελείται από δυο (2) μέρη, τη «Λειτουργία Ελέγχου Καταγραφής Δεδομένων» (Lawful Interception Control Function/ LICF) και τη «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF).

Επίσης, ομοιότητα έχουμε και στη λειτουργία τη «Διαμεσολάβησης και Παράδοσης» (Mediation/ Delivery Function/ MDF), η οποία διαχωρίζεται σε MDF2 και MDF3.

Επιπρόσθετα, έχουμε την λειτουργία του «Εξελιγμένου Πακέτου Πυρήνα» (Evolved Packet Core/ EPC) όπου ενεργοποιούνται και παρέχονται τα δεδομένα IRI, CC και εν συνεχεία μεταφέρονται, μέσω της λειτουργίας «Διαμεσολάβησης και Παράδοσης», στη «Λειτουργία Παρακολούθησης Δεδομένων» (Law Enforcement Monitoring Function/ LEMF) των Αρχών Επιβολής του Νόμου. Σημειώνεται ότι τα δεδομένα IRI που παρέχονται δεν έχουν το εύρος των δεδομένων που παρέχονται στα δίκτυα 5G.

Στα δίκτυα 4G όταν έχουμε την «Πύλη δικτύου πακέτων δεδομένων» (Packet Data Network Gateway/ PGW) το οποίο αποτελεί έναν κόμβο δικτύου που συνδέει το «Εξελιγμένο Πακέτο Πυρήνα» (EPC) με εξωτερικά δίκτυα IP, δηλαδή την δρομολόγηση πακέτων από και προς τα εξωτερικά δίκτυα IP και την «Πύλη εξυπηρέτησης» (Serving Gateway/ S-GW) που αποτελεί τον User Plane κόμβο σύνδεσης του EPC με το LTE RAN. Η «Πύλη δικτύου πακέτων δεδομένων» (Packet Data Network Gateway/ PGW) και η «Πύλη εξυπηρέτησης» (Serving Gateway/ S-GW) αποτελούν μεν μέρος του User Plane αλλά παράλληλα δε μπορούν να αποτελούν και μέρος της λειτουργίας Control Plane. Με αυτόν τον τρόπο ενεργοποιούνται και παρέχονται τα δεδομένα IRI, CC ή και τα δυο ταυτόχρονα.

5.4 Δημιουργία διαφορετικών διεπαφών.



Εικόνα 7: Γενική απεικόνιση της νόμιμης καταγραφής δεδομένων.

Πηγή: https://www.youtube.com/watch?v=u_WEnLRZZls

Στην παραπάνω εικόνα με αριθμό 6 παρατηρούμε ότι το σύννεφο είναι οι Πάροχοι Τηλεπικοινωνιών (Communication Service Provider/ CSP), τους οποίους μπορούμε να δούμε αναφέρονται και ως Mobile Provider (MP) ή Telecom Service Provider (TSP). Εντός αυτού βρίσκονται οι λειτουργίες του δικτύου, ενώ η νόμιμη καταγραφή δεδομένων που σχετίζεται με αυτές τις λειτουργίες είναι η «Λειτουργία Διαμεσολάβησης και Παράδοσης» (Mediation/ Delivery Function/ MDF) και η «Λειτουργία Administration Function» (ADMF).

Η λειτουργία Administration Function περιλαμβάνει επίσης τη «Λειτουργία Ελέγχου Καταγραφής» (Lawful Interception Control Function/LICF) και τη «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF).

Η «Λειτουργία Διαμεσολάβησης και Παράδοσης» (Mediation/ Delivery Function/ MDF) που στην εν λόγω εικόνα εμφανίζεται ως μια λειτουργία, ουσιαστικά χωρίζεται σε δυο (2), όπως αναφέρθηκε παραπάνω αναλόγως εάν αφορά σε

«Πληροφορία σχετικά με τα «Καταγραφέντα Δεδομένα» (Intercepted Related Information/IRI) ή «Περιεχόμενο Συνομιλιών» (Call Content/CC).

Στην εικόνα 6, η διεπαφή (interface), από πλευράς των Αρχών Επιβολής του Νόμου παρουσιάζεται ως «HI Interface» και δίνονται διάφορα νούμερα όπως 1,2,3,4, δηλαδή HI1, HI2 κτλ. Επίσης, στον τομέα των Αρχών Επιβολής του Νόμου είναι και η «Λειτουργία Παρακολούθησης Δεδομένων» (Law Enforcement Monitoring Function/ LEMF) η οποία είναι συνδεδεμένη με τη «Λειτουργία Διαμεσολάβησης και Παράδοσης» (Mediation/ Delivery Function/ MDF).

Η διεπαφή HI1, χρησιμοποιείται για την αποστολή του Βουλεύματος του Δικαστικού Συμβουλίου στο δίκτυο του Παρόχου Τηλεπικοινωνιών, η οποία προωθείται στη «Λειτουργία Ελέγχου Καταγραφής» (Lawful Interception Control Function/LICF) της λειτουργίας του Administration Function (ADMF) όπου επίσης υπάρχει και η «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF).

Αυτά τα «Σημεία Καταγραφής» (POIs), τα οποία μπορεί να είναι τα AMF, SMF, κτλ, παρέχουν τις απαραίτητες πληροφορίες σε μια διεπαφή, η παροχή αυτή μπορεί να είναι είτε απευθείας σε ένα «Σημείο Καταγραφής» (POI), ενώ σε ορισμένες περιπτώσεις η παροχή των στοιχείων της «Λειτουργίας Παροχής Καταγεγραμμένων Δεδομένων» δεν μπορεί να γίνεται απευθείας και έτσι έχουμε τη «Λειτουργία Πυροδότησης» (Triggering Function/ TF). Έτσι η παροχή γίνεται πρώτα στη «Λειτουργία Πυροδότησης» και ακολούθως προωθείται ένα «Σημείο Καταγραφής» (POI).

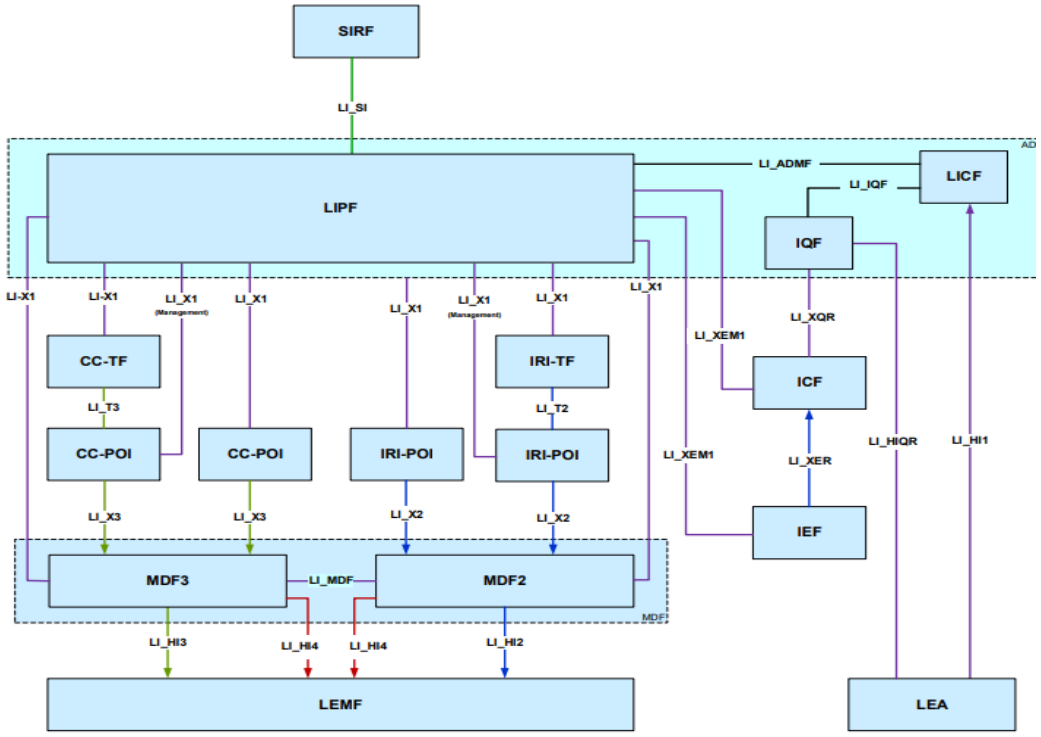
Σε αυτό το σημείο να σημειώσουμε ότι η «Λειτουργία Πυροδότησης» (Triggering Function/ TF) παρέχεται από τη LIPF, καθώς και ότι είναι αυτή που αναγνωρίζει την επικοινωνία του στόχου που επιθυμούμε την καταγραφή των δεδομένων του και στέλνει μια πυροδότηση στο σχετιζόμενο POI. Επίσης, στέλνει και όλους τους απαραίτητους κανόνες καταγραφής προκειμένου να αναγνωρίσουν τα POI τις επικοινωνίες που πρέπει να καταγραφούν, την ταυτότητα του στόχου και τις σχετιζόμενες πληροφορίες.

Ακολούθως, η εξαγωγή όλων αυτών των δεδομένων προωθείται στη «Λειτουργία Διαμεσολάβησης και Παράδοσης» (Mediation/ Delivery Function/ MDF) είτε στην MDF3 αν αφορά σε δεδομένα περιεχομένου φωνής (Call Content) και στην MDF2 αν αφορά σε δεδομένα IRI, τα οποία καταλήγουν στη «Λειτουργία Παρακολούθησης

Δεδομένων» (Law Enforcement Monitoring Function/ LEMF) των Αρχών Επιβολής του Νόμου.

5.5 Βασικές διασυνδέσεις της νόμιμης καταγραφής δεδομένων.

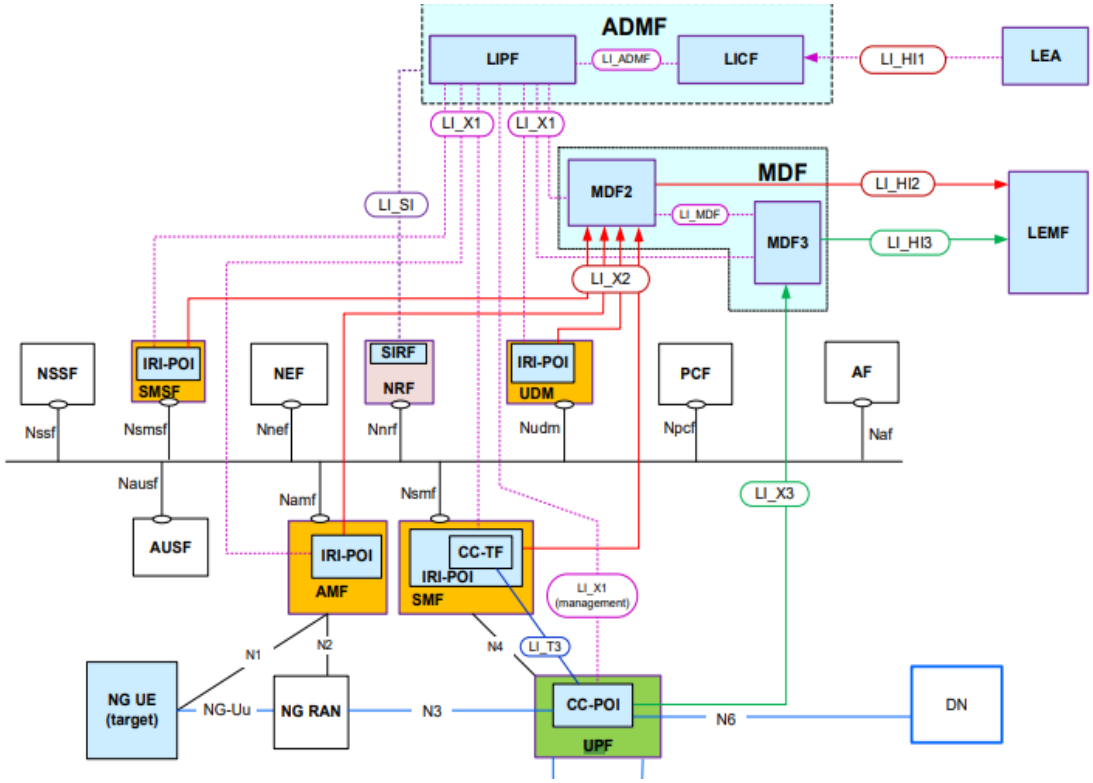
Σύμφωνα με τον προσδιορισμό που έχει δοθεί από το 3GPP τα παραπάνω περιγραφόμενα αποτυπώνονται στην εικόνα 8 με διάγραμμα αρχιτεκτονικής που δείχνει τις βασικές διασυνδέσεις της νόμιμης καταγραφής δεδομένων σημείο προς σημείο:



Εικόνα 8: Απεικόνιση διαγράμματος αρχιτεκτονικής των βασικών διασυνδέσεων της νόμιμης καταγραφής δεδομένων.

πηγή: https://www.etsi.org ETSI TS 133 127 V16.6.0 (2021-01)

Επίσης, στο ανωτέρω σχήμα της Εικόνας 8 αποτυπώνεται διεπαφή ανάμεσα στη «Λειτουργία Ελέγχου Καταγραφής» (Lawful Interception Control Function/LICF) και τη «Λειτουργία Ερωτήματος Αναγνωριστικού» (Identifier Query Function/ IQF) η οποία χρησιμοποιείται από τη «Λειτουργία Ερωτήματος Αναγνωριστικού», προκειμένου να αποστείλει πληροφορίες διαχείρισης που σχετίζονται με τη «Λειτουργία Συμβάντος Αναγνωριστικού» (Identifier Event Function/ IEF) και τη «Λειτουργία Προσωρινής Αποθήκευσης Αναγνωριστικού» (Identifier Caching Function / ICF) στη «Λειτουργία Ερωτήματος Αναγνωριστικού» (“ETSI - Welcome to the World of Standards!,” n.d.).



Εικόνα 9: Τοπολογία δικτύου που απεικονίζει την νόμιμη καταγραφή δεδομένων για τα δίκτυα 5G (από πλευράς παροχής υπηρεσιών) σημείο προς σημείο του συστήματος καταγραφών.

πηγή: https://www.etsi.org ETSI TS 133 127 V16.6.0 (2021-01)

Η ανωτέρω εικόνα 9 παρουσιάζει μια γενική τοπολογία δικτύου του συστήματος 5G σε μια αναπαράσταση από πλευράς υπηρεσιών, ωστόσο, όλες οι διεπαφές που σχετίζονται με νόμιμη καταγραφή δεδομένων των χρηστών των δικτύων 5G παρουσιάζονται σημείο προς σημείο.

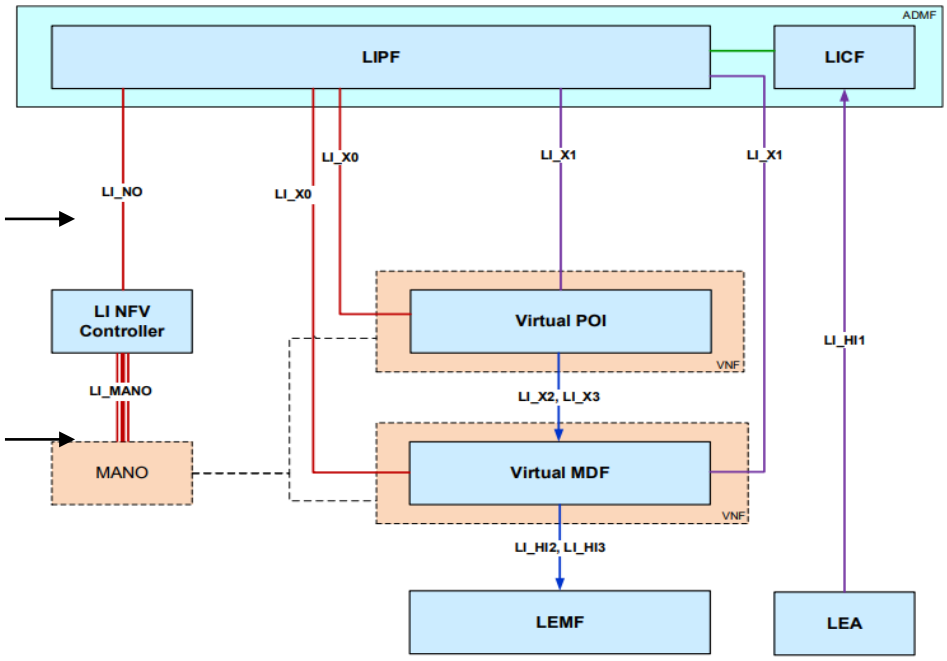
Τα «Καταγραφέντα Δεδομένα» (Intercepted Related Information/IRI) και τα «Σημεία Καταγραφών» (POIs) που υπάρχουν στο AMF, το UDM, το SMF και το SMSF παραδίδουν τα όλα τα δεδομένα xIRI στο MDF2 και τα δεδομένα xCC, δηλαδή όλα τα φωνητικά δεδομένα CC-POI που υπάρχουν στο UPF στο MDF3.

Η διεύθυνση MDF3 στο CC-POI που υπάρχει στο UPF παρέχεται από το CC-TF που υπάρχει στο SMF μέσω του LI_T3. Τα δεδομένα LIPF που υπάρχουν στο ADMF, παρέχουν τα IRI-POI που υπάρχουν στο NF με τα σχετιζόμενα καταγεγραμμένα δεδομένα, ενώ, οι διεπαφές LI_X1 μεταξύ του LIPF και του UPF χρησιμοποιούνται για την παρακολούθηση των δεδομένων χρήστη (User Plane Data).

5.5.1 Ανάπτυξη εικονικής καταγραφής δεδομένων στα δίκτυα 5G.

Γνωρίζουμε ότι τα δίκτυα 5G, αναπτύσσονται και ως «υπηρεσία», έτσι ως επακόλουθο είναι ολόκληρη η αρχιτεκτονική του δικτύου να είναι εικονική. Ακολούθως, οι λειτουργίες της νόμιμης καταγραφής, είναι επίσης εικονικές όπως η «Λειτουργία Διαμεσολάβησης και Παράδοσης» (Mediation/ Delivery Function/ MDF) η οποία για να υποστηριχθεί άμεσα χρειάζεται τη «Λειτουργία Διαχείρισης και Ενορχήστρωσης» (Management and Orchestration functions/ MANO).

Σύμφωνα με το σχήμα της εικόνας 19, υφίστανται δυο σημαντικές διεπαφές, αυτή η οποία αποτυπώνεται ως LI_NO και η LI_MANO. Η LI_NO επιτρέπει την ανταλλαγή πληροφοριών που αφορούν συσχετίσεις και ειδοποιήσεις ανάμεσα στην εφαρμογή/υπηρεσία της νόμιμης καταγραφής και στη λειτουργία του εικονικού δικτύου (Virtual Network Function/ VNF) και στη διαχείριση του κύκλου ζωής του στοιχείου της λειτουργίας εικονικού δικτύου (Virtual Network Function Component/ VNFC). Η LI_MANO επιτρέπει την ειδοποίηση ελεγκτή στη λειτουργία του εικονικού δικτύου και επιβάλει την πολιτική ασφαλείας της εικονικής ανάπτυξης της νόμιμης καταγραφής δεδομένων. Αυτές οι δύο διεπαφές θεωρείται ότι έχουν ήδη εγκατασταθεί μεταξύ των εμπλεκόμενων οντοτήτων μέσω μιας πιστοποιημένης και κρυπτογραφημένης σύνδεσης.



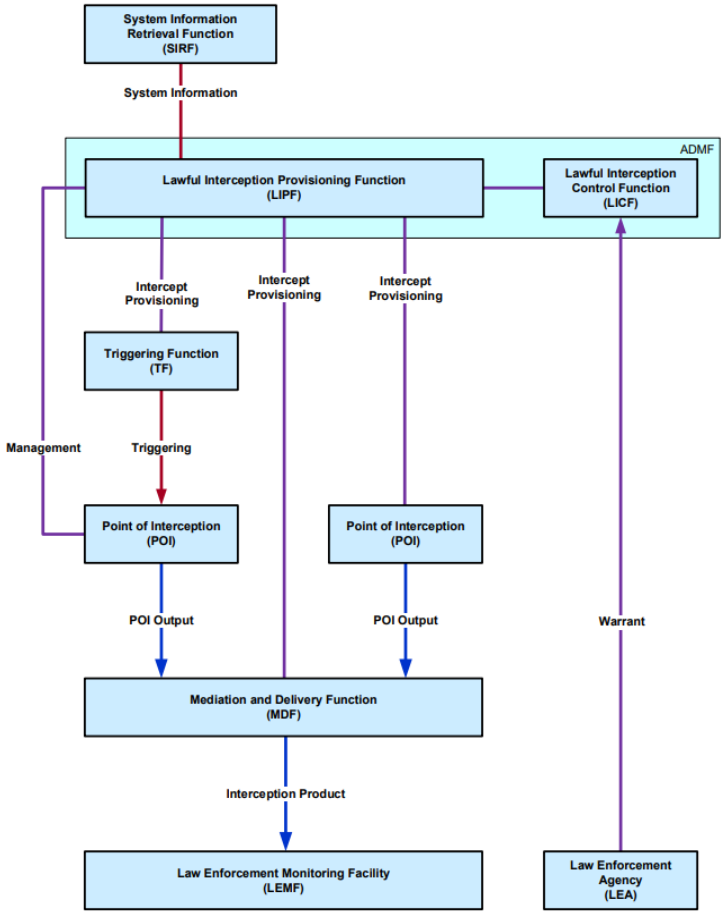
Εικόνα 10: Απλοποιημένη έκδοση της αρχιτεκτονικής της εικονικής λειτουργίας των νόμιμων καταγραφών δεδομένων.
πηγή: https://www.etsi.org ETSI TS 133 127 V16.6.0 (2021-01)

5.6 Συνολική απεικόνιση της διαδικασίας για την νόμιμη καταγραφή δεδομένων των χρηστών των δικτύων 5G.

Η συνολική απεικόνιση της διαδικασίας για την νόμιμη καταγραφή δεδομένων των χρηστών των δικτύων 5G παρουσιάζεται στην εικόνα 11. Σύμφωνα με την εν λόγω εικόνα, παρατηρούμε ότι οι Αρχές Επιβολής του Νόμου, μέσω του Βουλεύματος Δικαστικού Συμβουλίου περί άρσης του απορρήτου των επικοινωνιών, συνδέονται με τη λειτουργία ADMF η οποία περιλαμβάνει τη «Λειτουργία Ελέγχου Καταγραφής Δεδομένων» (Lawful Interception Control Function/ LICF) και -όπως ήδη έχει αναφερθεί παραπάνω- δίνει τις εντολές για την παροχή δεδομένων που απαιτούνται στη «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF).

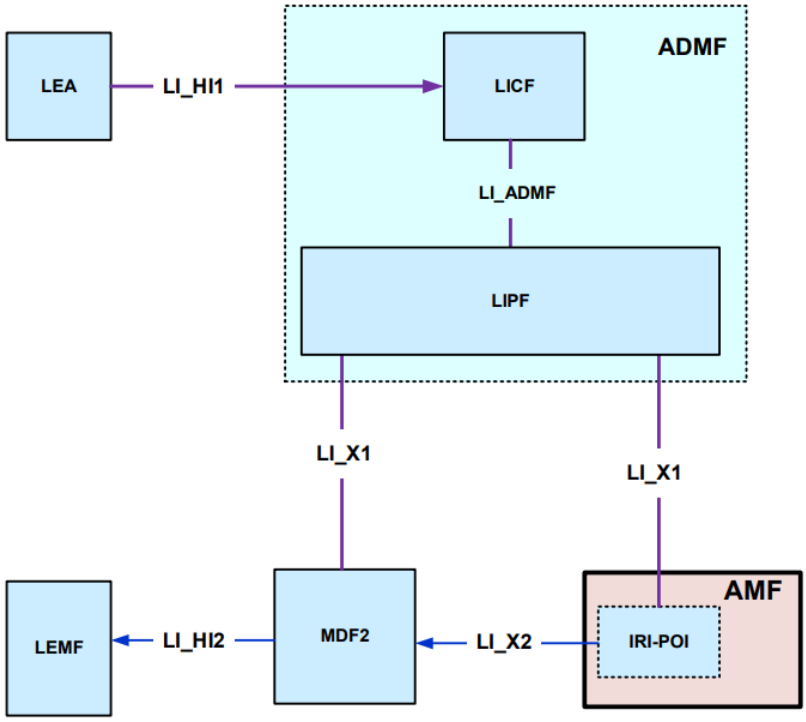
Σημειώνεται ότι «Λειτουργία Ελέγχου Καταγραφής Δεδομένων» (Lawful Interception Control Function/ LICF) μπορούμε να έχουμε μόνο μία, ενώ, «Λειτουργίες Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF) μπορούμε να έχουμε πολλαπλές.

Ακολούθως, αυτά τα στοιχεία που παρέχονται συνδέονται σε διαφορετικά «Σημεία Καταγραφής», είτε απευθείας, είτε μέσω της διαδικασίας πυροδότησης και παραδίδονται στη «Λειτουργία Παρακολούθησης Δεδομένων» (Law Enforcement Monitoring Function/ LEMF) των Αρχών Επιβολής του Νόμου.



Εικόνα 11: Συνολική εννοιολογική απεικόνιση της αρχιτεκτονικής της νόμιμης καταγραφής δεδομένων χρηστών- στόχων των δικτύων 5G.
πηγή: https://www.etsi.org ETSI TS 133 127 V16.6.0 (2021-01)

Εν συντομία, το LICF που εμφανίζεται στην εικόνα 12 εντός του ADMF, λαμβάνουν το Βούλευμα του Δικαστικού Συμβουλίου και προωθεί τα δεδομένα στο LIPF. Το LIPF παρέχει το IRI-POI, μέσω του L I_X1, στο AMF και στο MDF2. Το IRI-POI αναγνωρίζει τον στόχο και τίθενται σε λειτουργία όλες οι λειτουργίες που απαιτούνται προκειμένου να ληφθούν τα ζητούμενα επισυνδεδεμένα δεδομένα. Τα εν λόγω δεδομένα μέσω του LI_X2 παραδίδονται στο MDF2 και ακολούθως αυτό, μέσω του LI_HI2 παραδίδει τα μηνύματα IRI στο LEMF των Αρχών Επιβολής του νόμου.



Εικόνα 12: Αρχιτεκτονική της διαδικασίας καταγραφής δεδομένων στη «Λειτουργία Πρόσβασης και Κινητικότητας» (Access and Mobility Function/ AMF).

πηγή: https://www.etsi.org ETSI TS 133 127 V16.6.0 (2021-01)

Ειδικότερα, αυτό που κάνει η «Λειτουργία Ελέγχου Καταγραφής Δεδομένων» (Lawful Interception Control Function/ LICF) είναι να διαχειρίζεται τη χρονική διάρκεια ισχύος του Δικαστικού Βουλεύματος. Επίσης, το Control Function κρατάει όλες τις ευαίσθητες πληροφορίες, ενώ παράλληλα παίρνει όλες τις αποφάσεις του συνολικού συστήματος της διαδικασίας καταγραφής δεδομένων. Επιπρόσθετα, αναλαμβάνει τις

επικοινωνίες με τα βοηθητικά συστήματα των Αρχών Επιβολής του Νόμου. Τέλος, το Control Function παρέχει τις πληροφορίες περί των στόχων που αναφέρονται από το εκάστοτε Βούλευμα προς τα Σημεία Καταγραφής (POI), τη Λειτουργία Πυροδότησης (TF) και τη Λειτουργία Μεσολάβησης και Παράδοσης 2 και 3 (MDF2- 3).

Από τη άλλη πλευρά, η «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF) διαδραματίζει το ρόλο του ασφαλούς διακομιστή δεδομένων κατά την επικοινωνία του Control Function με τα POIs, TFs και MDFs. Επισημαίνεται ότι το Provisioning Function δεν αποθηκεύει καμία πληροφορία σχετικά με τους στόχους που επισυνδέονται και απλά μεταφέρουν τα μηνύματα από και προς το Control Function. Σε περίπτωση που έχουμε κάποια πυροδότηση το Provisioning Function είναι υπεύθυνο για την λήψη αυτής της πληροφορίας που πυροδοτήθηκε και να προωθεί την πυροδότηση στο κατάλληλο Σημείο Καταγραφής (POI).

5.7 Παροχή των καταγεγραμμένων δεδομένων στις Αρχές Επιβολής του Νόμου.

Τα συστατικά μέρη που χρησιμοποιούνται για την τροφοδοσία των καταγεγραμμένων δεδομένων είναι η «Λειτουργία Διαχείρισης» (Administration Function/ ADMF), η οποία αποτελεί αναπόσπαστο μέρος του δικτύου των Παρόχων Τηλεπικοινωνιών, τα «Σημεία Καταγεγραμμένων Δεδομένων (Points Of Intercept/POI), τα οποία αποτελούν τη λειτουργία δικτύου (NF) των Αρχών του Νόμου και τη «Λειτουργία Αποθετηρίου Δικτύου (Network Repository Function/ NRF). Το εκδοθέν Βούλευμα του Δικαστικού συμβουλίου αποστέλλεται στον Τηλεπικοινωνιακό Πάροχο και αντιστοίχως όλα τα στοιχεία των στόχων που αναφέρονται προς επισύνδεση τοποθετούνται στη «Λειτουργία Ελέγχου Καταγραφής Δεδομένων» (Lawful Interception Control Function/ LICF).

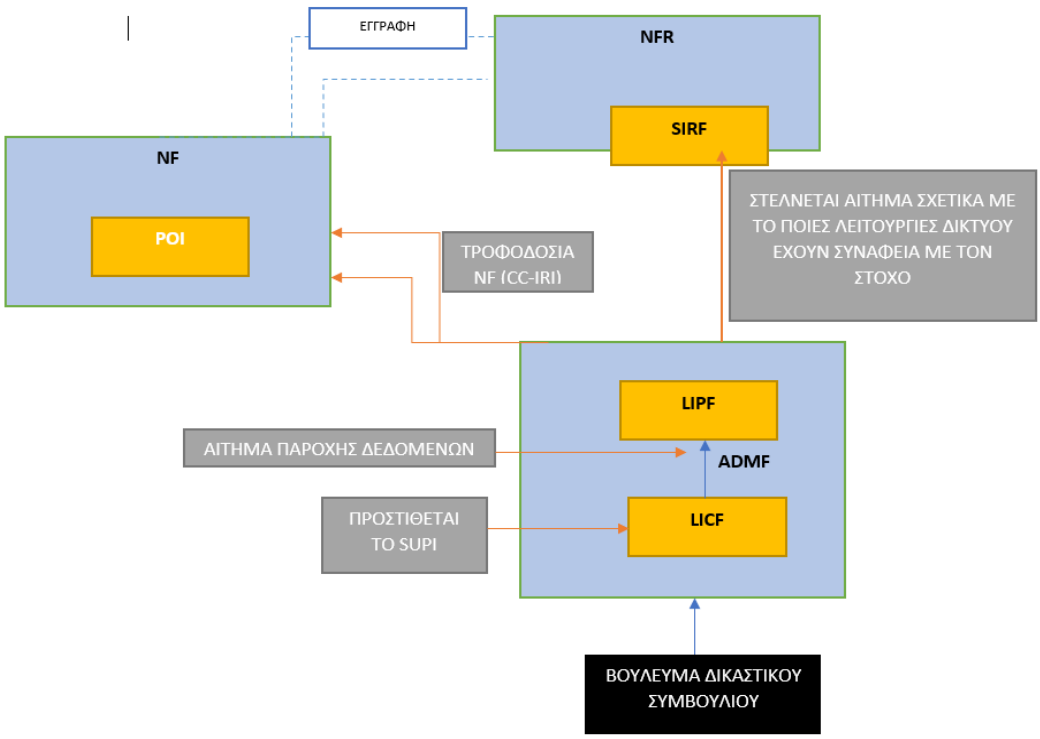
Με αυτόν τον τρόπο, η Λειτουργία Ελέγχου Καταγραφής Δεδομένων θα γνωρίζει ακριβώς την «Ειδική Ταυτότητα Δικτύου» (Network Specific Id) των στόχων, όπως για παράδειγμα τον τηλεφωνικό αριθμό κλήσης ή τη διεύθυνση του ηλεκτρονικού ταχυδρομείου που είναι προς επισύνδεση.

Οι Αρχές Επιβολής του Νόμου, μέσω των Βουλευμάτων μπορεί να παρέχουν πολύ συγκεκριμένες πληροφορίες για τους στόχους (όπως αυτές που προαναφέρθηκαν)

όμως, το δίκτυο μπορεί να χρειάζεται κάποιες παραπάνω πληροφορίες για τους στόχους προκειμένου να επιτύχει το βέλτιστο δυνατό αποτέλεσμα.

Για αυτόν το λόγο, προστίθεται το «Μόνιμο Αναγνωριστικό του Συνδρομητή» (Subscription Permanent Identifier/ SUPI) στην ταυτότητα του στόχου και με αυτό το αναγνωριστικό ο στόχος είναι έτοιμος προκειμένου να αιτηθούμε την τροφοδοσία δεδομένων. Ακολούθως, στέλνεται το ερώτημα με τα δεδομένα που χρειάζονται από τη «Λειτουργία Ελέγχου Καταγραφής Δεδομένων» (LICF) στη «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (LIPF). Με αυτή τη διαδικασία επιτυγχάνεται η καταγραφή του περιεχομένου των φωνητικών κλήσεων ή άλλων δεδομένων (CC ή IRI).

Το σύνολο των περιγραφόμενων δεδομένων αποθηκεύονται στο αποθετήριο, δηλαδή στη «Λειτουργία Αποθετηρίου Δικτύου (Network Repository Function/ NRF), εντός του οποίου υφίσταται η «Λειτουργία Αποθετηρίου Πληροφοριών Συστήματος» (System Information Repository Function/ SIRF). Η SIRF θα γνωρίζει ότι υπάρχει ένας συγκεκριμένος στόχος, για τον οποίο έχει ζητηθεί η παρακολούθησή του, και έτσι θα αποθηκεύει όλα τα απαραίτητα συστατικά στοιχεία του δικτύου τα οποία χρειάζονται.



Εικόνα 13: Διαδικασία παροχής των καταγεγραμμένων δεδομένων.
πηγή: https://www.youtube.com/watch?v=u_WEnLRZZls

Η «Λειτουργία Αποθετηρίου Πληροφοριών Συστήματος» (System Information Repository Function/ SIRF), παρέχει τις σχετιζόμενες πληροφορίες του συστήματος σχετικά με τη Λειτουργία Δικτύου στη «Λειτουργία Παροχής Καταγεγραμμένων Δεδομένων» (Lawful Interception Provisioning Function/LIPF), η οποία με τη σειρά της μεταφέρει αυτήν την πληροφορία στη «Λειτουργία Ελέγχου Καταγραφής Δεδομένων» (LICF).

Σημειώνεται ότι όποτε μια λειτουργία δικτύου (NF) επιθυμεί να επικοινωνήσει με μια άλλη λειτουργία δικτύου (NF), αυτό γίνεται μέσω της «Λειτουργίας Αποθετηρίου Δικτύου» (NRF). Η NRF είναι αυτή η οποία περιέχει όλες τις απαραίτητες πληροφορίες του δικτύου, όπως για παράδειγμα την διεύθυνση IP που χρειάζεται η μια λειτουργία δικτύου για να επικοινωνήσει με την άλλη. Αφ ης στιγμής έχουμε τη δημιουργία μιας AMF στο δίκτυο, άμεσα και ταυτόχρονα έχουμε την εγγραφή της στην NRF. Έτσι με αυτόν τον τρόπο η NRF γνωρίζει εάν έχουμε τη δημιουργία μιας νέας Λειτουργίας Δικτύου (NF).

Σύμφωνα με τα ανωτέρω περιγραφόμενα, γίνεται αντιληπτό ότι η «Λειτουργία Αποθετηρίου Πληροφοριών Συστήματος» (System Information Repository Function/ SIRF), ουσιαστικά είναι η «Λειτουργία Αποθετηρίου Δικτύου» (NRF) η οποία όμως εξειδικεύεται στην καταγραφή δεδομένων των Αρχών Επιβολής του Νόμου.

Αυτό σημαίνει ότι όποτε η Λειτουργία Τροφοδοσίας (LIPF) θέλει να τροφοδοτήσει ένα POI ή ένα TF ή ένα MDF, θα πηγαίνει πρώτα στη «Λειτουργία Αποθετηρίου Πληροφοριών Συστήματος» (System Information Repository Function/ SIRF) προκειμένου να λάβει τις απαραίτητες πληροφορίες.

Σημειώνεται ότι η «Λειτουργία Αποθετηρίου Πληροφοριών Συστήματος» (System Information Repository Function/ SIRF) δεν είναι ένα POI, αλλά μας λέει ποιο POI χρειαζόμαστε να παράσχουμε. Έτσι το LIPF συνδέεται με το SIRF.

5.8 Συνοπτική περιγραφή της νόμιμης καταγραφής δεδομένων χρηστών των δικτύων 5G.

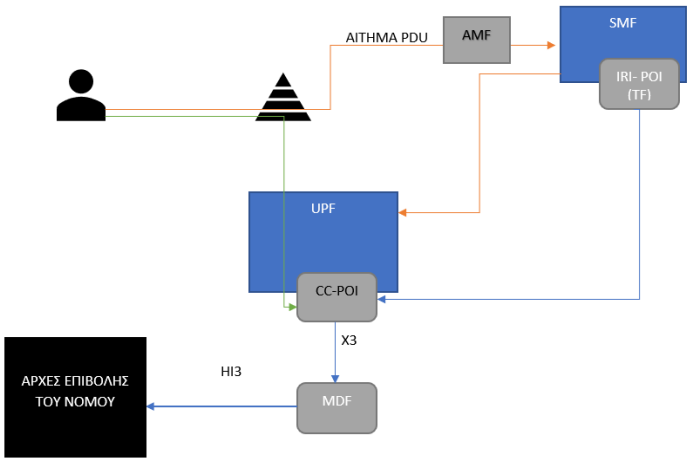
Σε αυτό το σημείο θα περιγράψουμε -πιο εξειδικευμένα- πως πραγματοποιείται η νόμιμη καταγραφή δεδομένων στο πλαίσιο άρσης του απορρήτου των τηλεπικοινωνιών ενός στόχου.

Ας υποθέσουμε ότι ένας στόχος, ο οποίος είναι ήδη συνδεδεμένος στο δίκτυο, επιχειρεί να πραγματοποιήσει μια κλήση δεδομένων (αναφέρουμε ότι ο στόχος επιχειρεί να πραγματοποιήσει μια κλήση δεδομένων διότι στα δίκτυα 5G οι κλήσεις είναι πάντα δεδομένων), αυτό σημαίνει ότι μετά την αρχική διαδικασία ελέγχου ταυτότητας (initial authentication process), ένα αίτημα της Μονάδας Δεδομένων Πρωτοκόλλου (Protocol Data Unit/ PDU Session Establishment Request) μεταφέρεται στο SMF, μέσω του AMF. Σημειώνεται ότι το PDU είναι ένα συγκεκριμένο μπλοκ πληροφοριών που μεταφέρεται μέσω του δικτύου 5G για την παροχή σύνδεσης από άκρη σε άκρη (end-to-end) μεταξύ του User Equipment (UE) και ενός συγκεκριμένου δικτύου δεδομένων, μέσω της «Λειτουργίας Επιπέδου Χρήστη» (User Plane Function/ UPF).

Ακολούθως, με αυτόν τον τρόπο, η «Λειτουργία Διαχείρισης Συνεδριών» (Session Management Function/ SMF) θα έχει τα δεδομένα που υπάρχουν για τον στόχο ως προς το IRI- POI. Δηλαδή, παρακολουθεί συνεχώς τα δεδομένα και όποτε διαβιβάζεται ένα αίτημα PDU το οποίο ταιριάζει με τα στοιχεία ταυτότητας του στόχου-χρήστη, άμεσα η SMF θα αιτηθεί από το UPF να δημιουργήσει τη φόρμα συνεδρίας και αυτό διότι δεν περιμένουμε να σταματήσει η κλήση δεδομένων και μετά να αρχίσουμε να τη συλλογή των δεδομένων.

Αφ ης στιγμής η συνεδρία εγκατασταθεί στο UPF, παράλληλα, το IRI- POI από την SMF θα δώσει εντολή στο CC- POI και αυτό θα ξεκινήσει στην καταγραφή των δεδομένων και το περιεχόμενό τους.

Επίσης, έχουμε και τη λειτουργία πυροδότησης, που πυροδοτεί το CC- POI. Αυτή η πυροδότηση πραγματοποιείται από το SMF και όχι στο UPF. Ακολούθως, το περιεχόμενο της επικοινωνίας μεταφέρεται στη Λειτουργία Μεσολάβησης (MDF) μέσω διεπαφών (όπως αναφέρθηκαν και παραπάνω) και έτσι καταλήγουν τα καταγεγραμμένα δεδομένα στην Αρχή που τα αιτήθηκε.



Εικόνα 14: Αρχιτεκτονική διαδικασίας καταγραφής δεδομένων χρηστών- στόχων.

5.9 Ιδιωτικές εταιρείες ανάπτυξης λογισμικού νόμιμης καταγραφής επικοινωνιών.

Για το σκοπό της παρούσης έρευνας πραγματοποιήθηκε μελέτη (πέραν των επιστημονικών άρθρων) και πηγών σε διαδικτυακούς τόπους ιδιωτικών εταιρειών οι οποίες δραστηριοποιούνται επιχειρηματικά και επιστημονικά στην υλοποίηση εφαρμογών σχετικά με τη χρήση των δικτύων 5G προς όφελος Αρχών Επιβολής του Νόμου και κρατικών οργανισμών. Συγκεκριμένα, το κομμάτι που απασχόλησε στην δική μας έρευνα ήταν σχετικά με τις παροχές τους στη διαδικασίας υλοποίησης νόμιμων επισυνδέσεων τηλεφωνικών επικοινωνιών σε συνεργασία με εταιρείες παροχής τηλεπικοινωνιών στην Ελλάδα και ανά τον κόσμο.

Ειδικότερα, οι εν λόγω εταιρείες έχουν προβεί στην ανάπτυξη λογισμικών και εφαρμογών τα οποία δύναται να πραγματοποιούν είτε παράλληλη επισύνδεση (parallel interception)- συνακρόαση συνομιλιών μεταξύ χρηστών του δικτύου, είτε να αποθηκεύουν και να λαμβάνουν το σύνολο των δεδομένων που διακινούνται μέσω εφαρμογών κινητών τηλεφώνων, για τον σκοπό της εξιχνίασης εγκλημάτων.

Διαδικασία νόμιμης καταγραφής μέσω των κυψελοειδών δικτύων 5G.

Προκειμένου να πραγματοποιηθεί αυτή η διαδικασία, η αρχιτεκτονική δικτύου εισάγει μια σειρά τεχνολογιών συμπεριλαμβανομένων των CUPS (Control and User

Plane Separation), NFV (Network Functional Virtualization), network slicing, and CIoT (Cellular Internet of Things) όπως έχει προαναφερθεί και σε άλλο σημείο της εργασίας .

Πιο συγκεκριμένα, καθεμία από τις ανωτέρω τεχνολογίες περιλαμβάνει τα εξής:

- **Διαχωρισμός της λειτουργίας ελέγχου και επιπέδου χρήστη- Control and User Plane Separation—(CUPS**).

Η ιδέα πίσω από τον Διαχωρισμό της Λειτουργίας Ελέγχου και Επιπέδου Χρήστη (CUPS) είναι να διαχωρίσει το την Λειτουργία Ελέγχου (control) και την Λειτουργία Επιπέδου Χρήστη (user plane) για την Πύλη Σηματοδότησης- SGW (Signaling Gateway) η οποία (πύλη) αποτελεί ένα στοιχείο δικτύου που χρησιμοποιείται για την αποστολή μηνυμάτων (σημάτων) μεταξύ κόμβων οι οποίοι επικοινωνούν με τη βοήθεια διαφορετικών πρωτοκόλλων, την Πύλη Δικτύου Δεδομένων Πακέτων- PGW (Packet Data Network Gateway), η οποία παρέχει συνδεσιμότητα από τον εξοπλισμό του χρήστη προς εξωτερικά δίκτυα δεδομένων πακέτων αποτελώντας ουσιαστικά το σημείο εισόδου κα εξόδου και την Λειτουργία Ανίχνευσης Κυκλοφορίας- Traffic Detection Function (TDF), δηλαδή μια λειτουργία δικτύου που επιβάλλει συγκεκριμένες διαδικασίες κυκλοφορίας σε πραγματικό χρόνο, με βάση είτε προκαθορισμένους κανόνες, είτε κανόνες που καθορίζονται δυναμικά.

Τα δίκτυα LTE και LTE-Advanced ήδη παρέχουν διαχωρισμό, εφαρμόζοντας τις περισσότερες από τις λειτουργίες ελέγχου (control functions) στην Οντότητα Διαχείρισης Κινητικότητας- Mobility Management Entity (MME) και η Λειτουργία Παράδοσης της κίνησης του χρήστη (user traffic delivery function) στο S/P-GW. Το CUPS πηγαίνει αυτόν ακριβώς τον διαχωρισμό ακόμη παραπέρα και επιτρέπει την ανεξάρτητη κλιμάκωση δικτύου, αναπτύσσοντας περισσότερους κόμβους χρήστη, έτσι ώστε να είναι πιο κοντά στα όρια του δικτύου χωρίς αύξηση του αριθμού των κόμβων ελέγχου για εφαρμογές, συμπεριλαμβανομένων των tethering (δηλαδή της χρήσης του κινητού τηλεφώνου ως ενδιάμεσου για την παροχή πρόσβασης στο διαδίκτυο), των τοπικών επικοινωνιών Vehicle-to-X, της επαυξημένης πραγματικότητας ή της βελτιστοποιημένης ροής βίντεο.

- **Λειτουργική Εικονοποίηση Δικτύου- Network Functional Virtualization (NFV)**

Τα συστήματα 5G αποτελούν εικονοποιημένες λειτουργίες δικτύου (NFV). Το NFV αναφέρεται στην αντικατάσταση παραδοσιακών εξειδικευμένων συσκευών υλικού με λογισμικό που μπορεί να εγκατασταθεί σε τυποποιημένο, μη διαθέσιμο υλικό hardware. Επίσης, υποστηρίζεται ότι σε περιπτώσεις όπου η τοποθεσία ή/και οι πληροφορίες της διεύθυνσης του ICE δεν είναι γνωστές, έως ότου καταχωρηθεί η ταυτότητα στόχου (ή πραγματοποιηθεί κλήση), η IRI παρέχει συνήθως τις απαραίτητες πληροφορίες για την παροχή του NFV (π.χ. διεύθυνση IP και θύρα για τις ροές περιεχομένου).

- **Τμηματοποίηση Δικτύου- Network slicing (NS).**

Το Network Slicing, δηλαδή η τμηματοποίηση δικτύου είναι μια επιλογή που επιτρέπει στους τηλεπικοινωνιακούς παρόχους να δημιουργούν προσαρμοσμένα τμήματα δικτύου αναλόγως της κίνησης των δεδομένων, των επιδόσεων ή τον τύπο του συνδρομητή. Οι πάροχοι, έχουν τη δυνατότητα να δημιουργήσουν ένα τμήμα δικτύου για συσκευές CIoT (Cellular Internet of Things) ή τμήματα για κάλυψη αναλόγως της ζήτησης, τα οποία αναφέρονται ως NSIs (Network Slice Instance(s)) και δύναται να περιέχουν ένα ή περισσότερα υποδίκτυα, τα NSSI (Network Slice Subnet Instance). Τα εν λόγω υποδίκτυα περιέχουν περαιτέρω λειτουργίες δικτύου, οι οποίες μπορούν να είναι επίσης εικονοποιημένες. Τέλος, με την εφαρμογή της τεχνολογίας του Network Slicing υπάρχει η δυνατότητα ενεργοποίησης ιδιωτικών μεμονωμένων τμηματικών δικτύων. Ωστόσο, με αυτά τα μεμονωμένα τμήματα ιδιωτικών δικτύων ενδέχεται να μην υφίσταται η δυνατότητα ρύθμισής τους, και έτσι οι έρευνες των χρηστών που ανήκουν ή χρησιμοποιούν ιδιωτικά δίκτυα να απαιτούν τον επαναπροσδιορισμό και επανασχεδιασμό τους προς όφελος των Αρχών Επιβολής του Νόμου.

- **Κυψελοειδές Διαδίκτυο των Πραγμάτων- Cellular Internet of Things (CIoT).**

Το ADMF (Administration Function) είναι υπεύθυνο για το συνολικό επίπεδο διαχείρισης/ελέγχου του συστήματος της νόμιμης καταγραφής- παρακολούθησης. Η συγκεκριμένη λειτουργία έχει τη δυνατότητα να προβλέπει το GSN (GPRS Support Node) ανάλογα με αντιστοίχιση στο τοπικό δίκτυο συγκεκριμένων MSISDN, IMSI και αριθμών IMEI που συνδέονται αποκλειστικά με συσκευές CIoT (οι πάροχοι συνήθως διαχωρίζουν του χρήστες ανάλογα με τους αριθμούς των IMSI/ MSISDN/ IMEI, αυτό όμως δύναται να δημιουργήσει μπέρδεμα σε περιπτώσεις που ένας χρήστης μπορεί να

εισάγει μια SIM σε μια συσκευή CIoT, κάτι για το οποίο οι Αρχές θα πρέπει να έχουν γνώση τέτοιων πιθανών ενεργειών αντιπαρακολούθησης).

- **Χρήση της υπηρεσίας εντοπισμού θέσης για συσκευές του κυψελοειδούς διαδικτύου των πραγμάτων (CIoT).**

Αυτή η υιοθέτηση φέρει αποτελέσματα τόσο σε πραγματικό χρόνο (real-time), όσο και σε μη πραγματικό χρόνο (non-real-time) εντοπισμό χρηστών.

5.9.1 Το παράδειγμα της ιδιωτικής εταιρείας ανάπτυξης λογισμικού καταγραφής των επικοινωνιών με την επωνυμία «GROUP2000».

Σύμφωνα με την ιδιωτική εταιρεία ανάπτυξης λογισμικού καταγραφής επικοινωνιών με την επωνυμία «GROUP2000» με έδρα την Ολλανδία, η δική τους λύση-πρόταση στο θέμα της νόμιμης καταγραφής έρχεται να βοηθήσει και να συνδράμει τους παρόχους τηλεπικοινωνιών και διαδικτύου καθώς και τα Σ.Α. μέσω της διαδικασίας αυτοματοποιημένης παροχής καταγραφής των συνομιλιών και τη μεσολάβηση και την παράδοση των δεδομένων που συλλέγονται, σύμφωνα με τις απαιτούμενες προδιαγραφές. Η εφαρμογή με την επωνυμία «LIMA Lawful Intercept» είναι συμβατή και μπορεί να εφαρμοστεί σε οποιοδήποτε σταθερό, καλωδιακό και κινητό δίκτυο, με οποιονδήποτε προμηθευτή και με όλες τις τεχνολογίες και υπηρεσίες, συμπεριλαμβανομένων των υπηρεσιών επικοινωνίας όπως IP Multimedia Subsystem (IMS) (“Specification # 23.228,” n.d.), Voice over LTE (VoLTE), VoLTE Roaming, Rich Communication Services (RCS), Narrowband-IoT (NB- IoT), και πολλά άλλα. Χάρη στην ευέλικτη αρχιτεκτονική πλατφόρμα του LIMA Lawful Intercept υπάρχει η δυνατότητα υποστήριξης και ρύθμισης πολλών δικτύων και πολλών χωρών (“LIMA Lawful Interception - Cost Efficient - Group 2000,” n.d.; “LIMA Mediator,” n.d.).

Τα αποτελούμενα μέρη που απαρτίζουν την ανωτέρω αναφερόμενη εφαρμογή συνακρόασης και εν γένει καταγραφής των επικοινωνιών μεταξύ χρηστών είναι τα εξής:

- LIMA Management System
- LIMA Mediator
- LIMA Monitors

- LIMA Location Services
- LIMA CC-PAG
- LIMA ÉLITE

Ειδικότερα:

LIMA Management System

Το Σύστημα Διαχείρισης LIMA έχει σχεδιαστεί για να παίζει κεντρικό ρόλο σε οποιαδήποτε λύση Νόμιμης «Υποκλοπής». Ο επεκτάσιμος σχεδιασμός του Συστήματος Διαχείρισης επιτρέπει να αναπτυχθεί σε λύσεις που κυμαίνονται από μια αυτοτελή νόμιμη λύση υποκλοπής σε ένα κατανεμημένο σύστημα που καλύπτει πολλές χώρες και φορείς. Το Σύστημα Διαχείρισης LIMA έχει τη δυνατότητα διαχείρισης και να επίβλεψης των ενεργών Βουλευμάτων από μια κεντρική τοποθεσία, ανεξάρτητα από τον τύπο και τον αριθμό των δικτύων.

LIMA Mediator

Το LIMA Mediator μπορεί να ενσωματωθεί σε ένα μεγάλο εύρος Δικτύου. Για να αντιμετωπιστεί αυτή η ποικιλία καταστάσεων, το LIMA Mediator έχει σχεδιαστεί γύρω από την έννοια της χρήσης Προσαρμογέα Εισόδου που χειρίζονται x2 (IRI ή CDC) και x3 (CC ή CCC) κίνηση. Οι προσαρμογείς εισόδου είναι διαθέσιμοι για τα περισσότερα δίκτυα και βρίσκεται συνήθως σε δίκτυα τηλεπικοινωνιών και ISP. Αυτό περιλαμβάνει προσαρμογείς για PSTN/ ISDN, VoIP/ IMS/ LTE, E-Mail, IP, Mobile IP, συμπεριλαμβανομένης της υποστήριξης για την τελευταία γενιά 5G X-διεπαφές. Για υποστήριξη του VoLTE S8 HomeRouting, μπορεί να επεκταθεί με ένα στοιχείο LMISF. Από την πλευρά εξόδου, το LIMA Mediator υποστηρίζει όλα τα Πρότυπα παράδοσης που χρησιμοποιούνται και εφαρμόζονται. Τα υποστηριζόμενα πρωτόκολλα περιλαμβάνουν τα κάτωθι: ETSI TS 102 232, ETSI TS 103 120, ETSI ES 201 671, 3GPP TS 33.108, J-STD-025-B, ATIS T1.678 DSR, ATIS LEAS, Packetcable CBIS.

LIMA Monitors

Το LIMA Monitor είναι ένας ισχυρός και ενσωματωμένος ανιχνευτής IP που συνδυάζει πολλαπλές λειτουργίες υποκλοπής IP σε ένα φυσικό σύστημα. Ο αισθητήρας

είναι σε θέση να υποκλέψει και να καταγράψει όλη την κοινή κίνηση IP, Email και VoIP. Η οθόνη IP LIMA είναι ευέλικτη και πολυλειτουργική, ενώ συνδυάζει ανάλυση κυκλοφορίας, παρακολούθηση και διαμεσολάβηση σε «ένα» όταν συνδυάζεται με το LIMA Mediator. Το LIMA IP Monitor είναι ένας παθητικός αισθητήρας, ο οποίος μπορεί να εγκατασταθεί σε ένα δίκτυο. Η εφαρμογή της υποκλοπής δεδομένων και στοιχείων μπορεί να γίνει με ελάχιστο αντίκτυπο και ορατότητα αποφεύγοντας την ενσωμάτωση με υπάρχοντα στοιχεία δικτύου.

LIMA Location Services

Η εφαρμογή LIMA Location Services παρέχει απαντήσεις σε αιτήματα περί τοποθεσία σε προκαθορισμένα χρονικά διαστήματα. Η παροχή συχνών πληροφοριών της τοποθεσίας τυχόν στόχων προσθέτει σημαντική αξία στις ποινικές έρευνες. Υποστηριζόμενοι τύποι δικτύου: GSM, UMTS, LTE, 5G, CDMA, DSL, VoIP, xDSL, IMS, PSTN κ.ά.

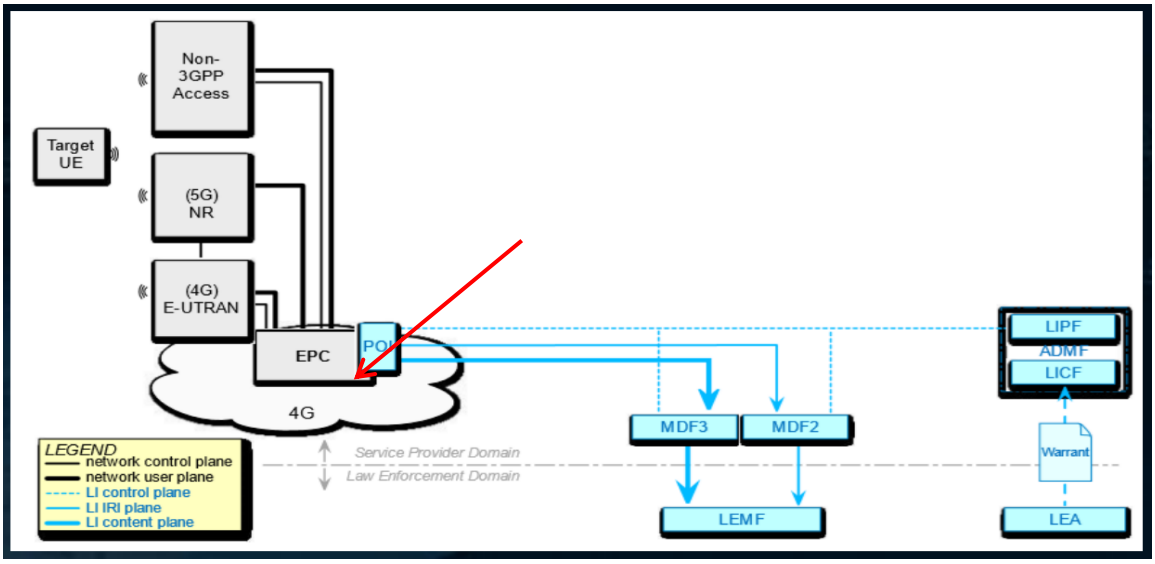
LIMA CC-PAG

Παρέχει συσσωμάτωση CC από διαφορετικά CC-POI ως προς τη λειτουργία MDF3 του LIMA Mediator, παρέχει βελτιστοποιημένη συνδεσιμότητα δικτύου, βελτιώνει την απόδοση του User Plane Function (UPF) και επιτρέπει τη μεταφόρτωση κρυπτογράφησης από UPF σε CC-PAG για κίνηση X3.

LIMA ÉLITE

Ανεξάρτητο δίκτυο και τεχνολογία, το οποίο εφαρμόζεται σε δίκτυα 2G, 3G και 4G όλων των παρόχων τηλεπικοινωνιών και δικτύων και υποστηρίζει καταγραφή φωνητικών κλήσεων, SMS και δεδομένων κινητής τηλεφωνίας. Τέλος, υποστηρίζει την καταγραφή Metadata και Περιεχόμενο Επισύνδεσης.

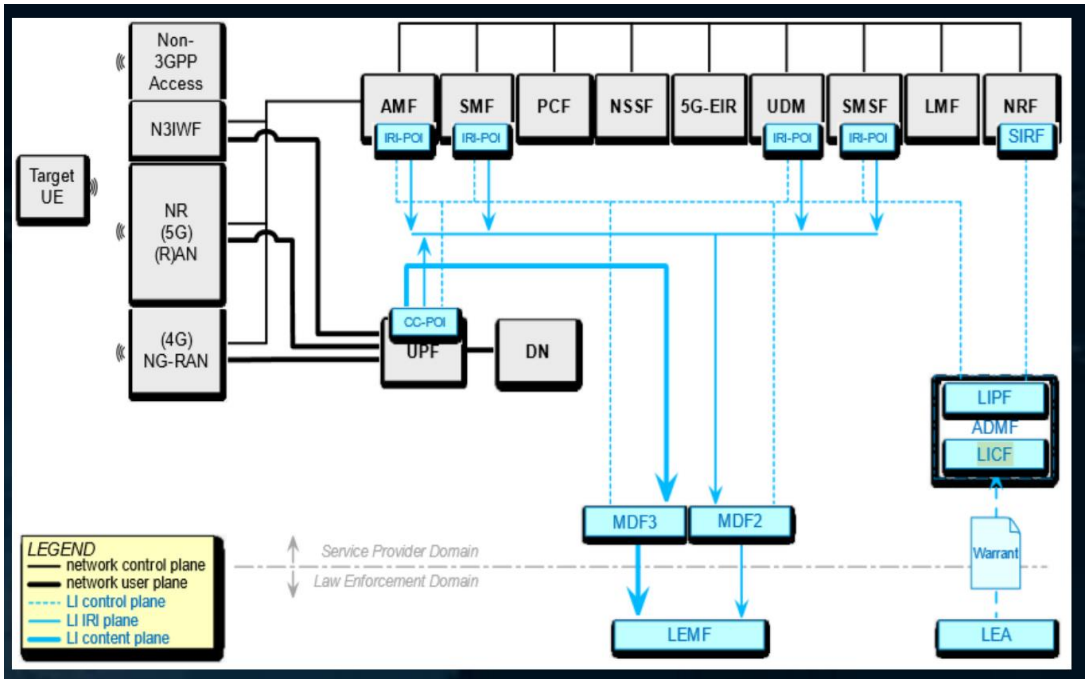
Ειδικότερα, σύμφωνα με το white paper της εν λόγω εταιρείας, αναφερόμενοι στην τεχνολογία την οποία ανέπτυξαν για την καταγραφή των επικοινωνιών μέσω των δίκτυών 5G, υποστηρίζουν ότι η λειτουργιά EPC (Evolved Packet Core), παραμένει απαράλλακτη με την αντίστοιχη στα δίκτυα 4G, παρόλο που υφίσταται μεγαλύτερο εύρος ζώνης (bandwidth).



Εικόνα 15: 4G EPC (Evolved Packet Core)

Ελήφθη από: https://group2000.com

Στην εικόνα 15 αποτυπώνεται η λειτουργία EPC (Evolved Packet Core), δηλαδή ο «εξελιγμένος πυρήνας πακέτων» στα δίκτυα 4G. Αντιστοίχως, στην εικόνα 16 αποτυπώνεται (όπως και στο 4G EPC και στο 5G EPC) η συγκέντρωση της κυκλοφορία δεδομένων από τις τελικές συσκευές. Επίσης, το 5G EPC πιστοποιεί τους συνδρομητές και τις συσκευές και διαχειρίζεται την κινητικότητα των συσκευών πριν από τη δρομολόγηση της κυκλοφορίας στο διαδίκτυο.



Εικόνα 16: 5G EPC (Evolved Packet Core)

Ελήφθη από: https://group2000.com

Με τη λειτουργία core-anchored στο δίκτυο 5G, επιτυγχάνεται η πλήρης δυναμική του δικτύου με τα κάτωθι αποτελέσματα:

• Υψηλότερο εύρος ζώνης.

• Αναγνώριση διαφορετικών ταυτοτήτων χρήστη και εξοπλισμού.

• Νέο σύνολο στοιχείων των διεπαφών στην επισύνδεση.

• Αλλαγές στην τοπολογία.

Σύμφωνα με την εταιρεία «Group2000» η νόμιμη επισύνδεση για την υποδομή του MEC (Multi-access Edge Computing), είναι μια διαδικτυακή λύση που παρέχει υπηρεσίες και υπολογιστικές λύσεις που απαιτούνται από τους χρήστες. Αυτό που πραγματοποιείται είναι να φέρνει πιο κοντά στου χρήστες τις υπηρεσίες εφαρμογών και περιεχομένου, παρέχοντας αξιόπιστη και απόλυτη εμπειρία χρήσης.

Αυτό επιτυγχάνεται με αρχιτεκτονική υψηλού επιπέδου μέσω των:

• LIMA Management System (Administration Function).

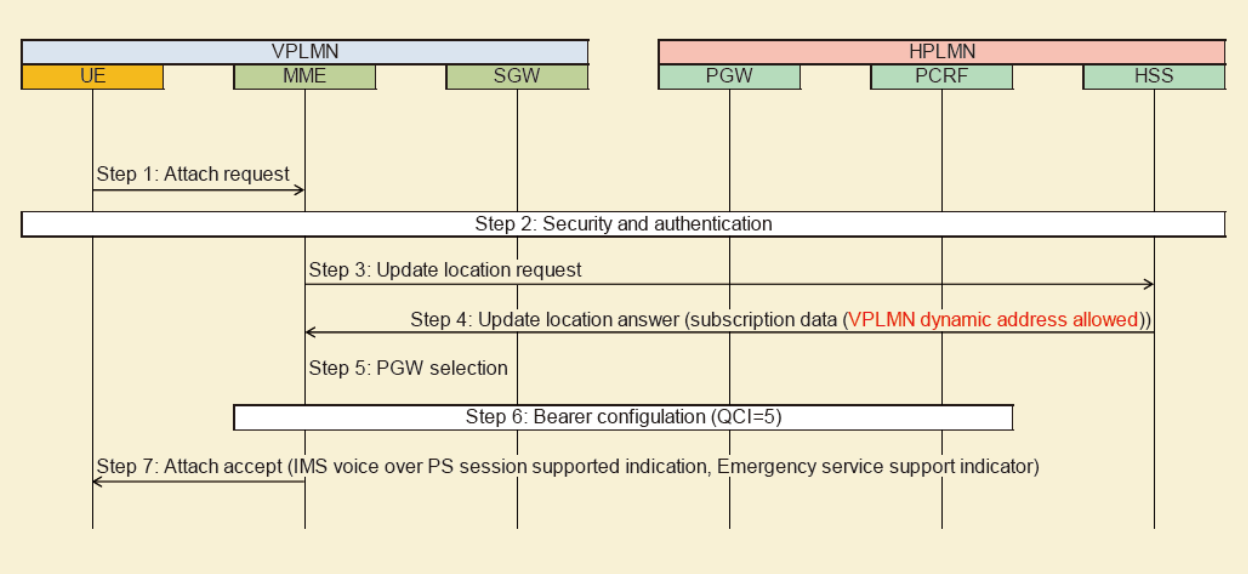
• LIMA Mediator (Mediation Function).

Και των Διασυνδέσεων:

• Handover Interfaces.

• X-interfaces

Νόμιμη καταγραφή χρηστών που επισκέπτονται το Επίγειο Δημόσιο Δίκτυο Κινητής Τηλεφωνίας VPLMN (Visiting Public Land Mobile Network) όταν το S8HR χρησιμοποιείται ως αρχιτεκτονική περιαγωγής στο VoLTE.



Εικόνα 17: Προσέγγιση της λειτουργίας του S8HR

πηγή: https://blog.3g4g.co.uk

Λειτουργία BBIFF (Bearer Binding Intercept and Forward) ((“Publications,”) ETSI TS 133 107 V14.2.0 (2017-07)).

Η συγκεκριμένη λειτουργία εισήχθη για την υποστήριξη της νόμιμης παρακολούθησης φωνητικών υπηρεσιών στο VPLMN όταν το S8HR χρησιμοποιείται ως αρχιτεκτονική περιαγωγής, παρέχοντας την επιλογή SGW για εξωτερική παρακολούθηση.

LMISF (Lawful Interception Mirror IMS State Function) Λειτουργία.

- Έλεγχος του BBIFF.
- Εξετάζει όλα τα SIP (signaling protocol) messages, δηλαδή τα πρωτόκολλα που δημιουργήθηκαν για να τροποποιούν και να τερματίζουν μια περίοδο λειτουργίας πολυμέσων μέσω του πρωτοκόλλου Διαδικτύου και συγκεκριμένα:

• Παρακολουθεί την κατάσταση του IMS (IP Multimedia Subsystem).

• Δημιουργεί IRI και για τα μέρη, τόσο του καλούμενου όσο και του καλούντος .

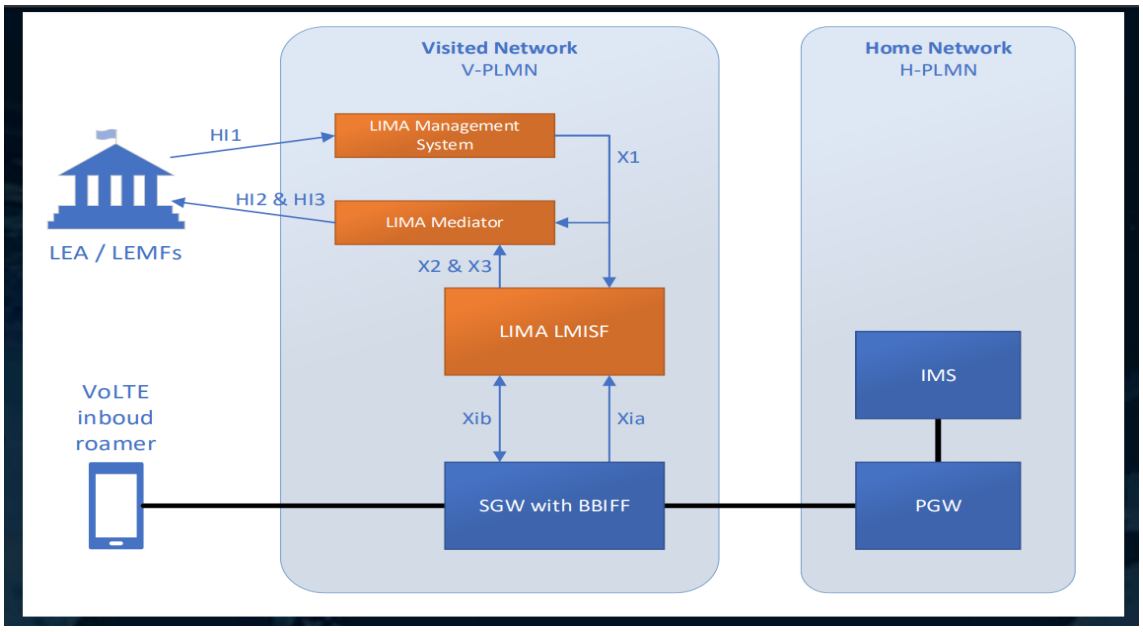
• Δημιουργεί αρχεία χρέωσης.

• Δημιουργεί βάσεις διατήρησης δεδομένων.

- Επεξεργασία μέσων:

• Συσχετίζει τα εν λόγω πακέτα με την κατάσταση του IMS.

• Δημιουργεί CC (Component Carrier).



Εικόνα 18: Υποστήριξη νέων τεχνολογιών στη νόμιμη καταγραφή δεδομένων των χρηστών των δικτύων 5G.

Ελήφθη από: www.group2000.com

Σύμφωνα με την εν λόγω τεχνολογία γεννάται το ερώτημα εάν θα δίδεται η δυνατότητα οι λύσεις off-air να χρησιμοποιούνται και στο μέλλον. Η απάντηση σε αυτό το ερώτημα είναι όχι και αυτό διότι το δίκτυο 5G έχει σχεδιαστεί έτσι ώστε να προστατεύεται από επιθέσεις καταγραφής του IMSI. Παράλληλα, έχουμε την είσοδο της τεχνολογίας SUPI (Subscription Permanent Identifier), το οποίο ουσιαστικά αποτελεί το παλιό IMSI και SUCI (Subscription Concealed Identifier), το οποίο λειτουργεί ως

Προσωρινή Ταυτότητα Συνδρομητή Κινητής Τηλεφωνίας- Temporary Mobile Subscriber Identity (TMSI) στα δίκτυα 5G και τα οποία ποτέ δεν στέλνονται over-the-air.

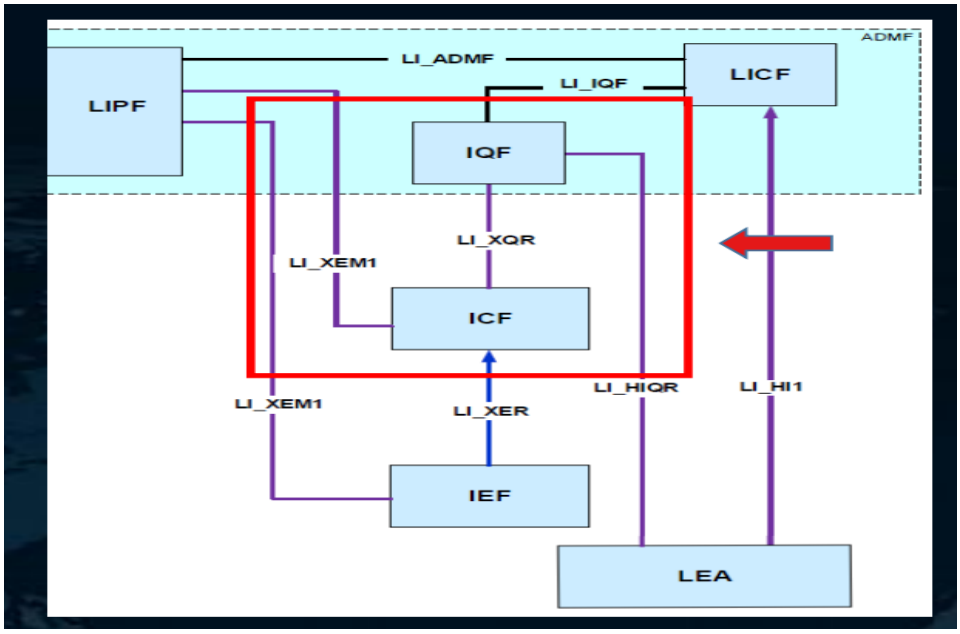
Εικόνα 19: Καταγραφή του IMSI μέσω των δικτύων 5G

Ελήφθη από: https://group2000.com

Πώς όμως «δουλεύει» αυτό στην πράξη;

Ο «5G Catcher» είναι αυτός που συλλέγει τις προσωρινές ταυτότητες (ID) και αυτό το γεγονός, θα χρειασθεί να συσχετισθεί με το SUPI. Το προσωρινό ID, θα αποσταλεί για συσχετισμό στη Λειτουργία Αναζήτησης Αναγνωριστικού- Identifier Query Function (IQF) το οποίο θα «ρωτήσει» τη Λειτουργία Προσωρινής Αποθήκευσης Αναγνωριστικών- Identifier Caching Function (ICF) και ο συσχετισμός που θα προκύψει θα αποσταλεί από το IQF στην Αρχή που διενεργεί την επισύνδεση.

Η εν λόγω τεχνολογία που αναπτύχθηκε από την εταιρεία «Group2000», υποστηρίζει τον εντοπισμό ταυτότητας των «5G ID catchers». Ειδικότερα, οι Αρχές Επιβολής του Νόμου, είναι εκεί όπου εδρεύει ο 5G ID Catcher, ενώ με τον όρο IQF αναφέρονται στο Identity Query Function, με τον ICF στον Identity Caching Function και με τον IEF στον Identifier Event Function. Η αναφερόμενη τεχνολογία αποτυπώνεται στην εικόνα 20:



Εικόνα 20: Τεχνολογία εντοπισμού ταυτότητας των χρηστών των δικτύων 5G. Ελήφθη από: https://group2000.com

Ένα άλλο θέμα που τάσσεται επί τάπητος από την εταιρεία «Group2000» είναι η λειτουργία και χρήση των ιδιωτικών δικτύων μέσω της «τμηματοποίησης» (slicing). Η λογική πίσω από την ανάπτυξη ιδιωτικών δικτύων είναι η χρήση του σε βιομηχανικούς και άλλους σημαντικούς τομείς μιας κοινωνίας όπως μεγάλα βιομηχανικής κλίμακας δίκτυα, δίκτυα διαδικτύου των πραγμάτων (Internet-of-Things) σε εργοστάσια, αποθήκες, λιμάνια και άλλα. Η ασύρματη δικτύωση σε αυτούς τους τομείς θεωρείται μια μεγάλη ανεκμετάλλευτη ευκαιρία ανάπτυξης για έξυπνα συνδεδεμένα συστήματα.

Προκειμένου να πραγματοποιηθούν τα ανωτέρω αυτή τη χρονική στιγμή υφίστανται δυο επιλογές. Η μια είναι η σύνδεση με ένα δημόσιο LTE/5G δίκτυο ή η επιλογή ενός ιδιωτικού LTE/5G δικτύου το οποίο δύναται να πραγματοποιηθεί είτε αγοράζοντας μια εταιρεία τη δική της υποδομή με σχετική σύμβαση με εταιρεία κινητής τηλεφωνίας, είτε κατασκευάζοντας και διατηρώντας το δικό της δίκτυο χρησιμοποιώντας δικό της ανεξάρτητο φάσμα.

Τα πλεονεκτήματα από μια τέτοια επιλογή για μια επιχείρηση είναι προδήλως εμφανή όπως η έξυπνη ρομποτική και πολλά άλλα τα οποία χρησιμοποιούνται όλο και περισσότερο σε καθημερινές λειτουργίες και αποφέρουν απτά οφέλη και στις δύο

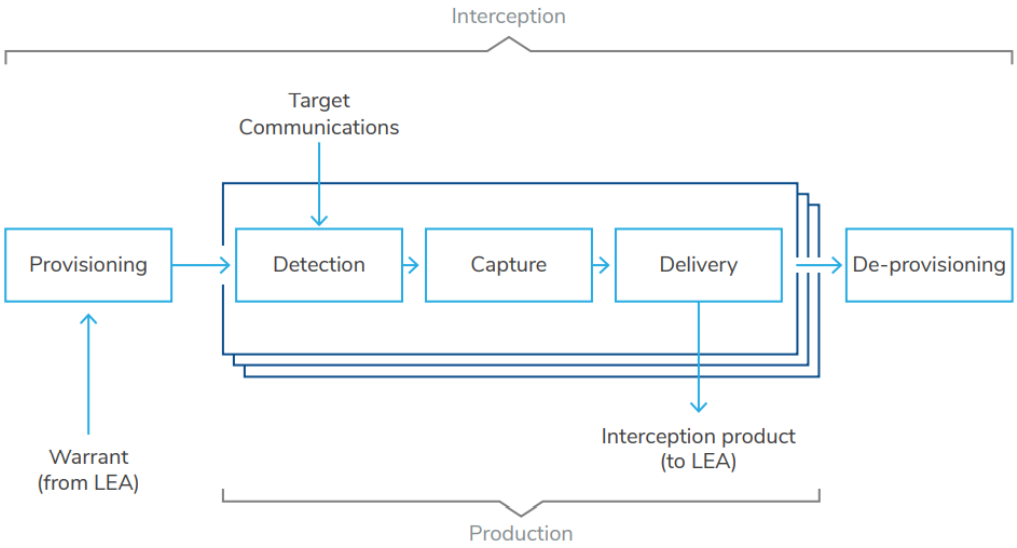
πλευρές του κόστους (αύξηση παραγωγικότητας) ή των εσόδων (νέες προτάσεις πελατών).

Παράλληλα όμως, η δημιουργία τέτοιων ιδιωτικών δικτύων αποτελεί και ένα σημαντικό θέμα για την δυνατότητα καταγραφής δεδομένων χρηστών οι οποίοι πέρα από τη χρήση των δημοσίων δικτύων θα προβαίνουν και σε χρήση ιδιωτικών δικτύων.

5.9.2 Το παράδειγμα της ιδιωτικής εταιρείας ανάπτυξης λογισμικού καταγραφής δεδομένων «Utimaco».

Σύμφωνα με την εταιρεία ανάπτυξης λογισμικού «Utimaco», η νομότυπη καταγραφή συνομιλιών αποτελεί μια καταστατική υποχρέωση των παρόχων τηλεπικοινωνιών προκειμένου να διασφαλίσουν τη δυνατότητα καταγραφής των επικοινωνιών για λογαριασμό των Αρχών Επιβολής του Νόμου. Οι εταιρείες παροχής τηλεπικοινωνιών πρέπει να είναι σε θέση να παρακολουθούν όλες τις επικοινωνίες των συνδρομητών ενός συγκεκριμένου στόχου, αδιάκοπα χωρίς κενά, ενώ παράλληλα θα πρέπει να παρέχουν ένα ασφαλές δίκτυο προκειμένου να μεταφέρονται με ασφάλεια οι καταγεγραμμένες πληροφορίες των χρηστών που ζητούν οι Υπηρεσίες Ασφαλείας (“Professional cybersecurity solutions,” n.d.).

Η νόμιμη παρακολούθηση, πρέπει να επισημανθεί ότι δεν έχει σε τίποτα να κάνει με την μαζική παρακολούθηση ή το hacking, πράγματα δηλαδή τα οποία εκ των πραγμάτων είναι παράνομες πράξεις. Οι περισσότερες χώρες ανά τον κόσμο συμμερίζονται την άποψη ότι η νόμιμη παρακολούθηση θα πρέπει να βασίζεται σε συγκεκριμένα πρότυπα για να επιτευχθεί η διαλειτουργικότητα και η ομαλή συνεργασία μεταξύ των Αρχών Επιβολής του Νόμου και των παρόχων υπηρεσιών, διεθνής συνεργασία για την επιβολή του νόμου και επαρκής προστασία δεδομένων. Δεδομένων των τεράστιων δυνατοτήτων των υπηρεσιών των 5G, η προοπτική διάπραξης εγκλημάτων μέσω χρήσης των εν λόγω δικτύων και συσκευών IoT είναι δεδομένη. Οι πάροχοι τηλεπικοινωνιών θα πρέπει να συνεργαστούν με τις Αρχές Επιβολής του Νόμου και να βεβαιωθούν ότι τα συστήματα νόμιμης παρακολούθησης μπορούν να υποστηρίξουν την αύξηση του εύρους ζώνης και να λάβουν δεδομένα σε πραγματικό χρόνο.



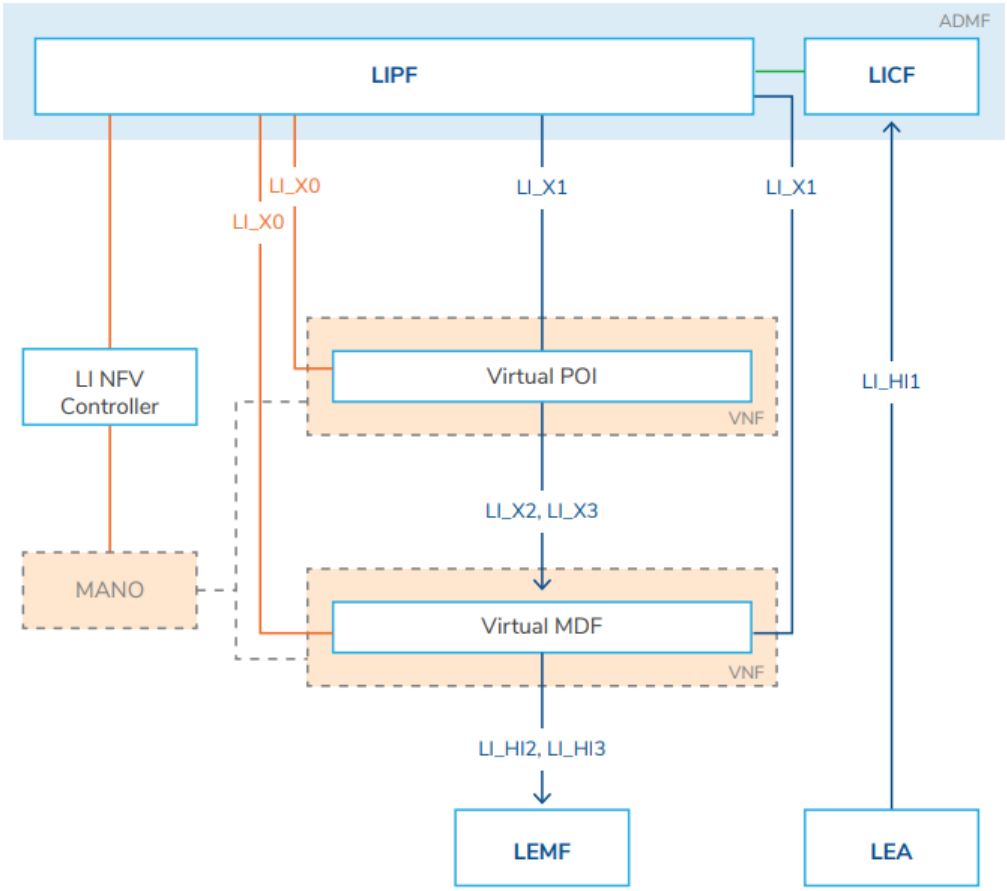
Εικόνα 21: Γενική αρχιτεκτονική του τρόπου λειτουργίας της νόμιμης καταγραφής δεδομένων των 5G.

Ελήφθη από: www.utimaco.com, 3GPP TS 33.126 version 15.1.0

Όταν όλα τα απαραίτητα κριτήρια για τον προσδιορισμό της επικοινωνίας ενός στόχου δεν είναι στατικά και δεν είναι διαθέσιμα από την αρχή, ορισμένα σημεία παρακολούθησης- Points Of Interception (POIs) δεν μπορούν να προβλεφθούν απευθείας, αλλά πρέπει να ενεργοποιηθούν. Η λειτουργία ενεργοποίησης ανιχνεύει τις επικοινωνίες-στόχους πραγματοποιώντας αναζητήσεις βάσει ορισμένων κριτηρίων (π.χ. συμβάντα δικτύου και υπηρεσιών) που ταιριάζουν με συγκεκριμένους κανόνες. Η εν λόγω λειτουργία, ενεργοποιεί δυναμικά το συσχετισμένο POI, το οποίο καταγράφει το περιεχόμενο επικοινωνίας-στόχου και εξάγει τις πληροφορίες που σχετίζονται με την παρακολούθηση, συμπεριλαμβανομένων των κανόνων που ενεργοποίησαν το POI αρχικά. Η ενεργοποίηση μπορεί να αλληλοεπιδράσει με άλλα POIs για τη λήψη πληροφοριών που συσχετίζονται.

Το 5G εισάγει ένα βελτιωμένο έλεγχο ταυτότητας χρήστη και μια ισχυρότερη κρυπτογράφηση δεδομένων το οποίο το κάνει πολύ πιο ασφαλές από το 4G επιτυγχάνοντας την καταπολέμηση απειλών που είχαν παραμείνει ανεπίλυτες ακόμη από το δίκτυο 2G. Οι προδιαγραφές ασφαλείας 5G δεν επιτρέπουν τη μετάδοση απλού κειμένου της μόνιμης ταυτότητας ενός συνδρομητή (SUPI) μέσω ραδιοεπικοινωνίας. Αντίθετα, η κρυπτογράφηση 256-bit σε επίπεδο συσκευής (που ονομάζεται "εξοπλισμός χρήστη" στη γλώσσα 5G) προστατεύει το SUPI (και κατ' επέκταση την τοποθεσία του

συνδρομητή) δημιουργώντας ένα λεγόμενο κρυφό αναγνωριστικό συνδρομής (SUCI) πριν από τη μετάδοση στο κεντρικό δίκτυο. Η SUCI καθιστά την τακτική παρακολούθηση κινητών συσκευών (από Αρχές αλλά και χάκερ) δύσκολη ή και αδύνατη (“Lawful Interception in the Digital Age - Utimaco,” n.d.).



Εικόνα 22: Απλουστευμένο εικονικό δίκτυο νόμιμης καταγραφής δεδομένων χρηστών 5G.
Ελήφθη από: www.utimaco.com

Η λύση της νόμιμης καταγραφής στο 5G, μπορεί να διασυνδέεται με όλες τις βασικές λειτουργίες δικτύου. Ιδίως η λειτουργία Ενοποιημένης Διαχείρισης Δεδομένων (Unified Data Management function), η οποία έχει τη δυνατότητα να αποκρύπτει την ταυτότητα του συνδρομητή. Σε αυτή τη βάση, η νόμιμη καταγραφή συνεχίζει να λειτουργεί στο 5G, παρά τη βελτιωμένη εμπιστευτικότητα της ταυτότητας συνδρομητή.
Σύμφωνα με την εταιρεία, όσον αφορά το εύρος ζώνης, ενώ το 4G επιτυγχάνει μέγιστη απόδοση περίπου 90 Mbps σήμερα, το 5G μπορεί αρχικά να επιτύχει μέγιστη απόδοση

6-7 φορές υψηλότερη. Έχοντας τις εν λόγω ταχύτητες κατά νου, η λύση για τις Αρχές Επιβολής του Νόμου θα πρέπει η καταγραφή επικοινωνιών σε αυτό το εύρος ζώνης και θα πρέπει να παρέχεται λειτουργία προσωρινής αποθήκευσης.

Στο δίκτυο 5G όλες οι λειτουργίες του είναι εικονικές. Η διαδικασία της νόμιμης καταγραφής δεδομένων σε ένα εικονοποιημένο περιβάλλον είναι μια ιδιαίτερη πρόκληση επειδή οι πάροχοι τηλεπικοινωνιών δεν μπορούν να διαμορφώσουν στατικά μια καταγραφή σε ένα φυσικό στοιχείο δικτύου. Τα «Σημεία Καταγραφών» (POIs) γίνονται ενεργά μέρη της λειτουργίας του δικτύου και αυτά μαζί με τη Λειτουργία Διαμεσολάβησης και Παράδοσης (MDF) ενδέχεται να γίνουν εικονικά και να έρθουν σε επαφή με τη λειτουργία παροχής μέσω μιας συγκεκριμένης εσωτερικής διεπαφής.

Το Multi-access Edge Computing και το Network Slicing Multi-access edge computing (MEC) αποτελούν cloud-based υπηρεσίες, οι οποίες είναι τεχνολογίες πραγματικού χρόνου (real-time), υψηλού εύρους ζώνης και χαμηλής καθυστέρησης, ενώ αποτελούν χαρακτηριστικά των AI, IoT και VR εφαρμογών, τα οποία στηρίζονται σε μια σταθερή και αδιάληπτη σύνδεση.

Το MEC σε όλο το 5G επιτρέπει την ταυτόχρονη χρήση ενός μεγάλου αριθμού συνδεδεμένων συσκευών χωρίς τη δημιουργία συμφόρησης (bottlenecks), το οποίο επιτυγχάνεται με τη χρήση των ορίων (edge) του δικτύου. Με αυτόν τον τρόπο έρχονται τα υπολογιστικά φορτία πιο κοντά στο κέντρο δεδομένων, γεγονός που βοηθά στην κατανομή των απαιτήσεων δικτύωσης.

Το κόνσεπτ «Μαζικά (Massive) IoT» (MIoT) έχει γίνει κοινός τόπος περιγραφής των τεραστίων ποσοτήτων διασυνδεδεμένων αισθητήρων και άλλων IoT συσκευών. Οι IoT συσκευές χρησιμοποιούν το ίδιο δίκτυο όπως και όλοι οι χρήστες, έτσι «Μαζικά (Massive) IoT» (MIoT) αναπόφευκτα σημαίνει ότι πολλές επικοινωνίες που δεν προέρχονται από φυσικά άτομα καθίστανται σχετικές με την πρόληψη και τη δίωξη του εγκλήματος.

Αυτό που η εν λόγω εταιρεία θεωρεί είναι ότι για όσο χρονικό διάστημα οι Αρχές Επιβολής του Νόμου μπορούν να αντιστοιχούν συσκευές IoT με τις συσκευές SUPI που επιτηρούν και αποτελούν στόχο, τότε οι πάροχοι τηλεπικοινωνιών μπορούν να προβλέπουν τυχόν «αναχαίτηση». Παρόλα αυτό το γεγονός ότι υφίστανται μεγάλοι αριθμοί IoT συσκευών και παρόχων επικοινωνιών, συνυπολογιζόμενου και του γεγονότος ότι πολλοί IoT χρήστες είναι ανώνυμοι στο δίκτυο, μας οδηγεί αναπόφευκτα στο γεγονός ότι οι Αρχές Επιβολής του Νόμου θα πρέπει να υποβάλλουν αιτήσεις στους

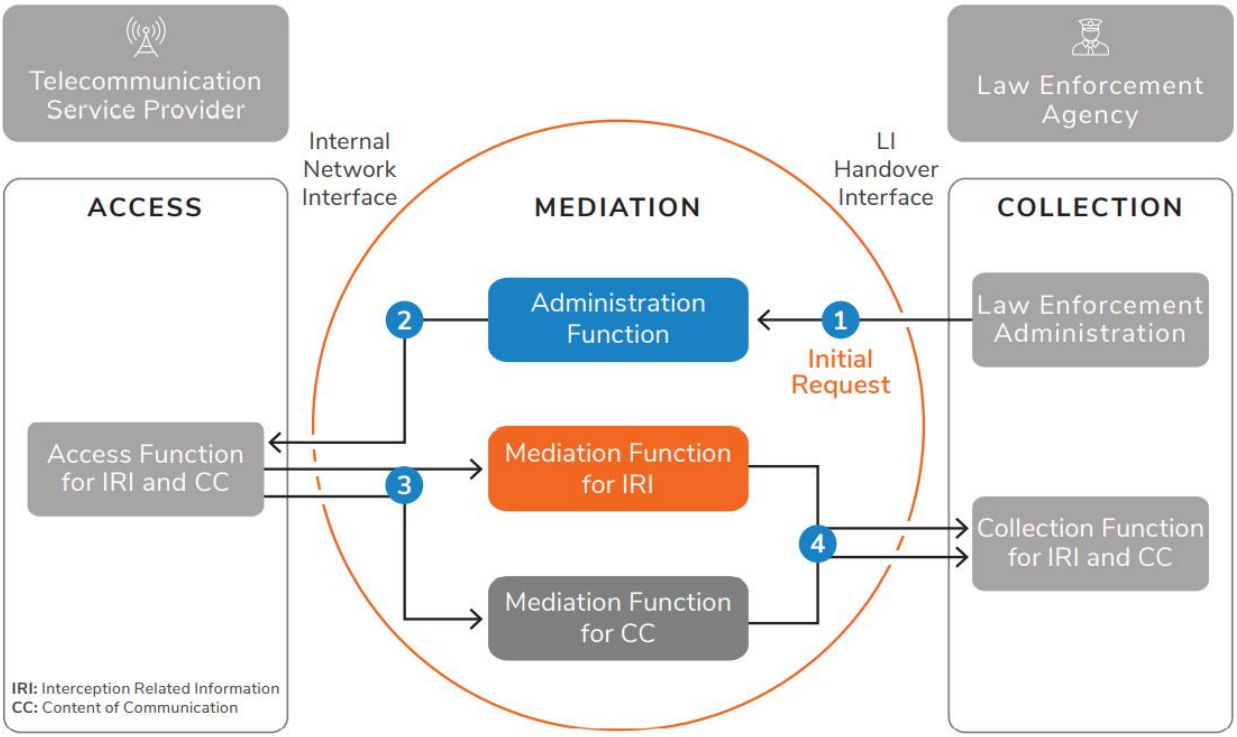
παρόχους IoT προκειμένου να ταυτοποιούν τους χρήστες των εν λόγω συσκευών-στόχων.

Επιπρόσθετα, σημαίνουσας σημασίας είναι η παραδοχή ότι η επικοινωνία μέσω συσκευών είναι με υψηλή κρυπτογράφηση και ακόμη και εάν οι πάροχοι δικτύου είναι σε θέση να καταγράψουν την κίνηση των δεδομένων και το περιεχόμενο των επικοινωνιών μεταξύ στόχων, αυτό δεν συνεπάγεται ότι έχουν και τα απαραίτητα κλειδιά αποκρυπτογράφησης ώστε να είναι επεξεργάσιμα από τις Αρχές.

Οι απαιτήσεις των Αρχών περί των νόμιμων καταγραφών προς τους παρόχους υπηρεσιών τηλεπικοινωνίας ((Internet service providers- ISPs)) που βασίζονται στο διαδίκτυο και στις υπηρεσίες σύννεφου (Cloud-based), αυξάνονται και η οδηγία της Ε.Ε. η οποία δημιουργεί ένα νέο Ευρωπαϊκό Ηλεκτρονικό Κώδικα Επικοινωνίας (European Electronic Communications Code (EECC)) είναι ένα παράδειγμα αυτού.

Σήμερα, οι πάροχοι υπηρεσιών σύννεφου υποστηρίζουν τα αιτήματα των Αρχών σύμφωνα με την ερμηνεία της διαδικασίας της άρσης απορρήτου των επικοινωνιών των εθνικών νόμων της κάθε χώρας ξεχωριστά και όχι σύμφωνα με την διεθνή πρότυπα καταγραφής δεδομένων.

Από την άλλη οι δρομολογητές (routers) και τα switches ανήκουν στις «έξυπνες» συσκευές καθώς διαμοιράζονται πληροφορίες και θεωρητικά θα ήταν πιθανό μια μη αυτόματη παροχή καταγραφής δεδομένων απευθείας σε αυτές τις συσκευές και ακολούθως απευθείας να αντιγράφεται η κίνηση αυτών των δεδομένων από εκεί. Όμως, οι πάροχοι τηλεπικοινωνιών δεν μπορούν να διασφαλίσουν ότι με την διαδικασία αυτή της καταγραφής σε κάποιο στοιχείο του δικτύου, δεν θα υπάρξει κατάχρηση της λειτουργίας. Δηλαδή, ενδεχομένως, δεν θα έχουν τη δυνατότητα να πιστοποιούν ότι η ενεργή καταγραφή δεδομένων σε συγκεκριμένη χρονική στιγμή αφορά σε χρήστη στόχο για τον οποίο υπάρχει σχετικό Βούλευμα Συμβουλίου Πρωτοδικών.



Εικόνα 23: Λειτουργικό μοντέλο αρχιτεκτονικής νόμιμης καταγραφής χρηστών δικτύων 5G.

Ελήφθη από: www.utimaco.com

«Ενεργητική» και «παθητική» καταγραφή δεδομένων χρηστών- στόχων.

«**Ενεργητική**» καταγραφή είναι η καταγραφή δεδομένων η οποία λειτουργεί ως λύση και αποτελεί αναπόσπαστο μέρος της υποδομής του δικτύου. Το σύστημα διαχείρισης καταγραφών χρηστών- στόχων δύναται άμεσα να ελέγχει τα στοιχεία του δικτύου όπως π.χ. δρομολογητές (routers) και σουιτς (switches), καθώς και να φιλτράρει και να ανακτά τα δεδομένα από το IRI και το CC απευθείας από τον κόμβο του δικτύου. Το εν λόγω σύστημα διαχείρισης λαμβάνει και λειτουργεί ως μεσάζων των IRI και CC προωθώντας τα στο εκάστοτε Κέντρο Διαχείρισης Καταγραφών των Αρχών Επιβολής του Νόμου (“Lawful Interception Addressing the Complex of 5G and MIoT - Utimaco,” n.d.).

Από την άλλη πλευρά, «**παθητική**» καταγραφή είναι αυτή κατά την οποία τα στοιχεία του δικτύου μεταφέρουν μια «αντιγραφή» όλων των καταγεγραμμένων

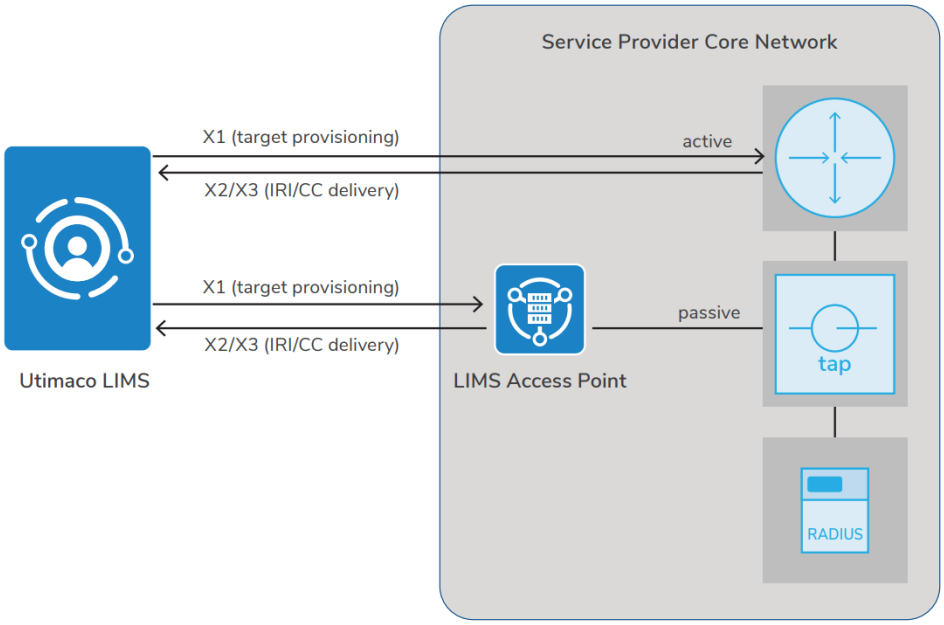
κινήσεων δεδομένων που πραγματοποιήθηκαν στο δίκτυο προς το σύστημα διαχείρισης καταγραφών.

Το φιλτράρισμα πραγματοποιείται στο αντίγραφο της κίνησης εντός του συστήματος διαχείρισης, που απορρίπτει την κυκλοφορία που ανήκει σε μη- στόχους. Αναλόγως, στέλνει τα δεδομένα των IRI και CC των στόχων στο Κέντρο Διαχείρισης Καταγραφών των Αρχών Επιβολής του Νόμου. Η «παθητική» καταγραφή θεωρείται απαραίτητη στην περίπτωση που τα στοιχεία του δικτύου δεν υπάρχει η δυνατότητα καταγραφής δεδομένων για μια συγκεκριμένη χρονική στιγμή. Η επισύνδεση της διεύθυνσης IP για παράδειγμα απαιτεί την ανίχνευση των κωδικών εισόδου του χρήστη στον κεντρικό διακομιστή του παρόχου τηλεπικοινωνιών περί ελέγχου ταυτότητας και εξουσιοδοτήσεων. Όμως, οι περισσότεροι κεντρικοί διακομιστές των παρόχων δεν υποστηρίζουν ένα ολοκληρωμένο σύστημα καταγραφών δεδομένων χρηστών- στόχων.

Υβριδικό μοντέλο καταγραφής δεδομένων χρηστών- στόχων.

Το «υβριδικό» μοντέλο καταγραφής αποτελεί έναν συνδυασμό της ενεργητικής και παθητικής τεχνικής και επικρατεί όλο και περισσότερο ως η αρτιότερη τεχνική καταγραφής δεδομένων. Η καταγραφή της κίνησης των δεδομένων στα δίκτυα μέσω των σουιτς (switches) είναι μια προσιτή τεχνική η οποία μπορεί εύκολα να πραγματοποιηθεί και αυτό διότι τα περισσότερα switches υποστηρίζουν ολοκληρωμένες λειτουργίες καταγραφών. Επίσης, ολοκληρωμένες λειτουργίες καταγραφών υποστηρίζουν οι περισσότερες εταιρείες δρομολογητών καθώς και οι εταιρείες των Voice-over-IP switches.

Η εν λόγω τεχνική καταγραφής δεδομένων αποτελεί την προτιμότερη επιλογή όταν οι συσκευές switches και routers παρέχουν την δυνατότητα καταγραφής της κίνησης των δεδομένων, παρόλα αυτά όμως πρέπει να επισημανθεί ότι η κίνηση που πρέπει να παρακολουθηθεί δεν μπορεί να εντοπιστεί άμεσα (π.χ. από έναν τηλεφωνικό αριθμό). Σε ένα δίκτυο αυτό θα σήμαινε ότι χρειάζεται να γίνει έρευνα ώστε να εντοπιστεί η δυναμική IP ενός συγκεκριμένου στόχου (χρησιμοποιώντας την «παθητική» τεχνική), δίνοντας εντολή στο δρομολογητή (router) να παρεμποδίσει την κυκλοφορία από τη συγκεκριμένη διεύθυνση IP (χρησιμοποιώντας την «ενεργητική» τεχνική), αναμεταδίδοντας την κίνηση στο σύστημα καταγραφής δεδομένων των Αρχών.



Εικόνα 24: Βασική αρχιτεκτονική υβριδικού μοντέλου καταγραφής δεδομένων. Ελήφθη από: www.utimaco.com

Τα βασικά συστατικά μέρη της εταιρείας «Utimaco» (όπως και των άλλων αντίστοιχων εταιρειών που εξετάστηκαν) σχετικά με την διαδικασία που ακολουθείται για τη νόμιμη καταγραφή δεδομένων χρηστών- στόχων είναι επιγραμματικά τα κάτωθι:

- Διακομιστής Διαχείρισης Συστήματος Νόμιμων Καταγραφών.
- Συσκευή Μεσολάβησης Συστήματος Νόμιμων Καταγραφών.
- Σημείο πρόσβασης Συστήματος Νόμιμων Καταγραφών.
- Πύλη (Gateway) Συστήματος Νόμιμων Καταγραφών.
- Μονάδα Απομακρυσμένης Προμήθειας Συστήματος Νόμιμων Καταγραφών.

5.10 Η επίδραση του 5G στη διαδικασία της νόμιμης καταγραφής δεδομένων χρηστών.

Η νόμιμη καταγραφή δεδομένων και πληροφοριών περιλαμβάνει τη συλλογή, χρήση και διαχείριση «μεταδεδομένων» (metadata) του περιεχομένου των κατασχεθεισών συσκευών ως μέσω αποδεικτικών στοιχείων, αντί της χρήσης της ίδιας της συσκευής από μόνη της ως πειστήριο.

Μια ουσιαστική λειτουργία για τις Αρχές Επιβολής του Νόμου κατά τη διαδικασία λήψης καταγεγραμμένων δεδομένων είναι η «Λειτουργία Μεσολάβησης». Ουσιαστικά αναφερόμαστε στον τρόπο με τον οποίο λαμβάνονται τα δεδομένα που ζητήθηκαν από το δίκτυο και τα οποία μορφοποιούνται σε επεξεργάσιμη μορφή. Η μορφοποίηση αυτή γίνεται με τέτοιο τρόπο ώστε να τα δεδομένα που έχουν ληφθεί (π.χ. μια φωνητική κλήση, ένα mms ή μια σελίδα διαδικτύου), να είναι επεξεργάσιμα και δυνατόν να αναλυθούν από τις Αρχές.

Υπάρχουν δυο (2) τρόποι προκειμένου να λάβουμε δεδομένα από το δίκτυο:

i) απευθείας μέσω των παρόχων δικτυακού εξοπλισμού (π.χ. Nokia, Ericsson, Samsung, κτλ), παρέχοντας, σε αυτούς, μια λίστα με τα στοιχεία των στόχων. Ακολούθως, όλα τα αιτούμενα δεδομένα δύναται να τα λάβουμε από αυτούς και

ii) μέσω της παθητικής προσέγγισης ή της τεχνολογίας αισθητήρων με χρήση οπτικών συνδέσμων. Έτσι, μπορούμε να εξάγουμε δεδομένα αφαιρώντας τις σχετικές κεφαλίδες (Headers), στοχοποιώντας την επιθυμητή συσκευή.

Σύμφωνα με ανάλυση της ιδιωτικής εταιρείας «SS8 Network» (“SS8,” n.d.), η οποία δραστηριοποιείται στον τομέα ανάπτυξης λογισμικού νόμιμων καταγραφών δεδομένων για λογαριασμό των Αρχών Επιβολής του Νόμου, πολλές χώρες ανά τον κόσμο προτιμούν τον δεύτερο προαναφερόμενο τρόπο διότι είναι απόλυτα ασφαλές και υπό τον έλεγχό τους. Με αυτόν τον τρόπο, κανένας δεν μπορεί να γνωρίζει τους στόχους τους οποίους επιτηρούν οι Αρχές. Η πρόκληση που υπάρχει με τη χρήση των δικτύων 5G είναι σχετικά με την κρυπτογράφηση που χρησιμοποιείται και με το γεγονός ότι αναφερόμαστε σε ένα δίκτυο που χρησιμοποιεί τεχνολογία σύννεφου (cloud native).

Μια άλλη σημαντική εφαρμογή της διαδικασίας νόμιμης καταγραφής δεδομένων, είναι η διατήρηση και αποθήκευση των ληφθέντων δεδομένων. Η εν λόγω λειτουργία αποτελεί ένα πολύ ισχυρό εργαλείο ειδικά όταν προβαίνουμε στην «ζωντανή» παρακολούθηση των δεδομένων ενός στόχου- χρήστη του δικτύου 5G.

Τέλος, μια άλλη χρήσιμη εφαρμογή είναι αυτή του γεωεντοπισμού του στόχου. Αυτό μπορεί να γίνει παθητικά για μαζική συλλογή πληροφοριών ή μπορεί να γίνει στοχευμένα από τα GMLC (Gateway Mobile Location Center) τα οποία περιέχουν λειτουργίες που απαιτούνται για την υποστήριξη υπηρεσίας βάσει τοποθεσίας. Η λήψη της τοποθεσία μέσω των προγενέστερων δικτύων 2G, 3G και 4G είναι αρκετά ακριβής ειδικά όταν εξάγονται τα δεδομένα από τις ίδιες τις συσκευές κινητών τηλεφώνων των στόχων, αλλά από το δίκτυο 5G με την βελτίωση της τοποθεσίας που λαμβάνουμε είναι σε ακόμη καλύτερο επίπεδο. Αυτό διότι δεν λαμβάνουμε απλά συντεταγμένες τύπου x και y στον άξονα αλλά λαμβάνουμε δεδομένα και του άξονα z όπου δίνεται η δυνατότητα οριζόντιας τοποθέτησης ανθρώπων και κτιρίων, κάνοντας ακριβέστερο τον γεωεντοπισμό.

Ακολούθως, υφίστανται σουίτες παρακολούθησης των καταγεγραμμένων δεδομένων που χρησιμοποιούν οι Αρχές. Αυτές οι σουίτες παρέχουν μια επανόρθωση, όπου μονίμως υφίσταται ένας προβληματισμός σχετικά με τη δυνατότητα επανόρθωσης των δεδομένων του ήχου. Παράλληλα όμως υπάρχουν και πλεονεκτήματα σχετικά με την ανάλυση μεγάλων δεδομένων καθώς και με την δυνατότητα χαρτογράφησης γεωεντοπισμούm, όπως η συνεχόμενη παρακολούθηση και ο σχεδιασμός της κίνησης του στόχου ακόμη και ανάμεσα σε κτίρια.

5.11 Αλλαγές που συντελέστηκαν με την έλευση των δικτύων 5G και η επίδρασή τους στη διαδικασία της νόμιμης καταγραφής δεδομένων.

Μπορούμε να διαχωρίσουμε τις αλλαγές που συντελέστηκαν με την εφαρμογή των δικτύων 5G σε **τέσσερις (4) βασικούς πυλώνες**. Έχουμε:

α) της εκτέλεση, όπου έχουμε σημαντικές διαφοροποιήσεις σε σχέση με τις παλαιότερες μορφές δικτύου όσον αφορά την εξαιρετικά χαμηλή καθυστέρηση, την υψηλή απόδοση και την αύξηση της χωρητικότητας (των ταυτόχρονων χρηστών). Αυτά με τη σειρά τους συμβάλουν στην παροχή δεδομένων τόσο σε λειτουργία «at the edge» όσο και «in the core»,

β) της τοπολογίας του δικτύου. Με την υψηλή απόδοση που παρέχεται, έχουμε πλέον την είσοδο νέων στοιχείων και νέες διαδικασίες αναγνώρισης στόχων (όπως π.χ.

το γεγονός ότι πλέον δεν χρησιμοποιούμε ως αναγνωριστικό τον αριθμό IMEI μιας συσκευής αλλά ένα μόνιμο αναγνωριστικό τα -αναφερόμενα και παραπάνω- SUPI και SUCI,

γ) της βελτιωμένης τοποθεσίας. Η εν λόγω αλλαγή επιτυγχάνεται από το γεγονός ότι έχουμε μικρότερες και διάσπαρτες σε πολλά σημεία κυψέλες εκπομπής σήματος δικτύου και έτσι μπορεί να συγκεκριμενοποιηθεί καλύτερα ο γεωεντοπισμός ενός στόχου. Αυτό συνεπάγεται ότι από την απεικόνιση στίγματος σε έναν χάρτη 2D, έχουμε πλέον τη δυνατότητα απεικόνισης σε ένα 3D χάρτη.

Τέλος, έχουμε τον πυλώνα **δ) της κρυπτογράφησης** και ό,τι αυτό συνεπάγεται με τους προσομοιωτές κυψελών.

5.12 Το 5G απαιτεί νέες προδιαγραφές για τη διαδικασία καταγραφής δεδομένων.

Τα δίκτυα 2G, 3G και 4G δεν χαρακτηρίζονται από ιδιαίτερες αλλαγές στις προδιαγραφές τους ως προς τη διαδικασία της νόμιμης καταγραφής δεδομένων. Με την έλευση των δικτύων 5G, έχουμε μεν την επαναχρησιμοποίηση των ίδιων στάνταρ με τα δίκτυα παλαιότερων γενεών αλλά παράλληλα έχουμε την ανάπτυξη νέων αρχιτεκτονικών- μερών.

Σε σχέση με τα παλαιότερης γενιάς δίκτυα, υπήρξε σε μεγάλο βαθμό επαναχρησιμοποίηση συστατικών μερών για την μεταφορά των δεδομένων όπως του HI2 και HI3 (τα οποία έχουν αναλυτικά αναφερθεί παραπάνω) ως προς τις διεπαφές. Δια μέσω αυτών των διεπαφών τα δεδομένα IRI και CC παραδίδονται από το δίκτυο στις Αρχές Επιβολής του Νόμου για την αξιοποίηση.

Αυτή η διαδικασία έχει -κατά βάση- παραμείνει η ίδια, έχει όμως θεμελιώδη διαφορά στη δομή του PDU, δηλαδή του ειδικού μπλοκ μεταφοράς των πληροφοριών μέσω του δικτύου. Αυτό ακριβώς απαιτεί αναβάθμιση τόσο στη διαδικασία που πραγματοποιείται η νόμιμη καταγραφή όσο και στη «Λειτουργία Παρακολούθησης Δεδομένων» (Law Enforcement Monitoring Function/ LEMF) των Αρχών του Νόμου.

Επίσης, αλλαγές έχουμε και σε άλλες διεπαφές. Για παράδειγμα, έχουμε την εμφάνιση της **X0** διεπαφής η οποία ουσιαστικά μεταφέρει δεδομένα από το σύστημα

διαμεσολάβησης στο δίκτυο και εγκαθιδρύει μια «εμπιστοσύνη» μεταξύ τους. Αυτό συμβαίνει διότι όλα τα δίκτυα 5G είναι εικονοποιημένα και έτσι θα πρέπει να υπάρχει μια διεπαφή «εμπιστοσύνης» για τη μεταφορά των δεδομένων. Επίσης, θα πρέπει να εγκατασταθεί και ένας κρυπτογραφημένος φορέας πριν την παροχή πληροφοριών από τον στόχο.

Επιπρόσθετα, έχουμε τη διεπαφή **Hi3a** η οποία έχει να κάνει με το «Περιεχόμενο Επικοινωνίας του Σημείου Καταγραφής» (Content Communication Point Of Interception Aggregator/ CC-PAG). Αυτή η λειτουργία μπορεί να αναπτυχθεί είτε κεντρικά είτε οπουδήποτε έχουμε πρόσβαση πακέτου στο δίκτυο. Η εν λόγω διεπαφή, πρέπει να είναι μια εικονική εφαρμογή που να μπορεί να μετατοπίζεται, ειδάλλως θα έχουμε στατικά στοιχεία δικτύου.

Η **HI4** αποτελεί μια νέα διεπαφή παράδοσης με τον αριθμό τέσσερα (4) που εμφανίζεται στα δίκτυα 5G, σχετικά με τη μεταβίβαση δεδομένων. Ουσιαστικά η λειτουργία της έγκειται στο να μεταφέρει αποκλειστικές πληροφορίες σύνδεσης και αποσύνδεσης στο σύστημα.

Ένα από τα πράγματα που έκανε την έλευσή του με τα δίκτυα 5G είναι η σύνδεση πολλαπλών συσκευών IoT, το οποίο παρατηρούμε να πραγματοποιείται βαθμιαία. Αυτό συνεπάγεται ότι όποτε έχουμε για παράδειγμα μια νέα σύναψη συμβολαίου για κινητή τηλεφωνία, δε θα έχουμε πλέον μόνο την συσκευή του κινητού τηλεφώνου ή το «έξυπνο ρολόι» μας συνδεδεμένο, αλλά και διάφορες οικιακές συσκευές όπως το ψυγείο, το πλυντήριο, το κλιματιστικό κ.ά., όλα σε έναν λογαριασμό με όλες τις επιλογές λειτουργίας των προαναφερόμενων συσκευών να γίνονται μέσω των δικτύων 5G. Τα ανωτέρω σημαίνουν ότι εάν επιθυμούμε να προσδιορίσουμε έναν στόχο και να λάβουμε όλα τα δεδομένα αυτού του χρήστη, μπορεί να προκύψουν παράπλευρες επιβαρύνσεις λαμβάνοντας και πληροφορίες που δεν είναι και τόσο χρήσιμες ή δεν απαιτούνται.

5.13 Προκλήσεις των δικτυών 5G σε σχέση με το πρωτόκολλο μεταφοράς TCP.

Στην δικτύωση των υπολογιστών το πρωτόκολλο μεταφοράς TCP είναι το πρωτόκολλο επικοινωνίας που χρησιμοποιείται στο διαδίκτυο. Ένα πρωτόκολλο

επικοινωνίας υπολογιστών (computer communication protocol) και αποτελεί μια περιγραφή κανόνων οι οποίοι θα πρέπει να ακολουθούνται από τους υπολογιστές προκειμένου να μπορούν να επικοινωνούν μεταξύ τους.

Το πρωτόκολλο TCP προορίζεται για την επικοινωνία από άκρη σε άκρη μεταξύ εφαρμογών των υπολογιστών. Ουσιαστικά, παρέχει αξιόπιστη, ταξινομημένη και ελεγχόμενη ως προς τα σφάλματα παράδοση μιας ροής οκτάδων (bytes) μεταξύ των εφαρμογών. Όταν μια εφαρμογή θελήσει να επικοινωνήσει με μια άλλη εφαρμογή μέσω του TCP, στέλνει μια «αίτηση επικοινωνίας». Αυτή η αίτηση θα πρέπει να σταλεί σε μια συγκεκριμένη διεύθυνση. Αφού καθιερωθεί μια χειραψία (handshake) ανάμεσα στις δύο εφαρμογές, το TCP θα καθιερώσει μια ταυτόχρονη αμφίπλευρη (full-duplex) επικοινωνία ανάμεσα στις δύο εφαρμογές. Παρέχει επίσης, υπηρεσίες όπως προσανατολισμένη επικοινωνία στη σύνδεση, αξιοπιστία και έλεγχο ροής (“Introducing the Internet Protocol Suite (System Administration Guide, Volume 3),” n.d.).

Το Πρωτόκολλο Ελέγχου Μετάδοσης (Transmission Control Protocol/ TCP) είναι ένα από τα κύρια πρωτόκολλα του διαδικτύου (“Wayback Machine,” 2016). Προήλθε από την αρχική εφαρμογή του δικτύου στην οποία συμπλήρωνε το Πρωτόκολλο Διαδικτύου (Internet Protocol/ IP), που εκτελούνται σε κεντρικούς υπολογιστές και επικοινωνούν μέσω ενός δικτύου IP.

Ένα από τα νέα στοιχεία που έχουμε στα δίκτυα 5G είναι η εξαιρετικά αυξημένη (συγκριτικά με τα παλαιότερης γενιάς δίκτυα) ταχύτητα μεταφοράς δεδομένων. Από την εμφάνιση των δικτύων της πρώτης γενιάς (1G) μέχρι τα τωρινά δίκτυα πέμπτης γενιάς (5G) υπάρχει μια σταθερή αύξηση και βελτίωση των επιδόσεων του ρυθμού ταχύτητας μεταφοράς δεδομένων.

Όταν αρχικώς πραγματοποιούνταν μια σύνδεση με ένα στοιχείο δικτύου, το μόνο που χρειαζόσουν ήταν μια μονή υποδοχή TCP και μια υποδοχή σύνδεσης, το οποίο ήταν αρκετό διότι η κίνηση (traffic) ποτέ δεν ξεπερνούσε το ένα (1) Gbps για έναν στόχο και έτσι υπήρχε η δυνατότητα να παραδοθούν αυτά τα δεδομένα χωρίς κάποιο πρόβλημα γεωμεσολάβησης (geomediation), να τα μορφοποιήσουν σωστά και να τα παραδώσουν.

Στα δίκτυα 5G για παράδειγμα -θεωρητικά- μεταφέρονται συγκεκριμένα μεγέθη δεδομένων παγκοσμίως μέσω πέντε (5) εφαρμογών και σε μια εξ αυτών των εφαρμογών έχουμε επτά μισή (7,5) Gbps δεδομένων προς παράδοση. Μια πιθανή λύση είναι η αλλαγή των συνδέσεων TCP σε UDP, το οποίο όμως αποτελεί ένα αναξιόπιστο πρωτόκολλο σε σύγκριση με το TCP, διότι, αν και επιτυγχάνονται υψηλότερες επιδόσεις,

επιτρέπει την απόρριψη μεμονωμένων πακέτων χωρίς επανάληψη, π.χ στη μετάδοση ομιλίας και βίντεο (“Computer Networks - A Tanenbaum - 5th edition.pdf,” n.d.). Έτσι, η λύση που προτάθηκε από την ιδιωτική εταιρεία ανάπτυξης λογισμικού «SS8 Networks» και «CISCO», ήταν η πολλαπλής υποδοχής σύνδεση TCP. Η πρόκληση σε αυτήν την περίπτωση ήταν η μεταφορά ενός μεγάλου όγκου δεδομένων από τη Λειτουργιά Διαμεσολάβησης στις Αρχές Επιβολής του Νόμου και η λήψη αυτών των δεδομένων.

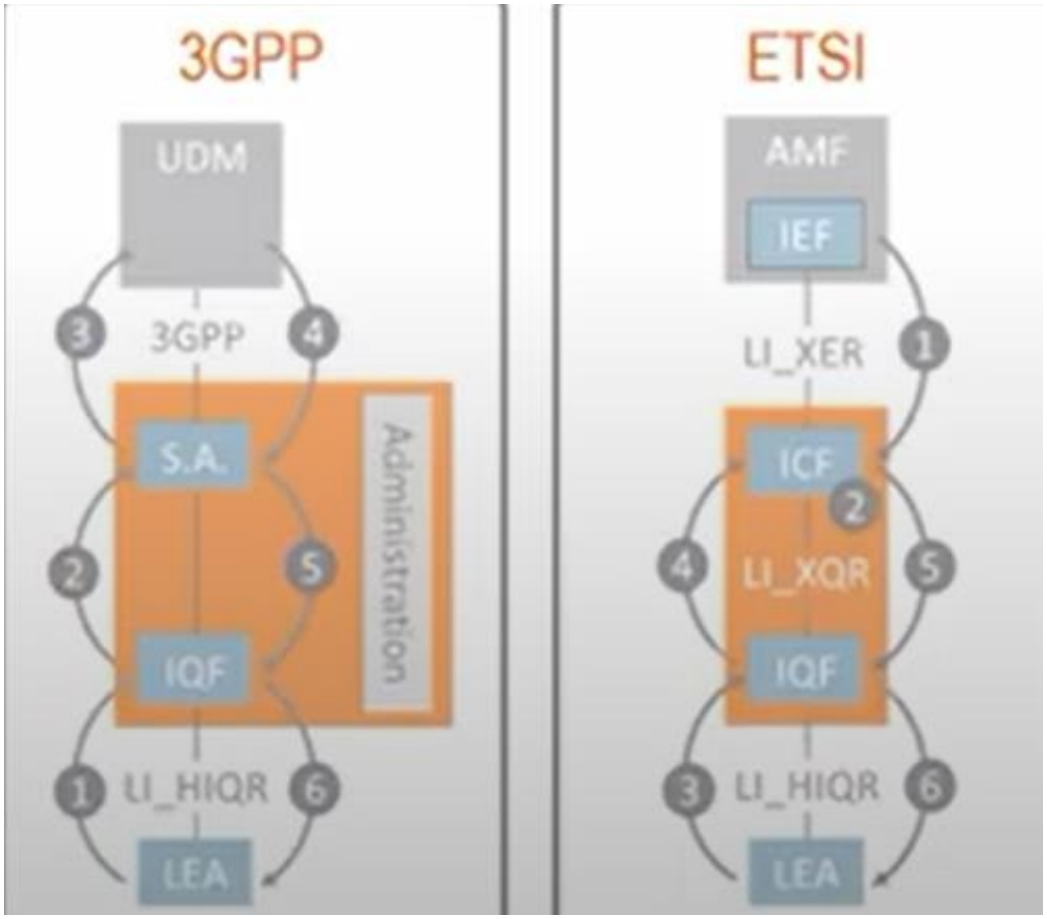
Αυτό που πραγματοποιείται πλέον κατά τη διαδικασία της νόμιμης καταγραφής δεδομένων είναι για παράδειγμα όταν έναν στόχος- χρήστης παρακολουθεί διάφορα βίντεο σε live streaming από πλατφόρμες όπως της Netflix ή της Youtube, να μην αποθηκεύονται και να μην αποστέλλονται στις Αρχές που διενεργούν την έρευνα, αλλά να τους μεταβιβάζεται μια αναφορά που να περιλαμβάνει μια περίληψη του τι παρακολουθείται ανά τριάντα δευτερόλεπτα (30’’) ή ένα λεπτό (1’). Ακολούθως, οι επιλογές που δίδονται είναι να απορριφθεί η αποθήκευση ενός βίντεο το οποίο δεν αποτελεί αντικείμενο έρευνας και έτσι επιτυγχάνεται η σημαντική μείωση του εύρους ζώνης που χρησιμοποιείται. Η άλλη επιλογή είναι η διατήρηση αυτών των δεδομένων και η παράδοσή τους στη Λειτουργία Παρακολούθησης για περαιτέρω ανάλυση από τις Αρχές.

5.14 Η ταυτοποίηση των συνδρομητών του δικτύου 5G.

Από την πλευρά των κυψελών του δικτύου, έχουμε την λειτουργία αποτύπωσης του IMSI το οποίο χρησιμοποιείται κατά κόρον από τις Αρχές για την αναγνώριση ατόμων και συσκευών καθώς και για τον εντοπισμό μιας συσκευής.

Αυτό που συμβαίνει όμως στα δίκτυα 5G είναι ότι σε αυτά δεν μεταφέρεται το SUPI δηλαδή η ταυτότητα της συσκευής ή του χρήστη, αλλά μεταφέρεται το SUPI ως SUCI. Με αυτόν τον τρόπο, είναι αδύνατον να δεσμευτούν τα δεδομένα που πρέπει από τις Αρχές.

Προκειμένου να προσπεραστεί αυτό το πρόβλημα και να επιτευχθεί η ταυτοποίηση ενός SUPI με ένα SUCI, υφίστανται δύο (2) τρόποι: α) μέσω της μεθόδου του 3GPP και β) μέσω της μεθόδου του ETSI.



Εικόνα 25: Μέθοδοι ταυτοποίησης SUPI με SUCI.

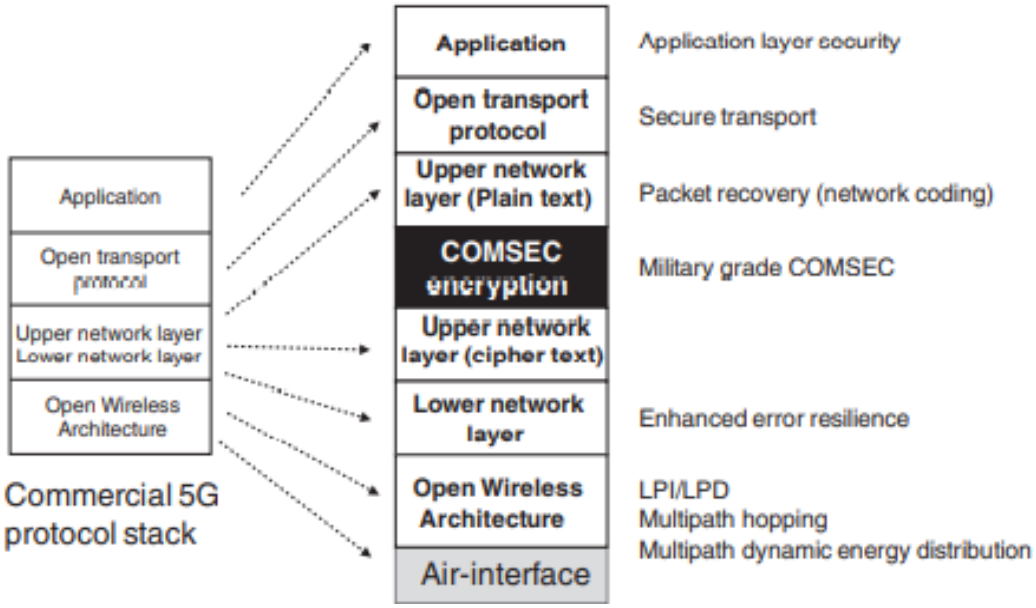
Ελήφθη από: https://www.youtube.com/watch?v=rgYt8jVxDkc "Telecoms Europe 5G 2021: Impact of 5G on lawful interception and law enforcement. By SS8 Networks"

6 Πρακτική εφαρμογή και συνδρομή των δικτύων 5G *(πέραν της νόμιμης καταγραφής δεδομένων)* στην εξιχνίαση υποθέσεων από τις Αρχές Επιβολής του Νόμου.

Σύμφωνα με μελέτη άρθρων ως προς την υιοθέτηση της χρήσης των δικτύων 5G από στρατιωτικές υπηρεσίες διαπιστώθηκε ότι οι εφαρμογές 5G δεν περιορίζονται μόνο στη λειτουργία των συσκευών των κινητών τηλεφώνων. Πολλές βιομηχανίες προσπαθούν να αξιοποιήσουν το εύρος ζώνης που κυκλοφόρησε για το 5G και τις δυνατότητες που αναπτύχθηκαν για την κατασκευή εταιρικών ασύρματων συστημάτων που βασίζονται σε φάσμα 5G,σε στοίβες πρωτοκόλλου (protocol stack) και πρωτόκολλα ανοιχτού κώδικα για την κατασκευή νέων ιδιωτικών ασύρματων συστημάτων υψηλής χωρητικότητας. Μία από αυτές τις βιομηχανίες να αποτελεί και ο τομέας των στρατιωτικών επικοινωνιών και των επικοινωνιών των Σωμάτων Ασφαλείας.

Όπως είναι ευλόγως κατανοητό, οι πιο σημαντικοί προβληματισμοί αναφορικά με την εφαρμογή και τη χρήση της τεχνολογίας 5G σε αυτούς τους τομείς αποτελούν η ασφάλεια και οι τυχόν ευπάθειες των δικτύων. Σύμφωνα με μελέτη του George F. Elmasry (Elmasry, 2020), η πιο σημαντική από τις πολλές προκλήσεις ασφαλείας που υφίστανται στις επικοινωνίες των εν λόγω τομέων είναι αυτή της πρόσβασης στο «Δυναμικό Εύρος Ζώνης» (Dynamic Spectrum Access/DSA).

Όσον αφορά την εφαρμογή του 5G στις στρατιωτικές επικοινωνίες, η έννοια σε αυτές τις φάσεις ανάπτυξης στρατιωτικών τεχνολογιών επικοινωνιών είναι να αναζητήσουμε τις τεχνικές βελτίωσης του air-interface όπου αυξάνουν την ασφάλεια 5G (Elmasry, 2020).



Εικόνα 26: Η υιοθέτηση του πρωτοκόλλου 5G από στρατιωτικές υπηρεσίες. Πηγή: https://ieeexplore.ieee.org/document/9200398 "DSA and 5G Adaptation to Military Communications"

Σύμφωνα με την παραπάνω εικόνα, τα βασικά συστατικά στοιχεία που απαιτούνται προκειμένου να επιτύχουμε μια ασφαλή επικοινωνία στα Σωμάτα Ασφαλείας και στο Στρατό είναι τα κάτωθι:

1. Η προσθήκη ενός ισχυρού επιπέδου εφαρμογής ασφαλείας (Application layer security). Η ασφάλεια επιπέδου εφαρμογής αναφέρεται σε τρόπους προστασίας εφαρμογών web στο επίπεδο εφαρμογής από κακόβουλες επιθέσεις. Δεδομένου ότι το επίπεδο εφαρμογής είναι το πλησιέστερο επίπεδο στον τελικό χρήστη, παρέχει στους χάκερ τη μεγαλύτερη δυνατότητα απειλής. Η μη ισχυρή ασφάλεια επιπέδου εφαρμογής μπορεί να οδηγήσει σε ζητήματα απόδοσης και σταθερότητας, κλοπή δεδομένων και, σε ορισμένες περιπτώσεις, μείωσης του δικτύου (π.χ. DDoS επιθέσεις, SQL injections, cross-site scripting).

2. Η προσθήκη ενός ισχυρού πρωτοκόλλου μεταφοράς (transport protocol).

3. Αύξηση των δυνατοτήτων ανάκτησης πακέτων απλού κειμένου (plain text layer packet recovery capabilities).

4. Προσαρμογή του πρωτοκόλλου 5G με κρυπτογράφηση στρατιωτικού τύπου.

5. Αύξηση της ανθεκτικότητας σφάλματος κατώτερου επιπέδου δικτύου.

6. Ανάπτυξη ειδικού MU MIMO hardware, δηλαδή τεχνολογίας που επιτρέπει τους δρομολογητές να επικοινωνούν με πολλαπλές συσκευές ταυτόχρονα, αυξάνοντας τις ταχύτητες και μειώνοντας το χρόνο.

Το 5G και η «Τμηματοποίηση» του Δικτύου επιτρέπουν τη λειτουργία πολλαπλών απομονωμένων δικτύων χρησιμοποιώντας μια κοινόχρηστη υποδομή δικτύου 5G. Έτσι, υπηρεσίες με αυστηρές απαιτήσεις για την ασφάλεια, όπως οι προαναφερόμενες, μελετούν τη δυνατότητα να κινηθούν προς την κατεύθυνση χρήσης δημόσιων δικτύων επικοινωνίας 5G.

Ωστόσο, καθίσταται πιο πρακτικό για το στρατό και τα Σ.Α. να χρησιμοποιούν το δημόσιο δίκτυο του 5G και το Network Slicing, όπου μπορούν να δημιουργηθούν απομονωμένα δίκτυα σε μια κοινόχρηστη υποδομή δικτύου. Αυτά τα δίκτυα έχουν συχνά ανώτερη κάλυψη και χωρητικότητα (Bastos et al., 2021).

Ενδεικτικά κάποιες σημαντικές απαιτήσεις που θα πρέπει να πληρούνται ώστε να είναι δυνατή η χρήση των δικτύων 5G από τα Σ.Α. και τον στρατό, είναι οι κάτωθι:

-Απομόνωση.

Η απομόνωση αφορά στους πόρους δικτύου και στο επιπέδου διαχείρισης. Η εν λόγω απαίτηση δύναται να οριστεί ως η ιδιότητα που οι υπηρεσίες σε ένα τμήμα μπορούν να λειτουργούν χωρίς καμία άμεση ή έμμεση επιρροή από δραστηριότητες σε άλλα τμήματα καθώς και τυχόν ανεπιθύμητης επιρροής των παρόχων.

-Ασφάλεια.

Καθώς η μεταφορά διαβαθμισμένων πληροφοριών μέσω ασφαλούς δικτύου αποτελεί υψηλή προτεραιότητα, κάποιοι φορείς επιθέσεων των κινητών δικτύων θα πρέπει να απομακρυνθούν όπως για παράδειγμα με την απόλυτη απομόνωση από το διαδίκτυο. Επίσης, η κρυπτογράφηση από άκρη σε άκρη (End-to-end encryption) αποτελεί μια σημαντική απαίτηση ασφαλείας.

-Υψηλή διαθεσιμότητα.

Η υψηλή διαθεσιμότητα αποτελεί μια σημαντική απαίτηση για τη χρήση των δικτύων 5G καθώς, ο χρόνος λειτουργίας σε οποιαδήποτε περιοχή θα πρέπει να είναι 99.999%

-Ποιότητα Υπηρεσιών (Quality of Service (QoS)).

-Διαχωρισμός του Control και του User Plane (CUPS)

6.1 Η Υπολογιστικής Νέφους (Cloud computing/ CC) και τα δίκτυα 5G.

Οι ολοένα αυξανόμενες ανάγκες τόσο για τον χειρισμό μεγάλου όγκου δεδομένων -τα οποία θα πρέπει να αποθηκεύονται προκειμένου οι Υπηρεσίες των Σωμάτων Ασφαλείας να έχουν πρόσβαση στις επιθυμητές πληροφορίες- όσο και η ανάγκη για άμεση και χωρίς καθυστερήσεις πρόσβαση σε αυτά, μας οδηγούν στη προτεινόμενη λύση της Υπολογιστικής Νέφους (Cloud Computing) και τις υπηρεσίες που απορρέουν από την χρήση αυτής της τεχνολογίας. Το πρόβλημα εντοπίζεται στο γεγονός ότι επιβάλλεται να δαπανώνται ολοένα και περισσότερα χρηματικά ποσά προκειμένου να αποθηκεύονται με ασφάλεια δεδομένα, χωρίς ουσιαστικά να υφίσταται μια και μοναδική βάση η οποία να χρησιμοποιείται από όλες τις Υπηρεσίες.

Στην περίπτωση που το ελάχιστο επίπεδο ασφαλείας δεν μπορεί να εγγυηθεί, απλά δεν τηρούνται βάσεις μεγάλων δεδομένων. Επιπρόσθετα, όλο αυτό δημιουργεί ανάγκες ίδρυσης ειδικών Κέντρων Δεδομένων ή εξεύρεσης ειδικών χειριστών με εξειδίκευση την Ασφάλεια δεδομένων, ειδάλλως η όποια υπηρεσία βρίσκεται σε ρίσκο ασφαλείας. Κομμάτι της λύσης με σημαντική εξοικονόμηση πόρων και ενέργειας είναι η χρήση της Υπολογιστικής Σύννεφου (Cloud Computing). Η εν λόγω τεχνολογία έρχεται να δώσει λύση στις ανάγκες για βάσεις μεγάλων δεδομένων, μιας και απαιτούνται σημαντικά αυξημένες δυνατότητες και πόροι (π.χ. υπολογιστική ισχύ, αποθηκευτικό χώρο, cooling system χρεώσεις κ.ά.). Με αυτόν τον τρόπο ταυτόχρονα εξαλείφεται -θεωρητικώς- και η ανάγκη εξεύρεσης εξειδικευμένου προσωπικού των Σωμάτων Ασφαλείας στην Ασφάλεια Δεδομένων, αφού με μια απλή σύνδεση μπορούν να συνδεθούν οι υπηρεσίες όλες μαζί. Η συγκεκριμένη πρακτική δίνει τη δυνατότητα να συνδέονται χιλιάδες υπηρεσίες ταυτόχρονα ακόμη και όλες οι υπηρεσίες των Σωμάτων Ασφαλείας σε μια ενιαία βάση.

Η Υπολογιστική Νέφους (Cloud Computing/ CC) χρησιμοποιεί διάφορες υπηρεσίες, όπως λογισμικό ή διακομιστές μέσω του Διαδικτύου για αποθήκευση και διαχείριση δεδομένων (Hayes, 2008). Επιτρέπει σε έναν χρήστη να αποθηκεύει δεδομένα σε μια ιδιωτική τοποθεσία. Οι υπηρεσίες υπολογιστικού νέφους μπορούν να ταξινομηθούν ως Υποδομές ως Υπηρεσία (IaaS), Λογισμικό ως υπηρεσία (SaaS) και Πλατφόρμα ως Υπηρεσία (PaaS).

Στο πλαίσιο της έρευνας ζητήθηκε η συνδρομή ξένων Υπηρεσιών επιβολής του Νόμου, προκειμένου να μελετηθούν -κατά το δυνατόν- οι προτιμήσεις και προθέσεις

τους ως προς την μετάβασή τους στην τεχνολογία της Υπολογιστικής Νέφους. Οι εν λόγω ξένες Υπηρεσίες είναι οι εξής:

Α) Η Εθνική Υπηρεσία Καταπολέμησης Οργανωμένου Εγκλήματος του Ηνωμένου Βασιλείου (National Crime Agency/ NCA), με τη συνδρομή του Εθνικού Κέντρου Κυβερνοασφάλειας (National Cyber Security Centre/ NCSC)

Β) Η Ευρωπαϊκή Αστυνομία (EUROPOL) και

Γ) Ο Ευρωπαϊκός Οργανισμός Συνοριοφυλακής και Ακτοφυλακής- FRONTEX.

Εθνική Υπηρεσία καταπολέμησης Οργανωμένου Εγκλήματος του Η.Β. (National Crime Agency/ NCA):

Λόγω της ιδιαιτερότητας και της φύσης του θέματος δεν είναι σε θέση να δώσουν ακριβείς πληροφορίες σχετικά με τους παρόχους με τους οποίους συνεργάζονται ως προς το εν λόγω θέμα και τα επίπεδα ασφαλείας που έχουν στη χρήση της Υπολογιστικής Νέφους (CC). Η ομάδα ανάλυσης δεδομένων «Bulk Data Analysis» της NCA μας πληροφόρησε ότι είναι στην απαρχή της ενσωμάτωσης υπηρεσιών CC στην υποδομή όλης της Υπηρεσίας, ώστε να παρασχεθεί η πλήρης διαχείριση και εκμετάλλευση των Μεγάλων Δεδομένων οπουδήποτε χρειαστεί από στελέχη της παγκοσμίως. Η υποδομή που χρησιμοποιούν είναι ένα μικτό σύστημα προσέγγισης πολύ-πλατφόρμας δια μέσου πολλαπλών παρόχων, ώστε να επιτυγχάνεται η υποστήριξη διαφορετικών και ανά περίπτωση αναγκών της Υπηρεσίας τους. Με αυτό τον τρόπο επιτυγχάνουν διαφορετικά επίπεδα ταξινόμησης δεδομένων επωφελούμενοι των διαφορετικών παροχών από τους παρόχους. Οι Πλατφόρμες Νέφους (Cloud Platforms) προσφέρουν τα επιπλέον πλεονεκτήματα των Software as a Service- SaaS και Infrastructure as a Service- IaaS. Στο κομμάτι της ασφαλείας, ως κυβερνητικός οργανισμός, τα πρότυπα ασφαλείας τους κατευθύνονται από την Κυβέρνηση του Ηνωμένου Βασιλείου. Η χρήση του Cloud Computing από την Υπηρεσία αποτελεί βασικό στόχο παγκοσμίως, όμως -ακόμη- δεν έχει ολοκληρωθεί. Λόγω της ποικιλίας και της πολυπλοκότητας του έργου, των πολιτικών, των διαδικασιών και της νομιμότητας που εμπλέκονται στις δραστηριότητες της NCA, το Cloud Computing θα αποτελέσει ένα ολοένα αυξανόμενο τμήμα, αλλά δεν θα αποτελέσει την απάντηση σε όλες τις περιστάσεις.

EUROPOL:

Στην ίδια λογική με την NCA εργάζεται και η Europol η οποία είναι στη φάση ανάπτυξης και επέκτασης της υπηρεσίας του CC. Προς το παρόν, εργάζονται απομακρυσμένα μόνο σε ειδικές περιπτώσεις, μέσω mobile offices όπου κάθε στέλεχος έχει έναν μοναδικό κωδικό και μέσω VM's σε laptops, που αποκτούν πρόσβαση στα δεδομένα με δυνατότητα εισαγωγής δεδομένων αλλά χωρίς τη δυνατότητα επεξεργασίας των ήδη αποθηκευμένων.

FRONTEX:

Έπειτα από σχετική επικοινωνία με τον Ευρωπαϊκό Οργανισμό Συνοριοφυλακής και Ακτοφυλακής- FRONTEX, μας ενημέρωσαν ότι μελετάται από πλευράς τους επικείμενη μεταφορά μέρους της υποδομής τους σε τεχνολογία Cloud Computing και ως εκ τούτου το μοντέλο, η υπηρεσία και ο πάροχος που θα χρησιμοποιηθούν είναι υπό μελέτη. Παράλληλα, μας επεσήμαναν ότι η χρήσης της εν λόγω τεχνολογίας θα εναρμονιστεί με τους κανόνες της Ευρωπαϊκής Επιτροπής και τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων. Παρόλο που δεν έχει ολοκληρωθεί η τάση του συγκεκριμένου Οργανισμού σε τεχνολογία Cloud Computing, είναι αξιοσημείωτο το γεγονός ότι οδηγούνται στη χρήση του ως βέλτιστης και σημαίνουσας λύσης.

Παράλληλα από μελέτη ανοιχτών πηγών αλλά και από τα διδάγματα προσωπικής ενασχόλησης διαπιστώθηκαν τα κάτωθι ως προς τη χρήση της Υπολογιστικής Νέφους από την Ομοσπονδιακή Αστυνομία των Η.Π.Α. (Federal Bureau of Investigation/ FBI) αλλά και από τα Σώματα Ασφαλείας στην Ελλάδα. Ειδικότερα:

Ομοσπονδιακή Αστυνομία των Η.Π.Α (Federal Bureau of Investigation/ FBI):

Το FBI προέβη στην υιοθέτηση μιας νέας ασφαλούς, μεγάλης κλίμακας υπηρεσίας Cloud Computing (από το έτος 2018). Επιδίωξε να αποκτήσει πλατφόρμα-ως-υπηρεσίας και λογισμικό-ως-υπηρεσία "από έναν καθιερωμένο πάροχο υπηρεσιών cloud με μια υπάρχουσα, μεγάλης κλίμακας εμπορική προσφορά" με τη δυνατότητα παροχής υπηρεσιών για πολλές κυβερνητικές υπηρεσίες. Το FBI χρησιμοποιεί την εμπορική υπηρεσία cloud που υιοθετεί και πληροί απαιτήσεις για χειρισμό διαβαθμισμένων δεδομένων, καθώς και υποστήριξη μεγάλης διαχείρισης και επεξεργασίας δεδομένων. Εστιάζουν σε υπηρεσίες middleware, όπως διαχείριση ταυτότητας και ασφάλειας, log

analysis και δυνατότητες ελέγχου. Τουλάχιστον, οι προμηθευτές υποχρεούνται να διατηρούν τουλάχιστον δύο κέντρα δεδομένων που έχουν δεσμεύσει, τείχος προστασίας για κυβερνητική χρήση, εντός των συνόρων των ΗΠΑ και σε απόσταση 1.000 μιλίων, για να υποστηρίξουν περίπου 50.000 χρήστες ("FBI seeks information on IaaS and SaaS providers as cloud push gathers pace," n.d.).

ΕΛΛΑΔΑ:

Στην Ελλάδα, μέχρι την παρούσα χρονική στιγμή, δεν χρησιμοποιείται η τεχνολογία της Υπολογιστικής νέφους για τα Σώματα Ασφαλείας. Η υφιστάμενη λειτουργία είναι η ενσύρματη διασύνδεση μέσω δικτύου intranet- σύζευξης. Σημειώνεται ότι στη χώρα ακριβώς λόγω του προβληματισμού σε θέματα ασφαλείας των συστημάτων Cloud, οι Υπηρεσίες των Σ.Α. χρησιμοποιούν κατά κόρον intranet- σύζευξης όπου διασυνδέονται όλες οι Υπηρεσίας ενσύρματα και ταυτόχρονα. Από τα παραπάνω γίνεται κατανοητό ότι οι Υπηρεσίες Ασφάλειας ανά την Ε.Ε επιθυμούν τη χρήση του CC και εργάζονται πάνω στη υλοποίησή του. Λόγω ακριβώς προβληματισμού σχετικά με θέματα ασφάλειας, αποθήκευσης και διαχείρισης ιδιαίτερων δεδομένων, η υιοθέτηση της εν λόγω τεχνολογίας είναι σε αρχαϊκό στάδιο.

Αποτελεί κοινό τόπο και παραδοχή ότι αυτή ακριβώς η εξαιρετική τεχνολογική δυνατότητα της Υπολογιστικής Νέφους δίδει στα Σώματα Ασφαλείας τεράστια δυνατότητα αποθήκευσης και ασφάλειας δεδομένων.

Η ασφάλεια και η ιδιωτικότητα των Μεγάλων Δεδομένων (Big Data/ BD) μέσω της χρήσης της Υπολογιστικής Νέφους αποτελεί μια εξαιρετικά γρήγορα αναπτυσσόμενη τεχνολογία η οποία μπορεί να λειτουργήσει προς όφελος των Σωμάτων Ασφαλείας με την μετάβαση της λειτουργίας τους στην τεχνολογία νέφους. Μια ενδεχόμενη πρόταση- λύση στο κομμάτι της ιδιωτικότητας των δεδομένων στην Υπολογιστική νέφους είναι η δυνατότητα δημιουργίας μιας Βάσης Δεδομένων όπου τα συμμετέχοντα μέρη θα έχουν άμεση πρόσβαση στα στατιστικά στοιχεία των διαδράσεών τους (Stergiou et al., 2018), όπου θα δημιουργηθεί ένα νέο δίκτυο συστήματος-πλαισίου στο περιβάλλον νέφους που θα συνδυάζει τεχνολογίες και ορισμένες άλλες τεχνολογίες (π.χ. IoT).

Επιπρόσθετα, όσον αφορά την ασφάλεια των δεδομένων μέσω της χρήσης αλγορίθμων που μπορούν να παρέχουν περισσότερη ιδιωτικότητα στα δεδομένα που σχετίζονται με την τεχνολογία των Βάσεων Δεδομένων σε έναν διακομιστή νέφους,

καθώς και μέσω της διαδικασίας ελέγχου ταυτότητας (είσοδος) μέσω του λογαριασμού που θα κάνει κάθε χρήστης. Με αυτόν τον τρόπο, κάθε χρήστης θα δύναται να συνδεθεί σε ένα πιο ασφαλές «ιδιωτικό» δίκτυο μέσω του οποίου ο χρήστης μπορεί να ανταλλάσσει δεδομένα. Το εν λόγω «ιδιωτικό» δίκτυο που δημιουργήθηκε θα βασίζεται, από άποψη σχεδιασμού, αρχιτεκτονικής και τοπολογίας, στο Διαδίκτυο των Πραγμάτων (Stergiou et al., 2017).

Η εν λόγω τεχνολογία όμως έρχεται και συμπληρώνεται με την έλευση των δικτύων 5G των οποίων η χρήση -με την ταχύτητα και την χαμηλή καθυστέρηση που μας δίδουν- αποτελούν μονόδρομο στην επιλογή και χρήση τους από τις Υπηρεσίες Ασφαλείας της χώρας και αυτό διότι θα δίδεται η δυνατότητα άμεσης πρόσβασης και διαχείρισης σε μια μεγάλη και χρήσιμη βάση δεδομένων χωρίς την ανάγκη μετάβασης στο γραφείο.

6.2 Μη Επανδρωμένα Εναέρια Οχήματα (Drones).

Τα Μη Επανδρωμένα Εναέρια Οχήματα ή αλλιώς Drones αποτελούν ήδη ένα εξαιρετικά σημαντικό εργαλείο για τα Σώματα Ασφαλείας. Αυτό όμως θα κάνει την χρησιμότητά τους ακόμη πιο σημαντική από πλευράς Αρχών είναι η χρήση τους μέσω των δικτύων 5G με όλα τα οφέλη που παρέχουν τα εν λόγω δίκτυα και τα οποία έχουμε αναφέρει ενδελεχώς στην παρούσα εργασία. Από την άλλη πλευρά όμως θα πρέπει να επισημανθεί ότι όπως όλα τα πράγματα έχουν και άλλη όψη, έτσι και εδώ θεωρείται ότι η χρήση της συγκεκριμένης τεχνολογίας -δυνητικά- θα αποτελέσει εργαλείο για τυχόν έκνομες πράξεις.

Σε αυτό το σημείο αξίζει να σημειωθεί ότι η χρήση της συγκεκριμένης τεχνολογίας αποτελεί μια ευκαιρία για τα Σώματα Ασφαλείας, όμως θα πρέπει να λαμβάνουμε υπόψη μας και τις διακυμάνσεις του σήματος που τυχόν θα προκύπτουν κατά τη διάρκεια της χρήσης τους. Η μοντελοποίηση καναλιών ασύρματων επικοινωνιών για τα Μη Επανδρωμένα Εναέρια Οχήματα αποτελεί μια πρόκληση και για το λόγο αυτό πραγματοποιούνται διάφορες επιστημονικές μελέτες επί του θέματος. Συγκεκριμένα, σύμφωνα με τους συγγραφείς του άρθρου «*Artificial Neural Network Optimal Modelling and Optimization of UAV Measurements for Mobile Communications Using the L-SHADE Algorithm»* (Goudos et al., 2019b) πραγματοποιήθηκαν μετρήσεις

πειραματικών δεδομένων τα οποία ελήφθησαν από ένα τέτοιο εναέριο όχημα σε διαφορετικά υψόμετρα και εφαρμόζοντας διάφορους αλγορίθμους παρουσιάζοντας ένα τεχνητό νευρωνικό δίκτυο για την εκτίμηση της ισχύος σε ετερογενές κυψελοειδές περιβάλλον. Τα δεδομένα που ελήφθησαν οδήγησαν συμπερασματικά ότι ο αλγόριθμος L-SHADE αποτελεί την βέλτιστη επιλογή, έναντι άλλων αλγορίθμων, για την βελτίωση των ασύρματων επικοινωνιών.

Μια εξαιρετικά σημαντική συμβολή της της αξιοποίησης του συνδυασμού των τεχνολογιών των δικτύων 5G- Drone είναι κατά τη διαδικασία έρευνας αγνοουμένων τόσο σε χερσαίες εκτάσεις όσο και σε θαλάσσιες περιοχές. Με την αξιοποίηση της χαμηλής καθυστέρησης και του μεγάλου εύρος ζώνης που προσφέρουν τα δίκτυα 5G δύναται να τοποθετηθούν κάμερες υψηλής ευκρίνειας αλλά και κάμερες νυκτός και έτσι αδιάλειπτα να υπάρχει ζωντανή εικόνα μια επιτηρούμενης περιοχής.

Για την σημαίνουσα σημασία των Drones υπάρχουν πολλά παραδείγματα όπως αυτό της εξαφάνισης ενός εννιάχρονου κοριτσιού στις Η.Π.Α. όπου με τη χρήση Μη Επανδρωμένου Εναέριου Οχήματος η Αστυνομία κατάφερε να εντοπίσει το κορίτσι.

Επιπρόσθετα, με την κατάλληλη αξιοποίηση έτερων τεχνολογιών δύναται να χρησιμοποιηθούν για πυρόσβεση σε σημεία όπου δε θα υφίστατο δυνατότητα μετάβασης χερσαίων δυνάμεων αλλά και για αναγνώριση προσώπου και όλα αυτά σε πραγματικό χρόνο, με ασφάλεια και από απόσταση.

6.3 Γεωεντοποσμός.

Μέσω του μικρότερου εύρους κάλυψης της εμβέλειας των κεραιών των δικτύων 5G, το οποίο προσδιορίζεται περί τα πεντακόσια μέτρα (500m) (“How far does 5G reach?,” 2020b), δίδεται μια εξαιρετική ευκαιρία στα Σώματα Ασφαλείας εργαλειοποίησής τους. Συγκεκριμένα, σε περίπτωση έρευνας απαγωγών και αναζήτησης θυμάτων να εργαλειοποιείται αυτή ακριβώς η «αδυναμία» του μικρού εύρους κάλυψης κεραιών των δικτύων 5G, μέσω της βέλτιστης συγκεκριμενοποίησης των πιθανών σημείων και της ακτίνας εντός της οποίας πιθανόν να βρίσκονται τα θύματα, η οποία (ακτίνα) θα δίδεται από το σήμα που τυχόν θα εκπέμψει η συσκευή του κινητού τηλεφώνου. Παράλληλα γίνεται ευκολότερη και η εύρεση θυτών, μέσω της ίδιας διαδικασίας και της ίδιας τεχνολογίας.

6.4 Φορητό «Κιτ» λήψης δακτυλικών αποτυπωμάτων.

Είναι εξαιρετικά σύνηθες το φαινόμενο πολλές φορές να πραγματοποιούνται είτε προσαγωγές είτε συλλήψεις από τα στελέχη των Σωμάτων Ασφαλείας και να μη γνωρίζουν -μέχρι την εξακρίβωσή τους- με τι άτομα έχουν να κάνουν, πόσο επικίνδυνοι μπορεί να είναι (ή και να μην είναι), εάν διώκονται, εάν αφορά σε άτομα φυγόποινα ή φυγόδικα κ.ά. Η εξακρίβωση όλων αυτών πραγματοποιείται -μέχρι την παρούσα χρονική στιγμή- με έλεγχο στα γραφεία μιας Υπηρεσίας.

Η τεχνολογία των δικτύων 5G δύναται να επιτύχει μια ακόμη καινοτομία και ε αυτόν τον τομέα προς όφελος των Σωμάτων Ασφαλείας με τη δημιουργία και χρήση φορητών κιτ λήψης δακτυλικών αποτυπωμάτων, τα οποία θα μπορούν να πραγματοποιούνται σε εξωτερικούς χώρους, εντός του πεδίου, και άμεσα μέσω διασύνδεσης 5G να δίδεται πρόσβαση στη βάση δεδομένων των Αρχών.

6.5 Η κατανάλωση ενέργειας και η χρήση δικτύων 5G.

Σημαίνουσας σημασίας, πέραν όλων των αναφερομένων - πρακτικών εφαρμογών των δικτύων 5G, τυγχάνει και η κατανάλωση ενέργειας. Η ενέργεια και η κατανάλωση αυτής απασχολεί όλο το φάσμα της εφαρμογής και χρήσης των εν λόγω δικτύων, ενώ επιπρόσθετα αποτελεί και μια εξαιρετικά σημαντική παράμετρο η οποία θα πρέπει να απασχολεί όχι μόνο τους παρόχους τηλεπικοινωνιών αλλά και χρήστες, όπως τα Σώματα Ασφαλείας.

Σύμφωνα με τους συγγραφείς του άρθρου «A Novel Design Approach for 5G Massive MIMO and NB-IoT Green Networks Using a Hybrid Jaya-Differential Evolution Algorithm» (Goudos et al., 2019a) υφίσταται η δυνατότητα σχεδιασμού και μετάβασης σε «πράσινα δίκτυα». Ειδικότερα, υποστηρίζεται ότι σύμφωνα με μελέτες που πραγματοποίησαν, τα αποτελέσματα έδειξαν ότι τα 5G Massive MIMO δίκτυα απαιτούν, κατά προσέγγιση, πενήντα τοις εκατό (50%) λιγότερη κατανάλωση ενέργειας συγκριτικά με τα δίκτυα τέταρτης γενιάς (4G).

Η εν λόγω γενιά (5G) δικτύων, υποστηρίζεται από όλη την επιστημονική κοινότητα ότι δύναται να προσφέρει ένα εξαιρετικά ευρύ φάσμα και ρυθμό δεδομένων για τους χρήστες τους. Στο εν λόγω αναφερόμενο άρθρο εξετάζονται δύο τύποι προβλημάτων βελτιστοποίησης, αφενός το πρόβλημα του εύρους περιοχής κάλυψης και αφετέρου το πρόβλημα μέγιστης κάλυψης χρήστη. Στην πρώτη φάση, μελετήθηκε το

«πράσινο δίκτυο» από πλευράς βελτιστοποίησης ενός δικτύου, χωρίς να συνυπολογίζονται οι χρήστες του δικτύου, όπου υφίσταντο δύο στόχοι βελτιστοποίησης, από τη μια η ελαχιστοποίησης κατανάλωσης ενέργειας και από την άλλη η μέγιστη κάλυψη μιας περιοχής. Στη δεύτερη φάση μελετήθηκε το «πράσινο δίκτυο» από πλευράς μέγιστης κάλυψης χρηστών. Τέλος, έπειτα από συγκριτική μελέτη αποτελεσμάτων διαφόρων αλγορίθμων καταλήγουν στην πρόταση ενός υβριδικού αλγοριθμικού μοντέλου το οποίο πέτυχε τις καλύτερες επιδόσεις ως προς το θέμα τόσο της κατανάλωσης ενέργειας -ανάμεσα στα δυο δίκτυα- όσο και στο εύρος περιοχής κάλυψης και μέγιστης κάλυψης χρηστών.

7 Επίλογος

Το θέμα της παρούσης διπλωματικής εργασίας ήταν «***5G ΔΙΚΤΥΑ ΚΑΙ ΣΩΜΑΤΑ ΑΣΦΑΛΕΙΑΣ.*** *Η συνδρομή τους στην εξιχνίαση υποθέσεων των Αρχών Επιβολής του Νόμου*».

Επιχειρήθηκε μέσα από τα κεφάλαια η ανάλυση, όσο το δυνατόν καλύτερα αλλά και πληρέστερα, ενός θέματος το οποίο θεωρείται σημαίνουσας σημασίας για τον μελλοντικό τρόπο λειτουργίας των Σωμάτων Ασφαλείας σε ένα σύγχρονο τεχνολογικά περιβάλλον.

Σύμφωνα με έρευνα των πηγών, διαπιστώθηκε ότι μέχρι την παρούσα χρονική στιγμή το εν λόγο θέμα αποτελεί ένα επιστημονικό (και όχι μόνο) αντικείμενο το οποίο δεν έχει επαρκώς αναλυθεί. Θεωρείται ότι η μέγιστη αξιοποίηση της τεχνολογίας των δικτύων 5G δύναται να αποφέρει τεράστια οφέλη στην εξιχνίαση υποθέσεων από τα Σώματα Ασφαλείας και κατ' επέκταση και για την ίδια την κοινωνία.

Οι θεματικές που επιλέχθηκα να αναλυθούν μέσω των κεφαλαίων ήταν αρχικώς να προβούμε σε μια σύντομη περιγραφή των δικτύων 5G και της διαφοροποίησής τους από τα δίκτυα 4G, έτσι ώστε να δίδεται η δυνατότητα να αντιληφθεί ακόμη και ένας μη ειδικός αναγνώστης επί του θέματος, την τεχνολογική πρόοδο που έχει επιτευχθεί από τη μετάβασή μας από τα 4G στα 5G δίκτυα επικοινωνίας.

Εν συνεχεία επιχειρήθηκε μια ουσιαστικότερη εισαγωγή στα δίκτυα 5G και στο επίπεδο της τεχνολογίας που έχει αναπτυχθεί. Ακολούθως, εξετάστηκε το επίπεδο και ο τύπος κρυπτογράφησης των δικτύων 4G- 5G με μια συγκριτική αναφορά μεταξύ τους, ενώ, έπειτα πραγματοποιήθηκε αναφορά και στην ασφάλεια που παρέχεται από τα εν λόγω δικτύων.

Το μεγαλύτερο και ουσιαστικότερο, κατά την κρίση μας, μέρος της εργασίας ήταν σχετικά με τη διαδικασία της άρσης απορρήτου των επικοινωνιών -εν γένει- και της διαδικασίας της νόμιμη καταγραφή δεδομένων των χρηστών των δικτύων 5G. Ειδικότερα, πραγματοποιήθηκε μια λεπτομερής αναφορά της αρχιτεκτονικής και της τεχνολογίας που αναπτύχθηκε και εφαρμόζεται σχετικά με το πως πραγματοποιείται η καταγραφή δεδομένων και ακολούθως πως δύναται να λαμβάνουν σε επεξεργάσιμη μορφή τα δεδομένα αυτά τα στελέχη των Σωμάτων Ασφαλείας και ακολούθως να τα αναλύουν.

Τέλος, αναφέρθηκαν συγκεκριμένες προτάσεις σχετικά με την πρακτική εφαρμογή των δικτύων 5G και σε άλλους τομείς που δύναται να αξιοποιηθούν από τα Σώματα Ασφαλείας, οι οποίες σε συνδυασμό με συγγενείς τους τεχνολογικές εφαρμογές δύναται να έχουν άμεσης αποτελεσματικότητας στην εξιχνίαση εγκλημάτων από τα Σώματα Ασφαλείας.

7.1 Σύνοψη και συμπεράσματα

Συμπερασματικά, καταλήγουμε ότι τα οφέλη και τα πλεονεκτήματα που δύναται η νέα αυτή τεχνολογία των δικτύων 5G να επιφέρει ως «σύμμαχος» στον τρόπο λειτουργίας της σύγχρονης κοινωνίας είναι πολλά. Παράλληλα, δε θα πρέπει να λησμονούμε και τις προκλήσεις που δημιουργούνται από τη χρήση τους, καθώς και τις αυξανόμενες ανησυχίες για την ασφάλεια λόγω της ραγδαίας αύξησης της χρήσης συσκευών του Διαδικτύου των Πραγμάτων (IoTs).

Παραδείγματος χάριν, οι πελάτες κινητής τηλεφωνίας θα απολαμβάνουν μεγαλύτερη διάρκεια ζωής της μπαταρίας καθώς θα χρειάζεται να έχει πρόσβαση στο δίκτυο μόνο περιοδικά. Οι κυβερνήσεις που σχεδιάζουν πρωτοβουλίες για έξυπνες πόλεις θα είναι πλέον σε θέση να ξεκινήσουν την απαραίτητη υποδομή για να ξεκινήσουν την επανάσταση της «έξυπνης πόλης». Οι ταχύτητες δεδομένων 5G θα επιτρέψουν την αποτελεσματική χρήση αισθητήρων και παρακολούθησης βίντεο που είναι θεμελιώδη δεδομένα για την υποστήριξη της κινητής υγειονομικής περίθαλψης και της τηλεϊατρικής.

Όσον αφορά το προσωπικό των Σωμάτων Ασφαλείας, θεωρείται δεδομένο ότι μέσω της χρήσης των δικτύων 5G θα απολαμβάνουν ταχύτερη απόδοση σε πραγματικό χρόνο, όπως η αναγνώριση προσώπου και η σάρωση πινακίδων κυκλοφορίας, καθώς η ακρίβειά τους ενισχύεται με υψηλότερο όριο δεδομένων. Η χαμηλή καθυστέρηση και η ταχύτερη απόδοση από εφαρμογές κρίσιμες θα δώσει τη δυνατότητα ψηφιακής αυτονομίας, καθώς μπορούν να περνούν περισσότερο χρόνο στο πεδίο και λιγότερο στο γραφείο, αφ ης στιγμής θα έχουν τη δυνατότητα να προβαίνουν σε οποιαδήποτε ενέργεια χρειάζονταν παλιότερα από τον σταθερό υπολογιστή της Υπηρεσίας τους, τώρα θα γίνεται από τις κινητές συσκευές.

Από την άλλη πλευρά, πέραν όλων των θετικών από τη χρήση των δικτύων 5G που αναλύθηκαν, διαπιστώθηκε ότι υφίστανται -ακόμη- σοβαρά θέματα σε κάποιες λειτουργίες, όπως το γεγονός ότι οι Υπηρεσίες Επιβολής του Νόμου βασίζονται σε μοναδικά αναγνωριστικά που σχετίζονται με κινητές συσκευές και αναλόγως λαμβάνουν πληροφορίες σχετικά με τον χρήστη- στόχο, όπως δεδομένα βάσει της τοποθεσίας του. Το 5G όμως, αντικαθιστά το μόνιμο αναγνωριστικό με ένα που είναι προσωρινό και το οποίο καταστρέφεται μετά τη δημιουργία σύνδεσης με έναν πύργο κινητής τηλεφωνίας. Το γεγονός αυτό αποτελεί αναμφισβήτητα μια πρόκληση στο κομμάτι της ταυτοποίησης ενός χρήστη- στόχου με μια κινητή συσκευή, καθώς η σχέση μεταξύ ενός χρήστη κινητής τηλεφωνίας και ενός πύργου κινητής τηλεφωνίας θα μπορούσε να γίνει ασαφής.

Το 5G επίσης περιπλέκει τη συλλογή και την παρακολούθηση ψηφιακών αποδεικτικών στοιχείων. Μέχρι σήμερα, οι κινητές συσκευές μεταφέρουν δεδομένα μέσω ενός μόνο σημείου, όπως το Wi-Fi ή ο πύργος δικτύου κινητής τηλεφωνίας. Το 5G επιτρέπει σε μια συσκευή να λαμβάνει δεδομένα τόσο από έναν πύργο δικτύου όσο και από εναλλακτικά μέσα, όπως η σύνδεση σε ένα hotspot Wi-Fi, δορυφόρο ή ISP. Αυτό σημαίνει ότι οι Αρχές θα πρέπει να ενώσουν τα ψηφιακά ίχνη των υπόπτων ή των θυμάτων χρησιμοποιώντας πολλαπλές πηγές δεδομένων και αρχεία καταγραφής. Έτσι, η σημασία μιας ψηφιακής λύσης που μπορεί να ενσωματώσει ανόμοια αρχεία καταγραφής δεδομένων και μέσα σε ένα χρονοδιάγραμμα είναι ζωτικής σημασίας για να αποφευχθεί η μη αυτόματη αντιστοίχιση δεδομένων και μορφών.

Παράλληλα όμως μας δίνει δυνατότητες οι οποίες είναι εξαιρετικά χρήσιμες στις Αρχές Επιβολής του Νόμου και συγκεκριμένα στα Σώματα Ασφαλείας όπως η απομακρυσμένη λειτουργία drones σε περιπτώσεις αναζήτησης ή επιχείρησης διάσωσης ατόμων, η απομακρυσμένη και αδιάλειπτη επιτήρηση στόχων, ο εντοπισμός τυχόν θυμάτων απαγωγής (κάτι το οποίο επιτυγχάνεται λόγω της μικρότερης εμβέλειας των δικτύων 5G, άρα και της καλύτερης συγκεκριμενοποίησης του στίγματος γεωεντοπισμού τυχόν κινητών τηλεφώνων).

Βιβλιογραφία

3GPP - LTE [WWW Document], 2008. URL https://web.archive.org/web/20081207052302/http://www.3gpp.org/article/lte (accessed 4.26.22).

5G Mobile Communications, 2021. Lawful Interception Architecture in 5G.

5G-Research_A4.pdf, n.d.

About 3GPP Home [WWW Document], n.d. URL https://www.3gpp.org/about-3gpp/about-3gpp (accessed 2.23.22).

Adebusola, J., Ariyo, A., Okeyinka, A., Olubunmi, A., Okesola, O., 2020. An Overview of 5G Technology. https://doi.org/10.1109/ICMCECS47690.2020.240853

Al-Turjman, F., Ever, E., Zahmatkesh, H., 2019. Small Cells in the Forthcoming 5G/IoT: Traffic Modelling and Deployment Overview. IEEE Commun. Surv. Tutor. 21, 28–65. https://doi.org/10.1109/COMST.2018.2864779

Andrade, M.P. de, 2021. Security aspects related to 5G networks | Valid Mobile Solutions. Valid. URL https://valid.com/blog-5g-network-security-aspects/ (accessed 1.26.22).

Andrés, S.B., 2020. Glossary:Long-Term Evolution (LTE) [WWW Document]. CROS - Eur. Comm. URL https://ec.europa.eu/eurostat/cros/content/Glossary%3ALong-Term_Evolution_%28LTE%29_en (accessed 4.26.22).

Barb, G., Otesteanu, M., 2020. 4G/5G: A Comparative Study and Overview on What to Expect from 5G, in: 2020 43rd International Conference on Telecommunications and Signal Processing (TSP). Presented at the 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), pp. 37–40. https://doi.org/10.1109/TSP49548.2020.9163402

Bastos, L., Capela, G., Koprulu, A., Elzinga, G., 2021. Potential of 5G technologies for military application, in: 2021 International Conference on Military Communication and Information Systems (ICMCIS). Presented at the 2021 International Conference on Military Communication and Information Systems (ICMCIS), pp. 1–8. https://doi.org/10.1109/ICMCIS52405.2021.9486402

Cao, J., Ma, M., Li, H., Ma, R., Sun, Y., Yu, P., Xiong, L., 2020. A Survey on Security Aspects for 3GPP 5G Networks. IEEE Commun. Surv. Tutor. 22, 170–195. https://doi.org/10.1109/COMST.2019.2951818

Computer Networks - A Tanenbaum - 5th edition.pdf [WWW Document], n.d. URL https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxza21pbmh8Z3g6NjQxMTI2MmYxMTAwZmNjZQ (accessed 3.27.22).

Dahiya, M., 2017. Need and Advantages of 5G wireless Communication Systems. Int. J. Adv. Res. Comput. Sci. Manag. Stud. 5, 48–51.

Dutta, A., Hammad, E., 2020. 5G Security Challenges and Opportunities: A System Approach, in: 2020 IEEE 3rd 5G World Forum (5GWF). Presented at the 2020 IEEE 3rd 5G World Forum (5GWF), pp. 109–114. https://doi.org/10.1109/5GWF49715.2020.9221122

Elmasry, G.F., 2020. DSA and 5G Adaptation to Military Communications, in: Dynamic Spectrum Access Decisions: Local, Distributed, Centralized, and Hybrid Designs. Presented at the Dynamic Spectrum Access Decisions: Local, Distributed, Centralized, and Hybrid Designs, IEEE, pp. 117–126. https://doi.org/10.1002/9781119573784.ch7

ETSI - Welcome to the World of Standards! [WWW Document], n.d. URL https://www.etsi.org/ (accessed 4.28.22a).
ETSI - Welcome to the World of Standards! [WWW Document], n.d. URL https://www.etsi.org/ (accessed 2.16.22b).
European Vision for the 6G Network Ecosystem ‹ 5G-PPP, n.d. URL https://5g-ppp.eu/european-vision-for-the-6g-network-ecosystem/ (accessed 1.26.22).
Eye on Tech, 2019. What is 5G? Everything You Need to Know About 5G.
FBI seeks information on IaaS and SaaS providers as cloud push gathers pace [WWW Document], n.d. . ComputerWeekly.com. URL https://www.computerweekly.com/news/252435449/FBI-seeks-information-on-IaaS-and-SaaS-providers-as-cloud-push-gathers-pace (accessed 5.12.22).
Ferrag, M.A., Maglaras, L., Argyriou, A., Kosmanos, D., Janicke, H., 2018. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. J. Netw. Comput. Appl. 101, 55–82. https://doi.org/10.1016/j.jnca.2017.10.017
Ghosh, A., Maeder, A., Baker, M., Chandramouli, D., 2019. 5G Evolution: A View on 5G Cellular Technology Beyond 3GPP Release 15. IEEE Access 7, 127639–127651. https://doi.org/10.1109/ACCESS.2019.2939938
Goudos, S.K., Deruyck, M., Plets, D., Martens, L., Psannis, K.E., Sarigiannidis, P., Joseph, W., 2019a. A Novel Design Approach for 5G Massive MIMO and NB-IoT Green Networks Using a Hybrid Jaya-Differential Evolution Algorithm. IEEE Access 7, 105687–105700. https://doi.org/10.1109/ACCESS.2019.2932042
Goudos, S.K., Tsoulos, G.V., Athanasiadou, G., Batistatos, M.C., Zarbouti, D., Psannis, K.E., 2019b. Artificial Neural Network Optimal Modeling and Optimization of UAV Measurements for Mobile Communications Using the L-SHADE Algorithm. IEEE Trans. Antennas Propag. 67, 4022–4031. https://doi.org/10.1109/TAP.2019.2905665
Hayes, B., 2008. Cloud computing. Commun. ACM 51, 9–11. https://doi.org/10.1145/1364782.1364786
How far does 5G reach? [WWW Document], 2020a. URL https://www.verizon.com/about/news/how-far-does-5g-reach (accessed 4.26.22).
How far does 5G reach? [WWW Document], 2020b. URL https://www.verizon.com/about/news/how-far-does-5g-reach (accessed 5.12.22).
Humayun, M., Hamid, B., Jhanjhi, N.Z., Suseendran, G., Talib, M.N., 2021. 5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey. J. Phys. Conf. Ser. 1979, 012037. https://doi.org/10.1088/1742-6596/1979/1/012037
Idrissi, Y.E.H.E., Zahid, N., Jedra, M., 2012. Security analysis of 3GPP (LTE) — WLAN interworking and a new local authentication method based on EAP-AKA. First Int. Conf. Future Gener. Commun. Technol. https://doi.org/10.1109/FGCT.2012.6476561
Introducing the Internet Protocol Suite (System Administration Guide, Volume 3) [WWW Document], n.d. URL https://docs.oracle.com/cd/E19455-01/806-0916/6ja85398m/index.html (accessed 3.21.22).
ITU global standard for international mobile telecommunications ´IMT-Advanced´ [WWW Document], n.d. URL https://www.itu.int/net/ITU-R/information/promotion/e-flash/2/article4.html (accessed 4.26.22).
Kennedy, D., 2019. How 5G networks are being built in the real world 10.

Lawful Intercept (LI) in 5G System - Techplayon - 5G Network Architectures [WWW Document], n.d. URL https://www.techplayon.com/lawful-intercept-li-in-5g-system/ (accessed 1.26.22).
Lawful Interception Addressing the Complex of 5G and MIoT - Utimaco [WWW Document], n.d. URL https://utimaco.com/lawful-interception-addressing-complex-5g-and-miot (accessed 1.26.22).
Lawful Interception in the Digital Age - Utimaco [WWW Document], n.d. URL https://utimaco.com/lawful-interception-digital-age (accessed 1.26.22).
LIMA Lawful Interception - Cost Efficient - Group 2000 [WWW Document], n.d. URL https://group2000.com/lima-lawful-intercept/ (accessed 1.26.22).
LIMA Mediator [WWW Document], n.d. . Group 2000. URL https://group2000.com/lima-mediator/ (accessed 1.26.22).
Liu, S., Liu, L., Yang, H., Yue, K., Guo, T., 2020. Research on 5G technology based on Internet of things, in: 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC). Presented at the 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), pp. 1821–1823. https://doi.org/10.1109/ITOEC49072.2020.9141671
Liyanage, M., Gurtov, A., 2012. Secured VPN Models for LTE Backhaul Networks, in: 2012 IEEE Vehicular Technology Conference (VTC Fall). Presented at the 2012 IEEE Vehicular Technology Conference (VTC Fall), pp. 1–5. https://doi.org/10.1109/VTCFall.2012.6399037
Liyanage, M., Ylianttila, M., Gurtov, A., 2013. A Case Study on Security Issues in LTE Backhaul and Core Networks, in: Case Studies in Secure Computing: Achievements and Trends. https://doi.org/10.1201/b17352-10
Mensah, I.K., Xiao, Z., Lu, M., 2020. Understanding the impact of 5G mobile technology on the development and diffusion of mobile government services, in: Proceedings of the 2nd Africa-Asia Dialogue Network (AADN) International Conference on Advances in Business Management and Electronic Commerce Research, AADNIC-ABMECR '20. Association for Computing Machinery, New York, NY, USA, pp. 1–9. https://doi.org/10.1145/3440094.3440388
Monshizadeh, M., Khatri, V., Varfan, M., Kantola, R., 2018. LiaaS: Lawful Interception as a Service. https://doi.org/10.23919/SOFTCOM.2018.8555753
Mpirical, 2019. What is 5G Core Network Architecture? Take a Look With Mpircial.
NAS [WWW Document], n.d. URL https://www.3gpp.org/technologies/keywords-acronyms/96-nas (accessed 5.16.22).
Piqueras Jover, R., Marojevic, V., 2019. Security and Protocol Exploit Analysis of the 5G Specifications. IEEE Access 7, 24956–24963. https://doi.org/10.1109/ACCESS.2019.2899254
Professional cybersecurity solutions [WWW Document], n.d. URL https://utimaco.com/ (accessed 1.26.22).
Publications [WWW Document], n.d. URL https://portal.etsi.org/Portal_Pub/APNProcPub.asp?ACTION_TYPE_NB=PU&FROM_DD=24&FROM_MM=Jul&FROM_YYYY=2017&TO_DD=30&TO_MM=Jul&TO_YYYY=2017&REAL_FROM_DD=24&REAL_FROM_MM=Jul&REAL_FROM_YYYY=2017&REAL_TO_DD=30&REAL_TO_MM=Jul&REAL_TO_YYYY=2017 (accessed 1.26.22).
Rommer, S., Hedman, P., Olsson, M., Frid, L., Sultana, S., Mulligan, C., 2020. Chapter 8 - Security, in: Rommer, S., Hedman, P., Olsson, M., Frid, L., Sultana, S.,

Mulligan, C. (Eds.), 5G Core Networks. Academic Press, pp. 171–201. https://doi.org/10.1016/B978-0-08-103009-7.00008-9
Sharevski, F., 2018. Towards 5G cellular network forensics. EURASIP J. Inf. Secur. 2018, 8. https://doi.org/10.1186/s13635-018-0078-7
Sicari, S., Rizzardi, A., Coen-Porisini, A., 2020. 5G In the internet of things era: An overview on security and privacy challenges. Comput. Netw. 179, 107345. https://doi.org/10.1016/j.comnet.2020.107345
Specification # 23.228 [WWW Document], n.d. URL https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=821 (accessed 5.22.22).
SS8: Network Intelligence Solutions [WWW Document], n.d. . SS8. URL https://ss8.com/ (accessed 3.14.22).
Stergiou, C., Psannis, K.E., Plageras, A.P., Kokkonis, G., Ishibashi, Y., 2017. Architecture for security monitoring in IoT environments, in: 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE). Presented at the 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), pp. 1382–1385. https://doi.org/10.1109/ISIE.2017.8001447
Stergiou, C., Psannis, K.E., Xifilidis, T., Plageras, A.P., Gupta, B.B., 2018. Security and privacy of big data for social networking services in cloud, in: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Presented at the IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 438–443. https://doi.org/10.1109/INFCOMW.2018.8406831
Sullivan, S., Brighente, A., Kumar, S.A.P., Conti, M., 2021. 5G Security Challenges and Solutions: A Review by OSI Layers. IEEE Access 9, 116294–116314. https://doi.org/10.1109/ACCESS.2021.3105396
Wayback Machine [WWW Document], 2016. URL https://web.archive.org/web/20160304150203/http://ece.ut.ac.ir/Classpages/F84/PrincipleofNetworkDesign/Papers/CK74.pdf (accessed 3.21.22).
What is a Radio Access Network (RAN)? [WWW Document], n.d. . SearchNetworking. URL https://www.techtarget.com/searchnetworking/definition/radio-access-network-RAN (accessed 4.26.22).
Whitepaper on security in 5G RAN and core deployment [WWW Document], 2019. URL https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments (accessed 5.12.22).
Yang, J., Johansson, T., 2020. An overview of cryptographic primitives for possible use in 5G and beyond. Sci. China Inf. Sci. 63, 220301. https://doi.org/10.1007/s11432-019-2907-4
Zou, Y., Zhu, J., Wang, X., Hanzo, L., 2016. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. Proc. IEEE 104, 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521
Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών [WWW Document], 2021. URL http://www.adae.gr/ (accessed 1.26.22).