ΣΧΟΛΗ ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Ηλεκτρόνιο

Τεύχος 3

Εφαρμογές Οπτικών Επικοινωνιών σε Εναέρια και χερσαία Αυτόματα Οχήματα

Η εξέλιξη του Πολέμου
Η Τεχνολογία των UAVs
στις Σύγχρονες Στρατιωτικές Επιχειρήσεις

Στρατιωτικές Εφαρμογές Επαυξημένης Πραγματικότητας

Πλευρική Κίνηση: Τεχνικές, Μεθοδολογίες και Βέλτιστες Πρακτικές Άμυνας

Τεχνικές και εργαλεία επιχειρηματικής ευφυΐας στο Πυροσβεστικό Σώμα

ΣΧΟΛΗ ΠΡΟΓΡΑΜΜΑΤΙΣΤΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΣΤΡΑΤΟΠΕΔΟ ΖΟΡΜΠΑ
Μεγάλου Αλεξάνδρου, Ζωγράφου

ΕΚΔΟΤΗΣ
ΤΜΗΜΑ ΜΕΛΕΤΩΝ ΣΠΗΥ

ΕΠΙΜΕΛΕΙΑ ΣΥΝΤΑΞΗΣ
Σχης (ΠΛΗ) Δημήτριος Ντόντος
Ανχης(ΠΛΗ) Αντώνιος Ηλιάκης
Υπχος(Ε) Ασημάκης Κυπριώτης
Ανθστης (ΠΛΗ) Αναστάσιος Σιούτης

ΠΕΡΙΕΧΟΜΕΝΑ

Χαιρετισμός Διοικητού ΣΠΗΥ
Σημείωμα Σύνταξης
Άρθρα
Εφαρμογές Οπτικών Επικοινωνιών σε Εναέρια και χερσαία Αυτόματα Οχήματα

Η εξέλιξη του Πολέμου: Η Τεχνολογία των UAVs στις Σύγχρονες Στρατιωτικές Επιχειρήσεις

Στρατιωτικές Εφαρμογές Επαυξημένης Πραγματικότητας

Πλευρική Κίνηση: Τεχνικές, Μεθοδολογίες και Βέλτιστες Πρακτικές Άμυνας

Τεχνικές και εργαλεία επιχειρηματικής ευφυΐας στο Πυροσβεστικό Σώμα

Δραστηριότητες ΣΠΗΥ

ΧΑΙΡΕΤΙΣΜΟΣ ΔΙΟΙΚΗΤΟΥ ΣΠΗΥ

Αγαπητοί Αναγνώστες

Το περιοδικό «Ηλεκτρόνιο» κλείνει ένα χρόνο ζωής ως φορέας επικοινωνίας της Σχολής Προγραμματιστών Ηλεκτρονικών Υπολογιστών με την κοινότητα της Πληροφορικής. Σε αυτή τη χρονική περίοδο η Σχολή, παρακολουθώντας τις εξελίξεις στην τεχνολογία, προσαρμόζεται στις νέες απαιτήσεις που αυτές θέτουν για την αποδοτική τεχνική εκπαίδευση. Στο πλαίσιο αυτό και συμμεριζόμενοι την άποψη ότι η τεχνολογία δεν είναι απλώς ένα εργαλείο αλλά ένας τρόπος σκέψης, δημιουργίας και καινοτομίας, επιδίωξη μας είναι οι σελίδες κάθε τεύχους του περιοδικού να αποτελούν δημιουργικές επεκτάσεις της εκπαίδευσης.

Η τεχνητή νοημοσύνη, η διαχείριση του κυβερνοχώρου, ο προγραμματισμός βρίσκουν νέες εφαρμογές τόσο στην άμυνα όσο και στην καθημερινότητά των ανθρώπων. Πίσω από τις εξελίξεις βρίσκεται η ανθρώπινη δημιουργικότητα και το πάθος για καινοτομία. Σκοπός των αρθρογράφων και της ομάδας σύνταξης του περιοδικού είναι να τα διατηρήσουν και να τα ενισχύσουν ώστε να προσφέρουν έγκυρη πληροφόρηση, έμπνευση και εργαλεία για την αξιοποίηση των δυνατοτήτων της πληροφορικής.

Επιδίωξη της έκδοσης του περιοδικού είναι να εμπνέουμε για εξερεύνηση των δυνατοτήτων και των προκλήσεων που συνδέονται με τις τεχνολογίες πληροφορικής, συμβάλλοντας στην αναβάθμιση των δυνατοτήτων των Ενόπλων Δυνάμεων.

Με εκτίμηση

Δημήτριος Ντόντος
Συνταγματάρχης (ΠΛΗ)

ΣΗΜΕΙΩΜΑ ΕΚΔΟΣΗΣ

Αγαπητοί Αναγνώστες,

Το τρίτο τεύχος του περιοδικού εστιάζει σε έναν τομέα που βρίσκεται στην αιχμή της τεχνολογικής καινοτομίας: τις εφαρμογές πληροφορικής στον αμυντικό και στρατιωτικό χώρο. Έχουν επιλεγεί άρθρα που καλύπτουν θέματα αιχμής:

- Εφαρμογές Οπτικών Επικοινωνιών σε Εναέρια και Χερσαία Αυτόματα Οχήματα, όπου αναλύεται η τεχνολογία που επιτρέπει την αποτελεσματική επικοινωνία σε σύγχρονα αυτόνομα συστήματα.
- Η Εξέλιξη του Πολέμου: Η Τεχνολογία των UAVs στις Σύγχρονες Στρατιωτικές Επιχειρήσεις, ένα άρθρο που εξετάζει τον κομβικό ρόλο των μη επανδρωμένων αεροσκαφών στη στρατιωτική στρατηγική.
- Στρατιωτικές Εφαρμογές Επαυξημένης Πραγματικότητας, που μας εισάγει σε έναν νέο τρόπο αντιμετώπισης επιχειρησιακών προκλήσεων μέσα από την τεχνολογία της επαυξημένης πραγματικότητας.
- Πλευρική Κίνηση: Τεχνικές, Μεθοδολογίες και Βέλτιστες Πρακτικές Άμυνας, μια ανάλυση για τις σύγχρονες προκλήσεις και τις καλύτερες πρακτικές στον τομέα της ασφάλειας.
- Τεχνικές και εργαλεία επιχειρηματικής ευφυΐας στο Πυροσβεστικό Σώμα

Με το παρόν τεύχος, φιλοδοξούμε να αναδείξουμε την πολυδιάστατη συμβολή της πληροφορικής στις στρατιωτικές εφαρμογές και να προκαλέσουμε έναν γόνιμο προβληματισμό για το πώς η τεχνολογία μπορεί να χρησιμοποιηθεί υπεύθυνα και αποτελεσματικά.

Τέλος είναι αξιοσημείωτο ότι μεγάλο μέρος της ύλης του παρόντος τεύχους έχει εκπονηθεί από σπουδαστές του Τμήματος Αναλυτών – Προγραμματιστών της Σχολής.

Καλή ανάγνωση

Με εκτίμηση

Η ομάδα σύνταξης

Εφαρμογές Οπτικών Επικοινωνιών σε Εναέρια και χερσαία Αυτόματα Οχήματα

Δημήτριος Μπουζιώτας
Ανδρέας Τζορμπατζόγλου

Εισαγωγή

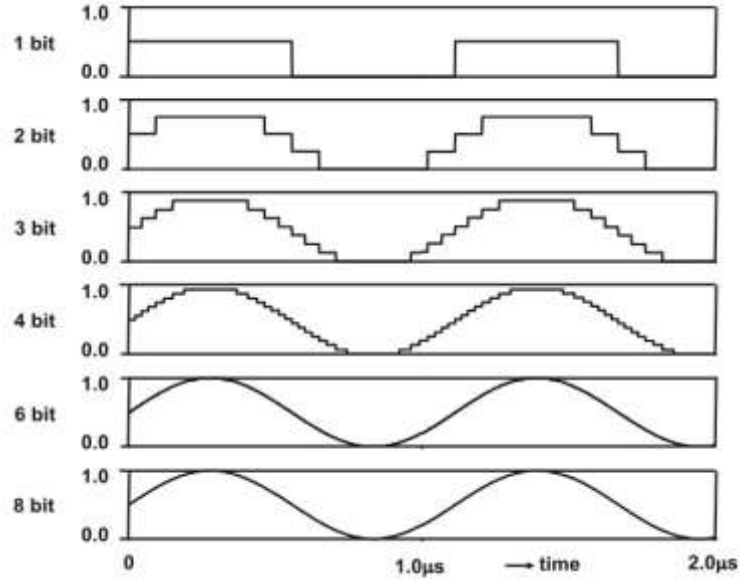
Οι σύγχρονες τεχνολογίες οπτικών επικοινωνιών, που χρησιμοποιούνται ευρέως σε συστήματα αυτόνομης οδήγησης, περιλαμβάνουν αισθητήρες και κάμερες. Ο κύριος στόχος αυτών των συσκευών είναι η συλλογή και επεξεργασία οπτικών σημάτων, τα οποία μετατρέπονται σε ψηφιακά δεδομένα για περαιτέρω επεξεργασία από υπολογιστικά συστήματα. Αυτές οι συσκευές ενσωματώνουν τεχνολογίες όπως αισθητήρες ανίχνευσης αποστάσεων, θερμικές κάμερες, αισθητήρες φωτός και συστήματα RTK (Real-Time Kinematics). Οι εν λόγω τεχνολογίες συμβάλλουν στην ακριβή ανίχνευση και καταγραφή δεδομένων σε πραγματικό χρόνο, ενισχύοντας την αποτελεσματικότητα και την ασφάλεια των οχημάτων. Επιπλέον, η ενσωμάτωσή τους με την τεχνητή νοημοσύνη επιτρέπει την προηγμένη ανάλυση δεδομένων και την αυτοματοποίηση λειτουργιών, προσφέροντας καινοτόμες δυνατότητες στον τομέα της αυτονομίας και της έξυπνης οδήγησης.

ΤΕΧΝΟΛΟΓΙΕΣ ΟΠΤΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Το Επεξεργάσιμο Σήμα

Πολλές συσκευές με αισθητήρες επεξεργάζονται οπτικά ή αλλιώς αναλογικά σήματα, τα οποία κωδικοποιούνται με τέτοιο τρόπο ώστε να γίνονται αναγνωρίσιμα από έναν υπολογιστή. Αυτή η διαδικασία ονομάζεται κβαντισμός [1-3] και έχει ως στόχο τη μετατροπή του αναλογικού σήματος σε ψηφιακό. Ωστόσο, η διαδικασία αυτή μπορεί συχνά να μειώσει την ανάλυση και τη λεπτομέρεια των δεδομένων που μπορούν να εξαχθούν από ένα αναλογικό σύστημα, οδηγώντας σε απώλειες στο ψηφιακό σήμα. Παρά τις απώλειες, ο κβαντισμός παραμένει μια αποτελεσματική μέθοδος μετατροπής σήματος για πολλές εφαρμογές ώστε να μειωθεί ο θόρυβος που μπορεί να εμφανιστεί στο αναλογικό σήμα (Σχήμα 1).

Παρόμοιες τεχνικές αξιοποιούνται και για την μετατροπή του ψηφιακού σήματος σε αναλογικό, αυτή η τεχνική ονομάζεται Interpolation [4]. Ένα σύστημα δέχεται στην είσοδο και επεξεργάζεται το ψηφιακό σήμα παράγοντας στην έξοδο ένα αναλογικό/οπτικό σήμα.

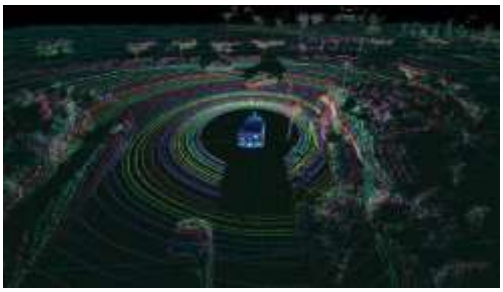
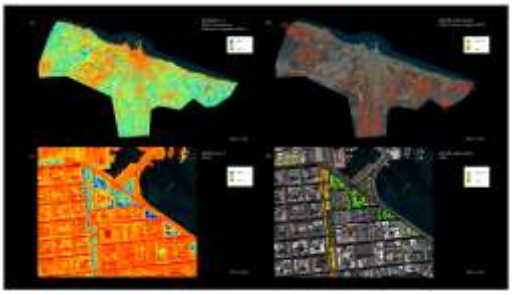


Σχήμα 1: Κβαντισμός ενός αναλογικού σήματος με διαφορετικά βάθη bit. Η κάθε κυματομορφή παρουσιάζει το ίδιο σήμα κβαντοποιημένο με αυξανόμενη ανάλυση στα bits, απεικονίζοντας τη βελτίωση λεπτομέρειας του ψηφιακού σήματος με βάση το αρχικό σήμα (900Khz). [1].

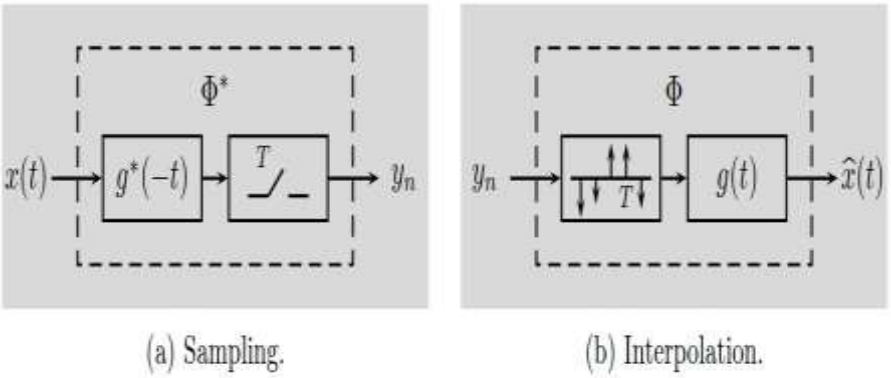
LiDAR (Light Detection and Ranging) τεχνολογία [5]

Η LiDAR τεχνολογία λειτουργεί με την χρήση συσκευών οι οποίες εκπέμπουν οπτικά σήματα μικρού μήκους κυμάτων περίπου 903nm-905nm (σχεδόν infrared), τα οποία διαδίδονται με τη ταχύτητα του φωτός (3 × 108 m/s). Οι ακτίνες που εκπέμπονται από τη συσκευή κατηγοριοποιούνται σε δύο κατηγορίες: Law Pulse Repetition Frequencies (PRFs) και High Pulse Repetition Frequencies (PRFs). Τυπικά, οι αισθητήρες με χαμηλή συχνότητα επανάληψης παλμών (Low PRFs) εκπέμπουν από 10 kHz έως 100 kHz, ενώ οι αισθητήρες με υψηλή συχνότητα επανάληψης (High PRFs) εκπέμπουν από 100 kHz έως 2 MHz. Αυτό σημαίνει ότι ένας αισθητήρας LiDAR με συχνότητα επανάληψης 2 MHz έχει τη δυνατότητα να παράγει έως και 2 εκατομμύρια 3D Point Clouds ανά δευτερόλεπτο. Οι ακτίνες αυτές ανιχνεύονται από έναν αισθητήρα ανίχνευσης φωτός, και το οπτικό σήμα μετατρέπεται σε ψηφιακή μορφή, δημιουργώντας τρισδιάστατα Point Clouds. Με αυτόν τον τρόπο, η απόσταση υπολογίζεται με υψηλή ακρίβεια, βασισμένη στον χρόνο που χρειάζεται το σήμα για να φτάσει στην επιφάνεια και να επιστρέψει στον αισθητήρα.

Στο σχήμα 4 παρουσιάζονται δύο είδη LiDAR συσκευών. Το πρώτο σχήμα δείχνει ένα ωφέλιμο φορτίο LiDAR αισθητήρα για drones της DJI. Το Σχήμα 4b, παρουσιάζει μια συσκευή η οποία αναπτύχθηκε ειδικά για την χαρτογράφηση μέσω δορυφόρων. Παρόμοιες συσκευές αξιοποιούνται και σε αυτόνομα οχήματα για την ανίχνευση αντικειμένων ή εμποδίων ή την χαρτογράφηση ορισμένων δεδομένων όπως φυλλώματα και βλάστηση σε αστικές περιοχές (Σχήμα 2b).

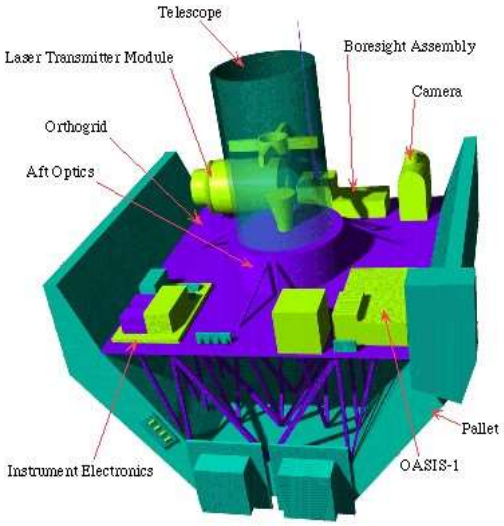
Σχήμα 2: Παραδείγματα LiDAR τεχνολογίας τα οποία αξιοποιούνται σε σύγχρονα αυτόνομα συστήματα δορυφόρων ή αυτοκινούμενων αυτοκινήτων.



Σχήςα 3: Interpolation & Sampling (Quantization)

RTK (Real-Time Kinematic) τεχνολογία [10]

Η τεχνολογία RTK χρησιμοποιείται για την ανάκτηση των GPS συντεταγμένων ενός κινούμενου αντικειμένου, όπως drones, αυτόνομα οχήματα ή γεωργικά μηχανήματα. Το σχήμα 6, απεικονίζει ένα σχήμα ενός συστήματος GNSS-RTK. Ο συνδυασμός της ονομασίας GNSS-RTK (Global Navigation Satellite System - Real-Time Kinematic), αναφέρει το είδος της τεχνολογίας η οποία αξιοποιείται ώστε να βρεθούν οι ακριβείς συντεταγμένες μιας συσκευής. Ενδεικτικά, η τεχνολογία “GNSS” χωρίς να συμπεριλάβουμε το “RTK” είναι ένα σύστημα το οποίο η συσκευή επικοινωνεί αποκλειστικά το ελάχιστο με τέσσερις δορυφορικούς σταθμούς όπως απεικονίζεται στο Σχήμα 6. Από την άλλη, η RTK τεχνολογία, η οποία συχνά αναφέρεται και ως GNSS-RTK, ώστε να τονίσει ότι βασίζεται σε δορυφορικές επικοινωνίες, εκτός της χρήσης τεσσάρων δορυφορικών σταθμών, συμπεριλαμβάνει και τον κοντινότερο σταθμό βάσης, με σκοπό την βελτίωση της ακρίβειας των συντεταγμένων με την χρήση DPGPS (Differential GPS). Η ακρίβεια της GNSS τεχνολογίας, προσφέρει ακρίβεια 3 - 10 μέτρα. Η τεχνολογία GNSS-RTK, προσφέρει υψηλή ακρίβεια με απόκλιση έως και εκατοστά .



(a) DJI Zenmuse L2 LiDAR Drone Payload. [6]

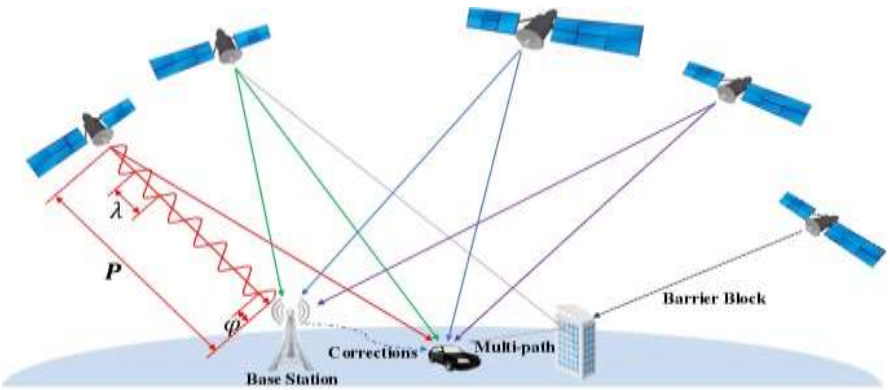
(b) LiDAR συσκευή για δορυφόρους. [7]

Σχήμα 4: LiDAR συσκευασίες Drone και δορυφόρων

(a) Ανίχνευση και ανάλυση συμπεριφοράς άγριας πανίδας του Αμβρακικού Κόλπου.

(b) Ανίχνευση οχημάτων και λωρίδων δρόμου [9]

Σχήμα 5: Παραδείγματα ενσωμάτωσης εξειδικευμένων μοντέλων τεχνητής νοημοσύνης σε οπτικές κάμερες drone ή οχημάτων



Σχήμα 6: Σύστημα που βασίζεται σε GNSS-RTK

Τεχνολογία Οπτικών Καμερών (RGB)

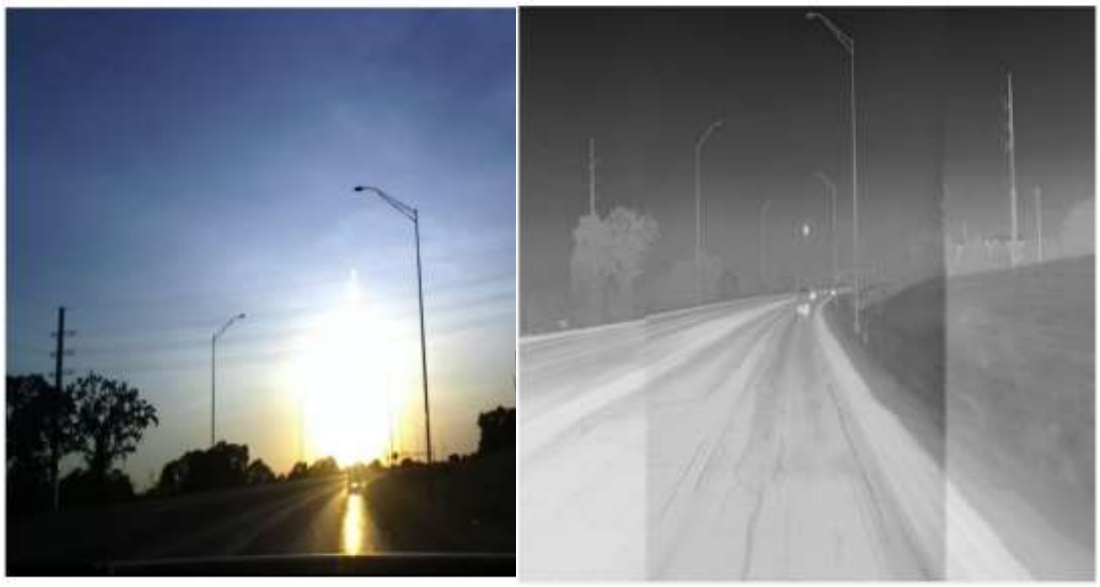
Ο σκοπός των οπτικών καμερών σε αυτόνομα οχήματα ή drones είναι η φωτογράφηση και βιντεοσκόπηση του περιβάλλοντος, ώστε οι εικόνες ή τα βίντεο που συλλέγονται να επεξεργαστούν με την χρήση συνελικτικών νευρωνικών δικτύων. Οι οπτικές κάμερες αποτελούνται από αισθητήρες ειδικά για ηλεκτρομαγνητικές συχνότητες συγκεκριμένα για το ορατό φως. Αξιοποιούνται για τη συλλογή φωτογραφιών ή βίντεο, τα οποία κβαντοποιούν και μετατρέπουν το οπτικό σήμα (αναλογικό) σε ψηφιακό με την χρήση CMOS (Complementary Metal-Oxide-Semiconductor) ή CCD [11]. Το ορατό φάσμα για τον άνθρωπο έχει ως μήκος κύματος από 4×10^{-7} έως 7×10^{-7} μέτρα και εύρος συχνοτήτων από 7.5×10^{14} έως 4.3×10^{14} Hz, ξεκινώντας από το μπλε έως το κόκκινο χρώμα. Αφού κβαντοποιηθεί το αναλογικό σήμα, μετατρέπεται σε ψηφιακή εικόνα, επεξεργάσιμη από υπολογιστή. Οι ψηφιακές εικόνες περιέχουν συνήθως τρία διαφορετικά κανάλια, με το κάθε κανάλι να παριστάνει ένα χρώμα, πχ οι χρωματικοί χώροι *RGB* (R: Red, B: Blue, G: Green), *CIELAB ή αλλιώς L*a*b* (L: Lightness, a: red/green, b: blue/yellow coordinates).

Τα συνελικτικά νευρωνικά δίκτυα έχουν την ικανότητα να εξάγουν στοιχεία από εικόνες και να αναγνωρίζουν σημαντικά πρότυπα από τα οποία έχουν εκπαιδευτεί να εντοπίζουν. Δύο έρευνες συνδυάζουν την τεχνητή νοημοσύνη με τελευταίας τεχνολογίας εμπορικά UAVs (Unmanned Aerial Vehicles) εξοπλισμένα με υψηλής ανάλυσης οπτικές κάμερες, για την αυτόματη παρακολούθηση της άγριας πανίδας του Αμβρακικού κόλπου [12], [13]. Το σχήμα 5a εμφανίζει τα αποτελέσματα ενός έξυπνου συστήματος μηχανικής όρασης, το οποίο αξιοποιεί πολυφασματικό drone εξοπλισμένο με οπτική και θερμική κάμερα, με σκοπό την ανίχνευση και αξιολόγηση της συμπεριφοράς της ορνιθοπανίδας του Αμβρακικού. Μια άλλη έρευνα συνδυάζει τα συνελικτικά νευρωνικά δίκτυα με βίντεο από οπτικές κάμερες, με σκοπό την ανίχνευση και παρακολούθηση οχημάτων και λωρίδων δρόμου για την οδήγηση αυτόνομων οχημάτων [9] (Σχήμα 5b).

Τεχνολογία Υπέρυθρων Καμερών

Οι υπέρυθρες κάμερες λειτουργούν παρόμοια με τις οπτικές κάμερες, αλλά είναι σχεδιασμένες για να ανιχνεύουν αποκλειστικά υπέρυθρες ακτίνες του ηλεκτρομαγνητικού φάσματος. Στην πράξη, το κάθε σώμα παράγει μια ποσότητα υπέρυθρης ακτινοβολίας το οποίο μετέπειτα μεταφράζεται ως η θερμοκρασία ενός αντικειμένου. Αυτή η τεχνολογία μπορεί να αξιοποιηθεί με σκοπό την ανίχνευση βιολογικών μορφών ζωής όπως και τον εντοπισμό βιολογικών εμποδίων όπως πεζοί ή ζώα. Οι υπέρυθρες κάμερες έχουν την ικανότητα να φιλτράρουν την φωτεινότητα που παράγει ο ήλιος σε σύγκριση με τις οπτικές κάμερες. Αυτό αποδεικνύεται αρκετά αποτελεσματικό για τον εντοπισμό αντικειμένων σε δύσκολες συνθήκες φωτισμού, συγκεκριμένα για την ανίχνευση αντικειμένων σε καταστάσεις χαμηλής/υψηλής φωτεινότητας (Σχήμα 7). Η αριστερή εικόνα απεικονίζει το πρόβλημα δύσκολων

συνθηκών υψηλής φωτεινότητας λόγω του ήλιου, δυσκολεύοντας την εξαγωγή σημαντικών χαρακτηριστικών από RGB εικόνες, όπως την ανίχνευση οχημάτων ή ανθρώπων. Από την άλλη, η δεξιά εικόνα απεικονίζει την θερμική, η οποία σχηματίζεται αποκλειστικά από την υπέρυθρη ακτινοβολία των σωμάτων του κάθε αντικειμένου.



a) Οπτική εικόνα (RGB) με υποβάθμιση από το ηλιακό φως. [14]

(b) Θερμική εικόνα (Infrared) με καλύτερη (λεπτομέρεια. [14]

Σχήμα 7: Παράδειγμα δύο εικόνων, RGB και θερμική εικόνα.

ΑΝΑΛΥΣΗ ΕΦΑΡΜΟΓΩΝ ΟΠΤΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ ΣΕ ΑΥΤΟΝΟΜΑ ΟΧΗΜΑΤΑ ΚΑΙ ΣΥΣΤΗΜΑΤΑ

Τεχνολογίες Αυτόνομων Χερσαίων Οχημάτων

Οι εφαρμογές οπτικών επικοινωνιών σε χερσαία αυτόνομα οχήματα, με την ραγδαία ανάπτυξη της τεχνολογίας, επιφυλάσσουν νέες προοπτικές με στόχο την αύξηση της ασφάλειας και τη μείωση του κόστους μετακίνησης. Επιπλέον έχει εμφανιστεί εκθετική αύξηση τα τελευταία χρόνια στην εμπορική κυκλοφορία αυτόνομων οχημάτων συγκεκριμένα σε ηλεκτρικά ή υβριδικά αυτόνομα οχήματα.

Τα αυτόνομα οχήματα συνδυάζουν προηγμένες τεχνολογίες βασισμένες στις οπτικές επικοινωνίες για την επίτευξη υψηλής ακρίβειας στην ανίχνευση αντικειμένων και την αποφυγή εμποδίων. Παράλληλα, χρησιμοποιούν τεχνολογίες όπως το RTK (Real-Time Kinematics) και το V2X (Vehicle-to-Everything) [15]. Η τεχνολογία RTK, σε συνδυασμό με το V2X, αποτελεί τη βάση για έξυπνα συστήματα πλοήγησης σε πραγματικό χρόνο, τα οποία αξιοποιούνται για την ανίχνευση μποτιλιαρίσματος, την

αυτόματη οδήγηση, τη σχεδίαση και τη βελτιστοποίηση διαδρομών, μεταξύ άλλων εφαρμογών.

Εφαρμογές και βιβλιογραφία: Η τεχνολογία RTK επιτρέπει στα αυτόνομα οχήματα να προσδιορίζουν με εξαιρετική ακρίβεια τη θέση τους σε συστήματα πλοήγησης. Αυτή η υψηλή ακρίβεια είναι κρίσιμη για την ασφαλή οδήγηση σε σύνθετα κυκλοφοριακά δίκτυα με μεγάλη ροή κίνησης, συμβάλλοντας στη μείωση του κινδύνου ατυχημάτων. Με τον συνδυασμό της τεχνολογίας V2X (Vehicle-to-Everything), τα οχήματα μπορούν να επικοινωνούν μεταξύ τους, ανταλλάσσοντας πληροφορίες σχετικά με την ροή κυκλοφορίας δρόμων, συμβάλλοντας στην μείωση ατυχημάτων. Ωστόσο, οι συσκευές που είναι εξοπλισμένες με αυτές τις τεχνολογίες συχνά βασίζονται σε εξωτερικές πηγές, όπως δορυφόρους ή σταθμούς βάσης, για να εξασφαλίσουν την επικοινωνία με άλλες συσκευές, παρέχοντας υψηλή ακρίβεια και αξιοπιστία. Επιπλέον, με τη μετάφραση του οπτικού σήματος σε ψηφιακή μορφή, ο χρόνος αντίδρασης των συσκευών μπορεί να αυξηθεί, επηρεάζοντας και την απόδοση τους σε εφαρμογές που απαιτούν άμεση επεξεργασία δεδομένων. Για την αντιμετώπιση αυτού του ζητήματος, τα αυτόνομα οχήματα είναι εξοπλισμένα με κάμερες και τεχνολογίες επεξεργασίας δεδομένων σε πραγματικό χρόνο, που τους επιτρέπουν να λαμβάνουν και να επεξεργάζονται πληροφορίες άμεσα.

Σήμερα, πολλές εταιρείες αξιοποιούν και συνδυάζουν τεχνολογίες αισθητήρων, οπτικές κάμερες και συστήματα LIDAR με σκοπό την αποφυγή εμποδίων σε πραγματικό χρόνο. Τα συστήματα αυτά συλλέγουν δεδομένα οπτικής φύσης, αλλά από μόνα τους δεν έχουν τη δυνατότητα να ανιχνεύουν εμπόδια με ακρίβεια. Για τον λόγο αυτό, συνδυάζονται με σύγχρονα μοντέλα τεχνητής νοημοσύνης που επεξεργάζονται τα δεδομένα που λαμβάνουν. Όπως αναφέρεται στο σχήμα 5, ειδικά στις εφαρμογές οπτικών καμερών, αυτό επιτυγχάνεται με τη χρήση μοντέλων ανίχνευσης αντικειμένων, όπως το YOLO (You Only Look Once) [16]. Επιπλέον, για την τρισδιάστατη ανίχνευση αντικειμένων, αξιοποιούνται δεδομένα από αισθητήρες LIDAR, ενισχύοντας την ακρίβεια και την αποδοτικότητα των συστημάτων [17] (Σχήμα 8).

Τεχνολογίες Αυτόνομων Εναέριων Οχημάτων

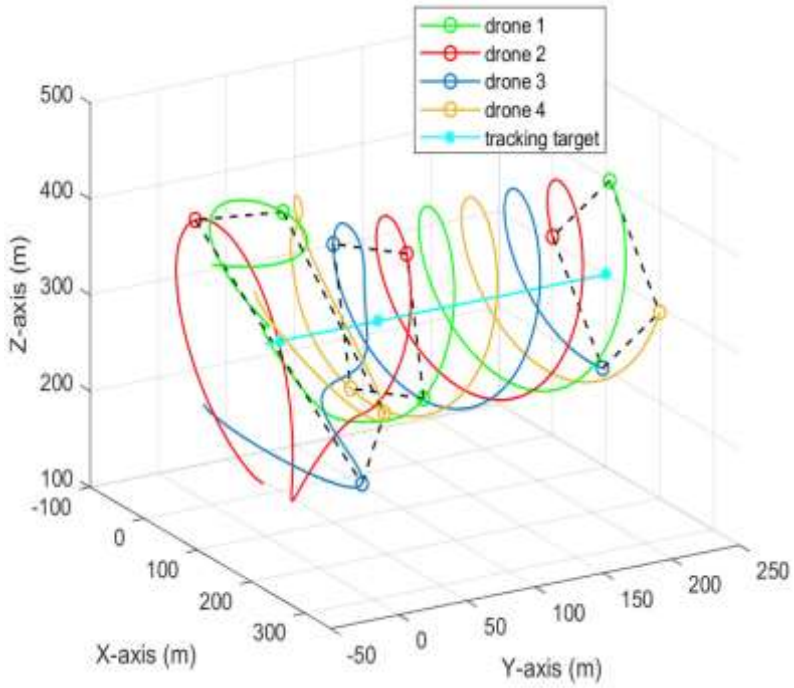
Τα αυτόνομα εναέρια οχήματα ή αλλιώς UAV (Unmanned Aerial Vehicles) όπως και τα χερσαία, τα τελευταία χρόνια παρουσίασαν απότομη αύξηση στην χρήση τους σε διάφορους τομείς, όπως τεχνικές γεωπονίας, χαρτογράφησης δεδομένων, γεωεντοπισμού, μεταφορά φορτίου και άλλα.

- Κεντρικές Τεχνολογίες*:* ΄Οπως και τα χερσαία οχήματα, τα εναέρια είναι εξοπλισμένα με διάφορες παρόμοιες τεχνολογίες αισθητήρων. Η LIDAR τεχνολογία αξιοποιείται και στα UAVs με σκοπό την χαρτογράφηση γεωγραφικών περιγραμμάτων σε μεγάλα υψόμετρα (Σχήμα 2b), ανίχνευση και αποφυγή εμποδίων κτλ. Με τον ίδιο τρόπο, τα UAV αξιοποιούν τεχνολογίες όπως το RTK και το V2X, οι οποίες χρησιμοποιούνται συχνά για τον

συγχρονισμό πολλαπλών drones, επιτρέποντας την επικοινωνία μεταξύ τους και τον ακριβή εντοπισμό της τοποθεσίας τους. Με αυτόν τον τρόπο επιτυγχάνεται και η υλοποίηση σχηματισμών για επιδείξεις drone swarm [19].

Σχήμα 8: Ανίχνευση Αντικειμένων με την χρήση LIDAR τεχνολογία. [18]

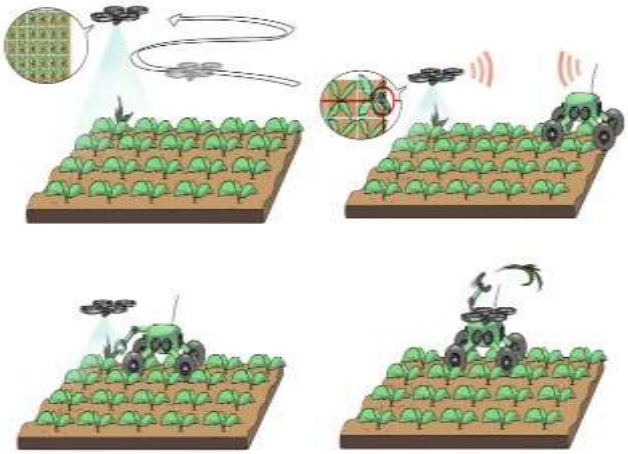
- Εφαρμογές και βιβλιογραφία: Μια ερευνητική ομάδα ανέπτυξε ένα έξυπνο σύστημα αυτόματης οδήγησης μέσα σε τούνελ, χρησιμοποιώντας drone [20].



Σχήμα 9: Σχηματισμός drone που πραγματοποιούν ελικοειδή κίνηση

Σχήμα 10: Οπτική προοπτική ενός αυτόνομου drone που πλοηγείται μέσα σε ένα τούνελ. [20]

Στην έρευνα αυτή αξιοποιούνται τεχνικές επεξεργασίας εικόνας με τεχνικές monocular depth estimation [21] για την παραγωγή χάρτη αποστάσεων, καθώς και τρισδιάστατες κινηματικές (3D kinematics) για την αυτόματη πλοήγηση του drone. Το Σχήμα 10 παρουσιάζει την οπτική προοπτική του drone κατά την πλοήγησή του στο τούνελ, μέσω της χρήσης τεχνικών επεξεργασίας εικόνας.
Μια άλλη έρευνα αξιοποιεί πολυφασματικά UAVs με σκοπό την χαρτογράφηση χωραφιών όπως και την αφαίρεση αγριόχορτων με την άμεση ενημέρωση χερσαίων αυτόνομων αγροτικών οχημάτων αφού έχει είδη ανιχνευθεί [22]. Η έρευνα αυτή συνδυάζει τελευταίας τεχνολογίας πολυφασματικά drone και τεχνικές μηχανικής όρασης, πιο συγκεκριμένα Semantic Segmentation [23], με σκοπό την αξιολόγηση υγείας βλάστησης χωραφιών. Το σχήμα 11 διευκρινίζει το σχέδιο που ακολουθεί το αυτοματοποιημένο σύστημα.



Σχήμα 11: Εναέριο-χερσαίο ρομποτικό σύστημα με την αξιοποίηση πολυφασματικού drone για την ακρίβεια καλλιέργειας

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΟΠΤΙΚΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ ΣΕ ΑΥΤΟΝΟΜΑ ΟΧΗΜΑΤΑ

Οι οπτικές επικοινωνίες προσφέρουν μια σειρά από πλεονεκτήματα για τα αυτόνομα οχήματα, τόσο για τα χερσαία όσο και για τα εναέρια. Συγκεκριμένα, τεχνολογίες όπως το LIDAR και το RTK αξιοποιούνται για την ακριβή χαρτογράφηση και τη γεωεντοπιστική παρακολούθηση αντικειμένων, με την ψηφιακή επεξεργασία τους από υπολογιστές. Επιπλέον, συστήματα ανίχνευσης εμποδίων που βασίζονται σε αισθητήρες, καθώς και κάμερες οπτικού ή υπέρυθρου φάσματος, ενισχύουν τις δυνατότητες πλοήγησης και αποφυγής κινδύνων.

Πολλές από τις τεχνολογίες οπτικών επικοινωνιών επιτρέπουν τη συλλογή πληθώρας δεδομένων, όπως και την αποθήκευση τους. Τα πλεονεκτήματα αυτών των συσκευών παρατίθενται παρακάτω:

- Η αξιοποίηση οπτικών συσκευών, όπως κάμερες ευαίσθητες σε μήκη κύματος μη ορατά από το ανθρώπινο μάτι (π.χ. υπέρυθρες ακτίνες, ακτίνες γάμα, υπεριώδεις ακτίνες κ.λπ.), ενισχύει τη συνολική πληροφορία που μπορεί να εξαχθεί, ειδικά για τα αυτόνομα οχήματα. Για παράδειγμα, οι θερμικές κάμερες επιτρέπουν τον εντοπισμό βιολογικών μορφών ζωής, δυνατότητα που δεν διαθέτουν οι οπτικές κάμερες ευαίσθητες μόνο στο ορατό φως.
- Η μετάδοση σημάτων με υψηλές ταχύτητες (ταχύτητα φωτός: 3 × 108m/s) επιτρέπει την άμεση επικοινωνία μεταξύ πολλών συσκευών ή οχημάτων με ελάχιστη καθυστέρηση. Αυτή η δυνατότητα είναι κρίσιμη για εφαρμογές όπου απαιτείται ταχεία ανταλλαγή δεδομένων σε μεγάλες αποστάσεις σε πραγματικό χρόνο, όπως στα αυτόνομα συστήματα οδήγησης και στις δικτυωμένες υποδομές μεταφορών.
- Η χαμηλή καθυστέρηση στις οπτικές τηλεπικοινωνίες αποτελεί σημαντικό πλεονέκτημα. Η καθυστέρηση εξαρτάται κυρίως από την απόδοση των κυκλωμάτων και των υπολογιστικών συστημάτων που υποστηρίζουν τη μετάδοση και επεξεργασία των δεδομένων. Η βελτίωση αυτών των υποδομών είναι κρίσιμη για την ελαχιστοποίηση της καθυστέρησης και την επίτευξη ταχύτερης και αποδοτικότερης επικοινωνίας.

Ο συνδυασμός αυτών των τεχνολογιών με την τεχνητή νοημοσύνη επιτρέπει την αυτοματοποίηση πολλών διαδικασιών στα αυτόνομα οχήματα. Μέχρι σήμερα, η τεχνητή νοημοσύνη, σε συνδυασμό με τις οπτικές τεχνολογίες στα αυτόνομα οχήματα, ιδίως στον τομέα της χερσαίας οδήγησης, έχει συμβάλει σε σημαντικές βελτιώσεις στις συνθήκες κυκλοφορίας. Αυτές οι βελτιώσεις περιλαμβάνουν:

- Μείωση ατυχημάτων μέσω της αξιοποίησης συστημάτων αυτόματου φρεναρίσματος και αισθητήρων ανίχνευσης εμποδίων, τα οποία συχνά διαθέτουν μικρό χρόνο καθυστέρησης για άμεση αντίδραση.
- Βελτίωση της ροής κυκλοφορίας, ιδιαίτερα σε έξυπνες πόλεις (Smart Cities), με τη χρήση προηγμένων τεχνολογιών διαχείρισης της κυκλοφορίας.
- Ελάττωση του χρόνου μετακίνησης μεταξύ δύο τοποθεσιών, μέσω αλγορίθμων βελτιστοποίησης διαδρομών.
- Αυτόματη οδήγηση για μεγάλες αποστάσεις, προσφέροντας άνεση και αποτελεσματικότητα στους χρήστες.

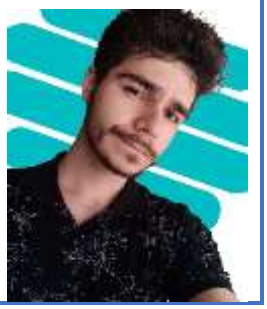
- Μείωση περιβαλλοντικών επιπτώσεων, ειδικά για ηλεκτρικά ή υβριδικά αυτόνομα οχήματα, με τη βελτιστοποίηση της ενεργειακής κατανάλωσης και της εκπομπής ρύπων.

Αναφορές

1. M. J. M. Pelgrom, *Quantization*. Cham: Springer International Publishing, 2022, pp. 425–470.
2. M. Hirz and B. Walzel, “Sensor and object recognition technologies for self-driving cars,” *Computer-Aided Design and Applications*, vol. 15, pp. 1–8, 01 2018.
3. X. Li, W. Y. Chen, G. Sanesi, and R. Lafortezza, “Remote sensing in urban forestry: Recent applications and future directions,” *Remote Sensing*, vol. 11, no. 10, 2019.
4. M. Vetterli, J. Kova˘cevi´c, and V. K. Goyal, *Foundations of Signal Processing*. Cambridge University Press, 2014.
5. S. Islam, M. S. Tanvir, M. R. Habib, T. T. Shawmee, M. A. Ahmed, T. Ferdous, M. R. Arefin, and S. Alam, “Autonomous driving vehicle system using lidar sensor,” in *Intelligent Data Communication Technologies and Internet of Things*, D. J. Hemanth, D. Pelusi, and C. Vuppalapati, Eds. Singapore: Springer Nature Singapore, 2022, pp. 345–358.
6. DJI Enterprise, “Zenmuse l
7. eoPortal Directory, “Lidar – laser imaging, detection, and ranging,” (Accessed on 26th of October, 2024). [Online]. Available: https://www.eoportal.org/ other-space-activities/lidar#topographiclidar
8. D. Mpouziotas, P. Karvelis, and C. Stylios, “A multimodal computer vision approach for wildlife bird surveillance using drones,” in *2024 9th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, 2024, pp. 63–68.
9. W. Farag and Z. Saleh, “An advanced vehicle detection and tracking scheme for self-driving cars,” in *2nd Smart Cities Symposium (SCS 2019)*, 2019, pp. 1–6.
10. Swift Navigation, “Moving baseline: Centimeter-accurate positioning for dynamic platforms,” 2017, (Accessed on 27th of October, 2024) Citation Generated by ChatGPT
11. R. Gounella, G. M. Ferreira, M. L. M. Amorim, J. N. Soares, and J. P. Carmo, “A review of optical sensors in cmos,” *Electronics*, vol. 13, no. 4, 2024.
12. D. Mpouziotas, P. Karvelis, I. Tsoulos, and C. Stylios, “Automated wildlife bird detection from drone footage using computer vision techniques,” *Applied Sciences*, vol. 13, no. 13, 2023.
13. D. Mpouziotas, P. Karvelis, and C. Stylios, “Advanced computer vision methods for tracking wild birds from drone footage,” *Drones*, vol. 8, no. 6, 2024.
14. Bhadoriya, V. Vegamoor, and S. Rathinam, “Vehicle detection and tracking using thermal cameras in adverse visibility conditions,” Sensors (Basel), vol. 22, no. 12, p. 4567, Jun. 2022, published 2022 Jun 17.
15. T. Huang, J. Liu, X. Zhou, D. C. Nguyen, M. R. Azghadi, Y. Xia, Q.-L. Han, and S. Sun, “V2x cooperative perception for autonomous driving: Recent advances and challenges,” *ArXiv*, vol. abs/2310.03525, 2023.
16. J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, “You only look once: Unified, real-time object detection,” in *2016 IEEE* Conference on Computer Vision and Pattern Recognition (CVPR). IEEE, 2016, pp. 779–788.
17. Q.-H. Pham, P. Sevestre, R. S. Pahwa, H. Zhan, C. H. Pang, Y. Chen, A. Mustafa, V. R. Chandrasekhar, and J. Lin, “A*3d dataset: Towards autonomous driving in challenging environments,” *2020 IEEE International Conference on Robotics and Automation (ICRA)*, pp. 2267–2273, 2019.
18. N. Ahmed, A. Anwar, S. Eckelmann, T. Trautmann, S. Latr´e, and P. Hellinckx, “Lane marking detection techniques for autonomous driving,” in *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*, L. Barolli, Ed. Cham: Springer International Publishing, 2022, pp. 217–226.
19. H. Gao, A. Zhang, W. Li, and H. Cai, “Drone swarm robust cooperative formation pursuit through relative positioning in a location denial environment,” *Drones*, vol. 8, no. 9, 2024.
20. C. Kanellakis, P. S. Karvelis, S. S. Mansouri, A.-A. AghaMohammadi, and G. Nikolakopoulos, “Towards autonomous aerial scouting using multi-rotors in subterranean tunnel navigation,” *IEEE Access*, vol. 9, pp. 66 477–66 485, 2021.
21. C. Zhao, Q. Sun, C. Zhang, Y. Tang, and F. Qian, “Monocular depth estimation based on deep learning: An overview,” *Science China Technological Sciences*, vol. 63, pp. 1612 – 1627, 2020.
22. A. Pretto, S. Aravecchia, W. Burgard, N. Chebrolu, C. Dornhege, T. Falck, F. Fleckenstein, A. Fontenla, M. Imperoli, R. Khanna, F. Liebisch, P. Lottes, A. Milioto, D. Nardi, S. Nardi, J. Pfeifer, M. Popovi´c, C. Potena, C. Pradalier, E. Rothacker-Feder, I. Sa, A. Schaefer, R. Siegwart, C. Stachniss, A. Walter, W. Winterhalter, X. Wu, and J. Nieto, “Building an aerial–ground robotics system for precision farming: An adaptable solution,” *IEEE Robotics & Automation Magazine*, vol. 28, no. 3, pp. 29–49, 2021.
23. G. Csurka, R. Volpi, and B. Chidlovskii, “Semantic image segmentation: Two decades of research,” *Found. Trends Comput. Graph. Vis.*, vol. 14, pp. 1–162, 2023.

Βιογραφικό συντακτών

Ο Τσορμπατζόγλου Ανδρέας έλαβε το Πτυχίο Φυσικής και το Μεταπτυχιακό στη «Φυσική Υλικών» από το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης. Η διδακτορική του διατριβή πραγματοποιήθηκε υπό συνεπίβλεψη του ΑΠΘ και του Institut National Polytechnique de Grenoble με θέμα: “Χαρακτηρισμός και ανάπτυξη μοντέλων τρανζίστορ MOSFET πολλαπλών πυλών νανοδιαστάσεων”. Από το 2021 είναι Επίκουρος Καθηγητής στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Ιωαννίνων, με γνωστικό αντικείμενο "Μη γραμμικές οπτικές διατάξεις νανοδομών για συστήματα οπτικών επικοινωνιών".



Ο Δημήτριος Μπουζιώτας είναι απόφοιτος του Τμήματος «Πληροφορικής και Τηλεπικοινωνιών» (2023) και μεταπτυχιακός φοιτητής στο Πρόγραμμα Μεταπτυχιακών Σπουδών «Πληροφορική και Δίκτυα» στο Πανεπιστήμιο Ιωαννίνων (2024). Εργάζεται ως ερευνητής και software developer στο «Ινστιτούτο Τεχνολογίας Υπολογιστών & Εκδόσεων - ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ», με εξειδίκευση σε μοντέλα μηχανικής όρασης. Από το 2023 έως και το 2024 συμμετείχε σε 5 δημοσιευμένα ερευνητικά άρθρα, εκ των οποίων τα δύο είναι συνεδριακά και τα παρουσίασε ο ίδιος.

Η εξέλιξη του Πολέμου: Η Τεχνολογία των UAVs στις Σύγχρονες Στρατιωτικές Επιχειρήσεις

Ιωάννης Σοφράς

Ευάγγελος Γκούμας

Εισαγωγή

UAV είναι το ακρωνύμιο των μη επανδρωμένων αεροχημάτων, τα οποία μπορούν λειτουργούν είτε υπό την καθοδήγηση ενός χειριστή από απομακρυσμένο κέντρο διοίκησης, είτε αυτόνομα [1].

ΠΗΓΗ: https://www.westernfrontassociation.com/world-war-i-articles/

Τα UAVs βρίσκονται σε χρήση ήδη από το 1903. Μερικοί, συγγραφείς υποστηρίζουν ότι τα αερόστατα τα οποία αναπτύχθηκαν στο δυτικό μέτωπο του Α΄Π.Π από το αεροπορικό σώμα των Η.Π.Α για να μειώσουν τις απώλειες σε πιλότους ήταν τα πρώτα UAVs, [2]. Κατά τη διάρκεια του Β΄Π.Π η γερμανική αεροπορική βιομηχανία ανέπτυξε το καινοτόμο για την εποχή V-1 (Vergeltungswaffe Eins) [3].

ΠΗΓΗ: « "V-1 Cruise Missile." National Air and Space Museum, accessed June 11, 2022.

Αυτό το γεγονός ώθησε τα μεταπολεμικά προγράμματα των ΗΠΑ να αντιμετωπίσουν αυτές τις εξελίξεις. Στον πόλεμο του Βιετνάμ [4] τη δεκαετία του 1960, τα UAV βρήκαν νέο ρόλο στην αόρατη επιτήρηση, οδηγώντας σε ευρύτερη εξερεύνηση της μη επανδρωμένης εναέριας τεχνολογίας από άλλα έθνη. Αυτές οι πρώιμες στρατιωτικές εφαρμογές εξελίχθηκαν, με τα μη επανδρωμένα αεροσκάφη να χρησιμοποιούνται για δόλωμα, εκτοξεύσεις πυραύλων και ψυχολογικές επιχειρήσεις.

Με την πάροδο του χρόνου, οι εξελίξεις, όπως η ηλιακή ενέργεια, διεύρυναν τις δυνατότητές τους, επιτρέποντας μεγαλύτερες και πιο εξελιγμένες πτήσεις [5]. Σήμερα, τα UAVs με την παρούσα τεχνολογία εξυπηρετούν ποικίλες λειτουργίες, από την παρακολούθηση του κλίματος και την αντιμετώπιση καταστροφών έως τη φωτογράφηση και την παράδοση αγαθών. Ωστόσο, η στρατιωτική τους χρήση, ιδίως

για επιτήρηση και στοχευμένες επιθέσεις μετά την 11η Σεπτεμβρίου 2001, παραμένει αμφιλεγόμενη, εγείροντας ηθικές ανησυχίες σχετικά με τις απώλειες αμάχων και τις επιπτώσεις του πολέμου από απόσταση [6].

Χρήσιμες πληροφορίες

Κατηγοροποίηση των μη επανδρωμένων οχημάτων

Τα UAVs με τα οποία θα ασχοληθούμε ανήκουν σε μία ευρύτερη κατηγορία μη επανδρωμένων οχημάτων (UVs) τα οποία ανάλογα με το περιβάλλον και για το σκοπό στο οποίο αξιοποιούνται κατηγοριοποιούνται ως εξής:

- Unmanned Ground Vehicles (UGVs): Τα μη επανδρωμένα οχήματα εδάφους, γνωστά και ως “UAV tanks”, αξιοποιούνται κυρίως στον στρατό για αποστολές εκκαθάρισης, έρευνας και διάσωσης και για την υποστήριξη του πεζικού. σε περιοχές υψηλού κινδύνου, επιτρέποντας ασφαλείς επιχειρήσεις [7]

ΠΗΓΗ: «Finn, A., & Scheding, S. (2010). Developments and challenges for Autonomous Unmanned Vehicles. Springer.»

- Unmanned Surface Vehicles (USVs): Τα μη επανδρωμένα οχήματα επιφάνειας νερού, χρησιμοποιούνται για ωκεανογραφική έρευνα και θαλάσσια επιτήρηση [8]. Αυτά τα συστήματα έχουν χρησιμοποιηθεί πρόσφατα έναντι στόχων επιφανείας [9, 10] .

ΠΗΓΗ: « Manley, J. E. (2008). Unmanned Surface Vehicles, 15 Years of Development.

- Aerial Drones: Τα πιο γνωστά και ευρέως χρησιμοποιούμενα UAVs είναι τα εναέρια drones, τα οποία μπορούν να πετούν και να εκτελούν αποστολές χαμηλού κόστους. Λειτουργούν σε διάφορα ύψη και συμβάλλουν σε εμπορικούς [11] και αμυντικούς σκοπούς [12].

ΠΗΓΗ: «Barnhart, R. K., Hottman, S. B., Marshall, D. M., & Shappee, E. (2012). Introduction to Unmanned Aircraft Systems. CRC Press.»

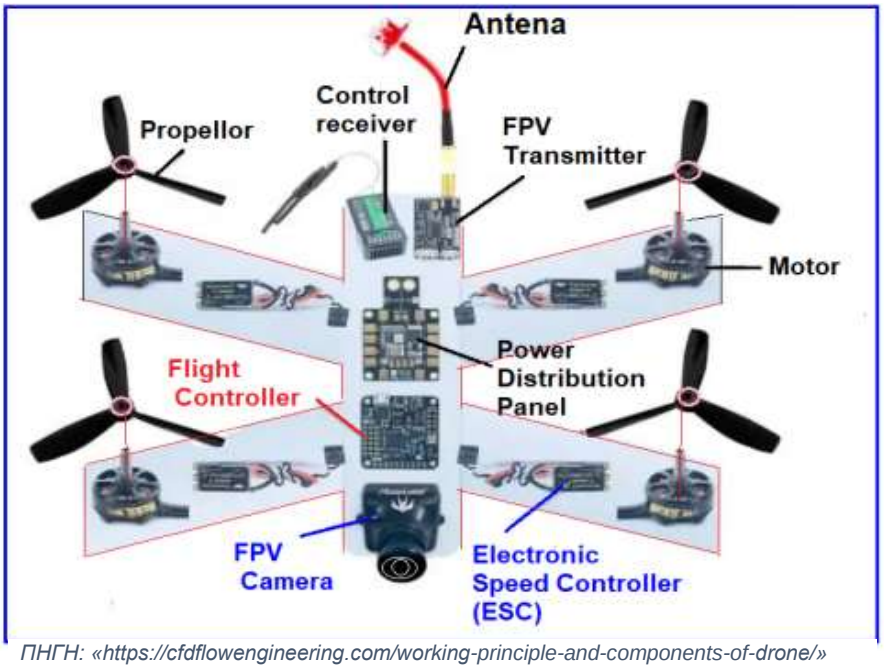
Υλικά και Κόστος Κατασκευής

Το κόστος κατασκευής UAV μπορεί να διαφέρει σημαντικά ανάλογα με τον τύπο, τα υλικά, την τεχνολογία και τα χαρακτηριστικά τους [13]. Η διαδικασία ανάπτυξης και παραγωγής περιλαμβάνει μια σειρά δαπανών, από υλικά και εξαρτήματα έως την ανάπτυξη λογισμικού και τις πιστοποιήσεις. Τα υλικά που χρησιμοποιούνται στην κατασκευή UAV πρέπει να παρέχουν ανθεκτικότητα, ελαφριές ιδιότητες και, σε ορισμένες εφαρμογές, αντοχή σε ακραίες συνθήκες [14]. Η επιλογή των υλικών είναι κρίσιμη, καθώς επηρεάζει άμεσα την απόδοση και την ενεργειακή αποδοτικότητα των

μη επανδρωμένων αεροσκαφών, καθιστώντας την βασικό παράγοντα για τον συνολικό σχεδιασμό και τη λειτουργικότητά τους.

Τα πιο διαδεδομένα υλικά που χρησιμοποιούνται από τις εταιρείες για την κατασκευή αυτών είναι:

- Σύνθετα Υλικά (Composite Materials): Όπως ίνες άνθρακα και ίνες γυαλιού, χρησιμοποιούνται ευρέως στην κατασκευή UAV λόγω της ανθεκτικότητας και του χαμηλού βάρους τους [15].
- Αλουμίνιο και Ελαφρά Κράματα (Aluminum and Light Alloys): Το αλουμίνιο και τα κράματα του είναι επίσης δημοφιλή λόγω του χαμηλού βάρους και της ευκολίας με την οποία μπορούν να διαμορφωθούν σε περίπλοκες δομές.



ΠΗΓΗ: «https://cfdflowengineering.com/working-principle-and-components-of-drone/»

- Πλαστικά Υψηλής Αντοχής (High-Strength Plastics): Πλαστικά όπως το ABS και το πολυανθρακικό βρίσκονται στα μικρότερα UAV, καθώς παρέχουν αντοχή και μειώνουν το κόστος κατασκευής [12].
- Τα ενεργειακά και ηλεκτρονικά συστήματα των UAV παίζουν καθοριστικό ρόλο στη λειτουργικότητα και την απόδοσή τους.
- Λιθίου Πολυμερή (Lithium Polymer) Μπαταρίες (Li-Po Batteries): Οι μπαταρίες πολυμερούς λιθίου είναι το βασικό υλικό ενέργειας για πολλά UAV. Οι μπαταρίες Li-Po προσφέρουν την απαιτούμενη ισχύ για πτήσεις μεγαλύτερης διάρκειας.
- Ηλεκτρονικά Συστήματα και Αισθητήρες: Τα UAV περιέχουν διάφορα ηλεκτρονικά εξαρτήματα, όπως μικροελεγκτές, κεραία GPS, κάμερα και αισθητήρες ανίχνευσης [7].

Τύποι μη επανδρωμένων αεροσκαφών ανάλογα με τους τύπους πτερύγων

Τα μη επανδρωμένα αεροσκάφη διατίθενται σε διάφορα μεγέθη και δυνατότητες, και κυμαίνονται από μικρά μοντέλα αναψυχής έως εξελιγμένα μη επανδρωμένα αεροσκάφη ελέγχου και επιτήρησης. Για να κατανοηθεί η ποικιλομορφία όσον αφορά την τεχνολογία UAVs [16], θα πρέπει να δούμε τις κατηγορίες τους ανάλογα με τον τύπο των πτερύγων.

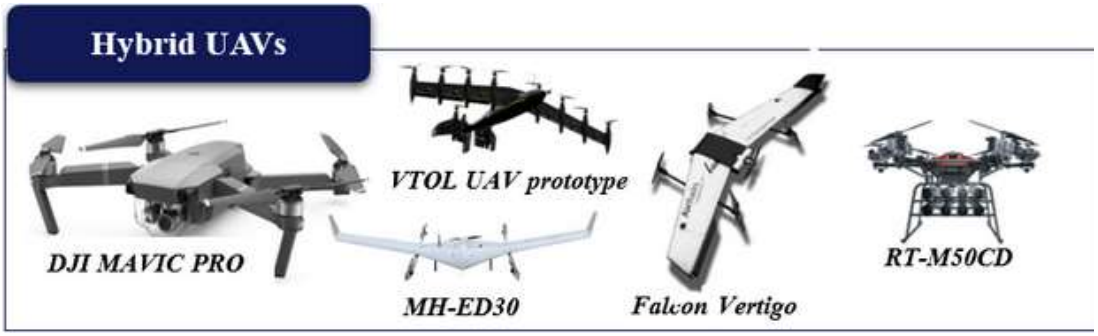
ΠΗΓΗ: Autonomous Unmanned Aerial Vehicles in Bushfire Management: Challenges and Opportunities.

- Fixed-Wing: Τα drones αυτά μοιάζουν με παραδοσιακά αεροπλάνα και έχουν πτέρυγες που δεν κινούνται. Είναι αποτελεσματικά για μεγάλες αποστάσεις και χρησιμοποιούνται σε γεωργικές εφαρμογές, έρευνες μεγάλων περιοχών και στρατιωτικές αποστολές αναγνώρισης.
- Multirotor: Τα πολυκόπτερα είναι drones με πολλούς ρότορες (συνήθως 4, 6 ή 8), που τους προσφέρουν ευελιξία και ακρίβεια στον έλεγχο. Αυτή η κατηγορία είναι δημοφιλής για εναέρια φωτογράφηση, βιντεοσκόπηση και εφαρμογές που απαιτούν σταθερότητα και δυνατότητα αιώρησης σε συγκεκριμένο σημείο. Ωστόσο, η διάρκεια πτήσης τους είναι περιορισμένη λόγω της κατανάλωσης ενέργειας από τους πολλούς ρότορες.

ΠΗΓΗ: Autonomous Unmanned Aerial Vehicles in Bushfire Management: Challenges and Opportunities.

- VTOL - Vertical Take-Off and Landing: Αυτά τα drones μπορούν να απογειώνονται και να προσγειώνονται κάθετα, όπως τα ελικόπτερα, και έπειτα να πετούν σαν drones σταθερής πτέρυγας. Το VTOL χαρακτηριστικό τα καθιστά ιδανικά για περιοχές όπου ο χώρος απογείωσης και προσγείωσης είναι περιορισμένος.

- Hybrid: Τα υβριδικά drones συνδυάζουν χαρακτηριστικά από πολυκόπτερα και σταθερής πτέρυγας, προσφέροντας αυξημένη ευελιξία και αντοχή πτήσης. Συνήθως χρησιμοποιούνται σε αποστολές όπου απαιτείται μεγάλη αντοχή σε πτήση και ικανότητα αιώρησης.



ΠΗΓΗ: Autonomous Unmanned Aerial Vehicles in Bushfire Management: Challenges and Opportunities

Λογισμικό

Λογισμικό Πτήσης (Flight Control Software)

Τα λογισμικά πτήσης αποτελούν βασικό κομμάτι για την επιτυχή και ακριβή λειτουργία των drones, καθώς ελέγχουν τις κινήσεις, την σταθερότητα και τη συνολική διαχείριση πτήσεων. Τα συστήματα λογισμικού πτήσης διασφαλίζουν ότι τα drones εκτελούν πτήσεις με ασφάλεια και αξιοπιστία, ενώ επιτρέπουν την αυτοματοποίηση και την ακρίβεια στους χειρισμούς. Δύο από τα πιο δημοφιλή λογισμικά πτήσης είναι το PX4 και το ArduPilot [17].

PX4

Το PX4 είναι ένα ανοιχτού κώδικα λογισμικό πτήσης που έχει αναπτυχθεί από την Dronecode Foundation. Χρησιμοποιείται κυρίως σε βιομηχανικές και εμπορικές εφαρμογές, καθώς και σε ερευνητικά προγράμματα [17]. Τα βασικά χαρακτηριστικά του PX4 περιλαμβάνουν:

- Υποστήριξη πολλών τύπων drones
- Αυτοματοποίηση και Ασφάλεια
- Διαλειτουργικότητα και Υποστήριξη

ArduPilot

Το ArduPilot είναι επίσης ένα ανοιχτού κώδικα λογισμικό πτήσης που έχει αναπτυχθεί με την υποστήριξη της κοινότητας προγραμματιστών και είναι γνωστό για την ευελιξία και τη σταθερότητά του. Χρησιμοποιείται τόσο σε καταναλωτικά όσο και σε εμπορικά drones, με τις βασικές του δυνατότητες να περιλαμβάνουν:

- Αυτοματοποιημένη Πλοήγηση
- Προηγμένες Δυνατότητες Ασφάλειας

- Ευρεία Υποστήριξη για Τύπους UAV

Αυτά τα λογισμικά προσφέρουν τη δυνατότητα για εύκολη προσαρμογή και συνεχείς βελτιώσεις, καθώς υποστηρίζονται από μεγάλες κοινότητες χρηστών και προγραμματιστών, γεγονός που διασφαλίζει την αξιοπιστία και την καινοτομία τους.

Συστήματα Αναγνώρισης και Αποφυγής (Sense and Avoid Systems)

Τα συστήματα αναγνώρισης και αποφυγής, γνωστά ως Sense and Avoid Systems, είναι απαραίτητα για τη βελτίωση της ασφάλειας των drones, ιδιαίτερα σε περιβάλλοντα με πολλαπλά εμπόδια και άλλες πτητικές δραστηριότητες. Αυτά τα συστήματα συνδυάζουν αισθητήρες και λογισμικό για να ανιχνεύουν εμπόδια στον περιβάλλοντα χώρο του drone και να προσαρμόζουν την πτήση του ώστε να αποφεύγει τις συγκρούσεις [18].

Βασικές Λειτουργίες των Sense and Avoid Systems

- Αναγνώριση Εμποδίων
- Αυτόματη Αποφυγή
- Αυτοματοποιημένη Πλοήγηση
- Αποτροπή Ατυχημάτων

Συστήματα Πλοήγησης και GPS

Τα συστήματα πλοήγησης και GPS είναι ουσιαστικά για τον έλεγχο και την ακρίβεια πτήσης των drones. Ενσωματώνονται στο λογισμικό των drones και επιτρέπουν τον προγραμματισμό διαδρομών και την ακριβή παρακολούθηση της θέσης, ακόμα και σε περιβάλλοντα με απαιτήσεις υψηλής ακρίβειας. Δύο από τις πιο συχνά χρησιμοποιούμενες τεχνολογίες είναι το GPS και το RTK GPS [19].

Βασικά Συστήματα Πλοήγησης

- GPS (Global Positioning System)
- RTK GPS (Real-Time Kinematic GPS)
- Συστήματα Προγραμματισμού Πτήσεων
- INS (Inertial Navigation System)

Artificial Intelligence (AI) Και Machine Learning (ML) Εφαρμογές στα Drones

Η τεχνητή νοημοσύνη (AI) και η μηχανική μάθηση (ML) έχουν μεταμορφώσει τη λειτουργικότητα και την απόδοση των drones, δίνοντάς τους τη δυνατότητα να λειτουργούν με υψηλό επίπεδο αυτονομίας και να εκτελούν περίπλοκες αποστολές. Με τη βοήθεια αυτών των τεχνολογιών, τα drones δεν περιορίζονται πλέον σε προκαθορισμένες διαδρομές και βασικές λειτουργίες, αλλά μπορούν να αναγνωρίζουν αντικείμενα, να πλοηγούνται με αυτονομία και να αναλύουν δεδομένα σε πραγματικό χρόνο [15].

Αυτόνομη Πλοήγηση με AI και ML

Η αυτόνομη πλοήγηση είναι μια από τις πιο σημαντικές εφαρμογές της AI στα drones. Χάρη στη μηχανική μάθηση, τα drones μπορούν να μάθουν να αντιλαμβάνονται και να αντιδρούν στο περιβάλλον τους με ελάχιστη ή καθόλου ανθρώπινη παρέμβαση [18]. Στις δυνατότητες τους περιλαμβάνονται:

- Ανίχνευση και Αποφυγή Εμποδίων
- Αυτόματη Αναγνώριση και Εντοπισμός Αντικειμένων
- Χαρτογράφηση και Εξερεύνηση

Ανάλυση Δεδομένων με AI και ML

Εκτός από την πλοήγηση, οι AI και ML τεχνολογίες δίνουν στα drones τη δυνατότητα να επεξεργάζονται και να αναλύουν τα δεδομένα που συλλέγουν, χωρίς να χρειάζεται μεταφορά των δεδομένων σε εξωτερικούς υπολογιστές για ανάλυση [19].

Στις δυνατότητες τους περιλαμβάνονται:

- Ανάλυση Εικόνας και Βίντεο
- Ανάλυση Περιβαλλοντικών Δεδομένων

Χώρες Παραγωγοί και χρήσης UAVs σε στρατιωτικές τους επιχειρήσεις.

ΠΗΓΗ:https://www.statista.com/chart/20005/total-forecast-purchases-of-weaponized-military-drones/

Η αύξηση της στρατιωτικής χρήσης των τηλεχειριζόμενων μη επανδρωμένων αεροσκαφών (UAV), κοινώς μη επανδρωμένων αεροσκαφών, είναι εκπληκτική. Τα μη επανδρωμένα αεροσκάφη έχουν καταστεί κεντρικής σημασίας για τον τρόπο με τον οποίο οι ένοπλες δυνάμεις διεξάγουν πολέμους και προβάλλουν ισχύ στις αρχές του εικοστού πρώτου αιώνα. Παράλληλα με τη διευρυμένη χρήση τους, υπήρξε σημαντική αύξηση των εγκαταστάσεων κατασκευής UAV παγκοσμίως. Ενώ κάποτε οι ΗΠΑ και το Ισραήλ μονοπωλούσαν τον τομέα, ένας αυξανόμενος αριθμός χωρών, συμπεριλαμβανομένης της Κίνας και της Τουρκίας, φιλοξενεί πλέον προηγμένα κέντρα παραγωγής UAV και εξάγει μια εκπληκτική σειρά στρατιωτικών μη επανδρωμένων αεροσκαφών, αντανακλώντας την αυξανόμενη παγκόσμια ζήτηση για αυτή τη μετασχηματιστική τεχνολογία.

- **Ηνωμένες Πολιτείες:** Η General Atomics και η Northrop Grumman κατασκευάζουν drones για στρατιωτική και πολιτική χρήση. Το MQ-9 Reaper είναι ένα από τα πιο γνωστά στρατιωτικά drones από τις ΗΠΑ [20].

- **Κίνα:** Μία από τους μεγαλύτερους παραγωγούς εμπορικών drones, με την DJI να κατέχει μεγάλο μερίδιο της αγοράς σε drones καταναλωτικής χρήσης και μικρούς επαγγελματικούς τομείς [21].

- **Τουρκία:** Έχει εξελιχθεί σε σημαντικό κέντρο παραγωγής στρατιωτικών drones, με γνωστότερο παράδειγμα το Bayraktar TB2, το οποίο έχει χρησιμοποιηθεί σε πολλές στρατιωτικές αποστολές [22].

- **Ρωσία:** Η Ρωσία αναπτύσσει δικά της drones, όπως το Orlan-10, κυρίως για στρατιωτικές επιχειρήσεις και επιτήρηση, εστιάζοντας σε drones με μεγάλη αντοχή και ανθεκτικότητα σε δύσκολες συνθήκες [23].

- **Ισραήλ:** Το Ισραήλ είναι πρωτοπόρο στην ανάπτυξη στρατιωτικών drones με μακρά παράδοση στον τομέα αυτό και έχει κατασκευάσει drones όπως το Heron για αναγνωριστικές και άλλες αποστολές [24].

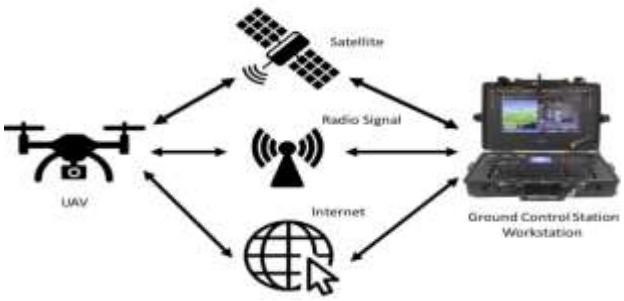
Παρόλο που δεν διαθέτουν όλες οι χώρες εγχώρια εργοστάσια παραγωγής UAVs, πολλές επιδιώκουν να εντάξουν τα μη επανδρωμένα αεροχήματα στα οπλοστάσια των ενόπλων δυνάμεών τους, είτε μέσω εγχώριας ανάπτυξης είτε αγοράζοντας τα από άλλες χώρες που διαθέτουν προηγμένη τεχνογνωσία στον τομέα αυτό [25].

Ο κάτωθι πίνακας παρουσιάζει ενδεικτικά παραδείγματα αυτής της τάσης.

Χώρες	Έτος ένταξης	Τύπος UAV	Χώρα παραγωγός
Η.Π.Α	2001	MQ-9 Reaper MQ-1 Gray Eagle MQ-1 Avenger	Η.Π.Α
Ρωσία	2020	Orion Forpost-R Shahed-129 Mohajer-6	Ιράν
Ισραήλ	2004	Hermes 450 Hermes 900 Heron TP	Ισραήλ
Τουρκία	2016	Bayraktar TB-2 Ankas-S Akinci-A	Τουρκία
Κίνα	2011	CH-series Wing-Loong I/II Cloud Shadow	Κίνα
Ιράν	2014	Shahed-129 Mohager-6	Ιράν
Ουκρανία	2021	Bayraktar TB-2	Τουρκία
Γαλλία	2019	MQ-9 Reaper	Η.Π.Α
Πακιστάν	2015	Burraf(CH-3) CH-4 Bayraktar TB-2	Πακιστάν Κίνα

Πρωτόκολλα Επικοινωνίας

Τα μη επανδρωμένα αεροσκάφη (UAVs) βασίζονται σε ισχυρά συστήματα επικοινωνίας για τη σύνδεση με τους επίγειους σταθμούς ελέγχου (GCS). Η αποτελεσματική επικοινωνία εξασφαλίζει ακριβή έλεγχο, μετάδοση δεδομένων και αξιόπιστη λειτουργία. Οι τρεις κύριες μέθοδοι για την εγκαθίδρυση αυτής της σύνδεσης είναι η δορυφορική επικοινωνία, τα ραδιοσήματα και η επικοινωνία μέσω διαδικτύου. Κάθε σύστημα προσφέρει μοναδικά πλεονεκτήματα και συμβιβασμούς ανάλογα με τις απαιτήσεις της αποστολής.



ΠΗΓΗ: https://www.researchgate.net/figure/Default-ways-of-controlling-UAVs-through-the-ground-control-stations-in-both-manual-and_fig1_341296640

Δορυφορική επικοινωνία (SATCOM)

Το SATCOM [26] χρησιμοποιείται συχνά για τη μετάδοση κρίσιμων δεδομένων ISR (πληροφοριών, επιτήρησης και αναγνώρισης) από μακρινά UAV, σε περιπτώσεις όπου οι υπεύθυνοι λήψης αποφάσεων απαιτούν πρόσβαση στα δεδομένα σε πραγματικό ή σχεδόν πραγματικό χρόνο και δεν έχουν την πολυτέλεια να περιμένουν την επιστροφή του αεροσκάφους. Χρησιμοποιείται επίσης για τη δημιουργία ασφαλών, αξιόπιστων συνδέσεων C2 μεταξύ μη επανδρωμένων οχημάτων και GCS (σταθμών ελέγχου εδάφους), επιτρέποντας στους χρήστες να παρακολουθούν την κατάσταση, να ελέγχουν εξ αποστάσεως το όχημα και να εναλλάσσονται μεταξύ απομακρυσμένου ελέγχου και αυτόνομης λειτουργίας.

Επικοινωνία μέσω ραδιοσυχνοτήτων

Η επικοινωνία ραδιοσυχνοτήτων (RF) [27] αποτελεί τη ραχοκοκαλιά της σύνδεσης μεταξύ ενός drone και του τηλεχειριστηρίου του, χρησιμοποιώντας δημοφιλείς ζώνες ISM, όπως τα 2,4 GHz και 5,8 GHz, για ισορροπία μεταξύ εμβέλειας και ταχύτητας δεδομένων. Αυτό το ψηφιακό πρωτόκολλο επικοινωνίας διασφαλίζει την αξιοπιστία και ελαχιστοποιεί τις παρεμβολές, επιτρέποντας τη λειτουργία και την ευελιξία του drone σε πραγματικό χρόνο [28].

Πώς λειτουργεί η επικοινωνία RF:

- Μετάδοση: Οι είσοδοι του χειριστή του drone μετατρέπονται σε ηλεκτρικά σήματα από τον πομπό του τηλεχειριστηρίου. Τα σήματα αυτά διαμορφώνονται σε ένα κύμα φορέα σε συγκεκριμένη ραδιοσυχνότητα και στη συνέχεια μεταδίδονται ασύρματα στο drone.
- Δέκτης του drone: Ο δέκτης του drone, συντονισμένος στην ίδια συχνότητα, συλλαμβάνει τα σήματα RF και τα αποδιαμορφώνει για να ανακτήσει τα αρχικά σήματα ελέγχου.
- Ελεγκτής πτήσης: Ο ελεγκτής πτήσης, ένας ενσωματωμένος υπολογιστής, ερμηνεύει αυτά τα σήματα και τα μεταφράζει σε εντολές για τους κινητήρες του drone. Για παράδειγμα, μια κίνηση του joystick έχει ως αποτέλεσμα την αντίστοιχη κίνηση του drone.
- Ανατροφοδότηση τηλεμετρίας: Πολλά μη επανδρωμένα αεροσκάφη στέλνουν επίσης δεδομένα τηλεμετρίας σε πραγματικό χρόνο πίσω στον χειριστή, συμπεριλαμβανομένων πληροφοριών σχετικά με το υψόμετρο, την ταχύτητα, τη στάθμη της μπαταρίας και τη θέση, ενισχύοντας την επίγνωση της κατάστασης και τον έλεγχο.

Αυτή η απρόσκοπτη αλληλεπίδραση εξασφαλίζει ακριβή και ευέλικτο έλεγχο, καθιστώντας την επικοινωνία RF ένα κρίσιμο στοιχείο των λειτουργιών των drone.

Επικοινωνία μέσω διαδικτύου

Η ενσωμάτωση κινητών κυψελοειδών δικτύων στις επιχειρήσεις μη επανδρωμένων αεροσκαφών (UAV) προσφέρει εκτεταμένη κάλυψη από απόσταση, ασφαλή

επικοινωνία και βελτιωμένη ασφάλεια. Αυτά τα χαρακτηριστικά ενισχύουν την ανάπτυξη UAV σε μια ποικιλία κρίσιμων εφαρμογών.

Προηγούμενες μελέτες για την ενσωμάτωση κυψελοειδών δικτύων

Αρκετές μελέτες έχουν διερευνήσει τη χρήση των κυψελοειδών δικτύων, ιδίως των υποδομών Long-Term Evolution (LTE) και τέταρτης γενιάς (4G), σε επιχειρήσεις UAV:

- LTE-Based Control of Small UAVs: Οι Lin et al. [29] απέδειξαν ότι τα υπάρχοντα δίκτυα 4G μπορούν να υποστηρίξουν ασύρματη συνδεσιμότητα ευρείας περιοχής για επιχειρήσεις UAV χαμηλού υψομέτρου. Η μελέτη τους ανέδειξε τεχνικές βελτίωσης των επιδόσεων για τη βελτιστοποίηση της συνδεσιμότητας LTE, εξασφαλίζοντας αποτελεσματική επικοινωνία UAV και ελαχιστοποιώντας παράλληλα τις παρεμβολές με επίγειες κινητές συσκευές. Επιπλέον, προτάθηκαν εναέριες εικόνες και ροή βίντεο με τη χρήση UAV που ελέγχονται μέσω δικτύου κινητής τηλεφωνίας για εφαρμογές κεντρικής παρακολούθησης.
- Αρχιτεκτονική παρακολούθησης σε πραγματικό χρόνο: Μια άλλη μελέτη [30] πρότεινε ένα πλαίσιο παρακολούθησης κλειστού κυκλώματος που χρησιμοποιεί δίκτυα 4G. Αυτή η αρχιτεκτονική υποστήριζε ροή βίντεο σε πραγματικό χρόνο από UAV για την αποτελεσματική παρακολούθηση εσωτερικών και εξωτερικών περιβαλλόντων. Η έρευνα προσομοίωσε επίσης τις επιδράσεις των επιδόσεων του δικτύου, ιδίως της απόδοσης δεδομένων, για εργασίες παρακολούθησης που βασίζονται σε UAV.
- Απώλεια διαδρομής και παρεμβολές στον έλεγχο UAV: Μια ξεχωριστή έρευνα [31] εξέτασε την επίδραση του ύψους του UAV στην απώλεια διαδρομής και την απόδοση του κυψελοειδούς δικτύου. Τα αποτελέσματα έδειξαν ότι οι παρεμβολές στην καθοδική ζεύξη αποτελούν σημαντικό περιορισμό κατά τη χρήση κυψελοειδών δικτύων για τον έλεγχο UAV. Παρόλο που προτάθηκαν σχήματα ακύρωσης παρεμβολών, ήταν λιγότερο πρακτικά για UAV σε σύγκριση με τους χρήστες εδάφους. Παρόλα αυτά, η αξιοποίηση της ετερογένειας των μακροδικτύων έδειξε δυνατότητες βελτίωσης της συνδεσιμότητας και της αξιοπιστίας για την επικοινωνία UAV-σταθμού ελέγχου εδάφους (GCS).

Ενσωμάτωση WiFi και δικτύου Ad-Hoc

Το WiFi και τα ad-hoc δίκτυα διερευνώνται επίσης για την ενίσχυση της συνδεσιμότητας του συστήματος UAV:

- Εναέριοι κόμβοι WiFi: Η μελέτη στο [32] πρότεινε ένα πλαίσιο όπου τα UAV χρησιμεύουν ως εναέριοι κόμβοι WiFi, είτε ως σημεία πρόσβασης είτε ως ad-hoc ενδιάμεσα hops. Τα ευρήματα αποκάλυψαν έναν συμβιβασμό μεταξύ της κάλυψης και των ρυθμών δεδομένων, με την ad-hoc λειτουργία να επιδεικνύει υψηλότερη ανταπόκριση.

- Αυτοματοποίηση μέσω αισθητήρων WiFi χαμηλού κόστους: Στο [33], παρουσιάστηκε ένα πλαίσιο για αυτοματοποιημένα μικρο-UAVs που χρησιμοποιούν WiFi 802.11b. Η απόδοση του UAV παρακολουθήθηκε μέσω των αρχείων καταγραφής πτήσης που εμφανίζονταν σε ένα απλό GUI, παρουσιάζοντας τη σκοπιμότητα του WiFi ως μέσο επικοινωνίας μεταξύ του GCS και των UAV.

Η Στρατηγική Αξία των UAVs στη Μάχη

Ρώσο – Ουκρανικός Πόλεμος (2023-έως σήμερα)

Η σύγκρουση μεταξύ Ρωσίας και Ουκρανίας έχει αναδείξει την τεχνολογία των drones ως ένα από τα πιο κρίσιμα εργαλεία στη σύγχρονη πολεμική στρατηγική. Ρωσία και Ουκρανία έχουν χρησιμοποιήσει εκατέρωθεν drones για ποικίλες στρατιωτικές αποστολές, όπως αναγνώριση, επιτήρηση, και επιθέσεις ακριβείας φέρνοντας τη χρήση των UAV στο προσκήνιο των στρατιωτικών τακτικών [34].

Τύποι Drones και Ρόλοι στη Σύγκρουση

Οι στρατιωτικές δυνάμεις της Ουκρανίας και της Ρωσίας έχουν ενσωματώσει διαφορετικούς τύπους drones, που ανταποκρίνονται στις ανάγκες τους στον πόλεμο[23].

- Εναέρια Drones για Αναγνώριση και Επίθεση: Η Ουκρανία έχει χρησιμοποιήσει ευρέως drones όπως το Bayraktar TB2, που παράγεται στην Τουρκία, το οποίο είναι γνωστό για την αποτελεσματικότητά του σε αποστολές αναγνώρισης και ακριβείας. Η Ρωσία έχει επίσης χρησιμοποιήσει drones όπως το Orlan-10, το οποίο επικεντρώνεται σε αναγνωριστικές αποστολές και επιτήρηση πεδίου μάχης.

ΠΗΓΗ : https://www.pbs.org/newshour/world/how-ukraine-soldiers-use-inexpensive-commercial-drones-on-the-battlefield

- Drones Αυτοκτονίας (Loitering Munitions): Η χρήση drones αυτοκτονίας, όπως το ιρανικό Shahed-136 που έχει ενσωματωθεί στις ρωσικές

επιχειρήσεις, έχει αλλάξει τη φύση της μάχης, προσφέροντας τη δυνατότητα αποστολών επίθεσης μεγάλων αποστάσεων με χαμηλό κόστος [22].

Στρατηγική Σημασία των Drones στη Σύγκρουση

Η χρήση των drones επέτρεψε τόσο στη Ρωσία όσο και στην Ουκρανία να εκτελούν αποστολές με ακρίβεια και να συλλέγουν πληροφορίες χωρίς να εκθέτουν το ανθρώπινο δυναμικό σε κίνδυνο. Η δυνατότητα για συνεχείς αναγνωριστικές αποστολές βοήθησε και τις δύο πλευρές να παρακολουθούν τη θέση των αντιπάλων και να προσαρμόζουν την τακτική τους [20].

- Ασυμμετρική Αντίσταση: Η Ουκρανία, παρά το στρατιωτικά υποδεέστερο υλικό, μπόρεσε να αντισταθεί αποτελεσματικά χρησιμοποιώντας φθηνά drones εμπορικού τύπου, τα οποία έχουν προσαρμοστεί για στρατιωτική χρήση.
- Επιθέσεις ακριβείας και Ψυχολογικός Πόλεμος: Οι επιθέσεις drones προκάλεσαν ψυχολογική πίεση, με αεροπορικές επιδρομές σε πόλεις και στρατηγικές εγκαταστάσεις, κάτι που έχει κλονίσει τον ηθικό των στρατιωτών και των πολιτών και από τις δύο πλευρές.

Επιπτώσεις στην Αντίληψη της Πολεμικής Τεχνολογίας

Η ευρεία χρήση των drones στη σύγκρουση αυτή έχει ενισχύσει τη σημασία τους σε σύγχρονες στρατιωτικές επιχειρήσεις [35], με αποτέλεσμα:

- Αλλαγή στη Στρατηγική Αμυντικών Δαπανών: Η σύγκρουση υπογράμμισε ότι οι φθηνές και εύκολα διαθέσιμες τεχνολογίες drones μπορούν να είναι εξαιρετικά αποτελεσματικές, οδηγώντας πολλές χώρες να αναθεωρήσουν τις στρατιωτικές τους επενδύσεις προς την ανάπτυξη και ενσωμάτωση των UAV.

- Πολυδιάστατος Πόλεμος: Τα drones αναδεικνύουν την έννοια του πολυδιάστατου πολέμου, όπου εναέριες, θαλάσσιες και επίγειες μονάδες drones μπορούν να ενσωματωθούν σε ενιαίες στρατιωτικές επιχειρήσεις.

Πιθανοί Κίνδυνοι και Αντιμετώπιση

Η χρήση drones στον πόλεμο Ρωσίας-Ουκρανίας αναδεικνύει και τους κινδύνους της ανεξέλεγκτης χρήσης αυτής της τεχνολογίας. Οι κίνδυνοι περιλαμβάνουν:

- Κυβερνοεπιθέσεις: Η εξάρτηση των drones από τα συστήματα GPS και τις δικτυακές επικοινωνίες τα καθιστά ευάλωτα σε κυβερνοεπιθέσεις και παρεμβολές.

- Ηθικά Ζητήματα: Η ευκολία με την οποία τα drones μπορούν να χρησιμοποιηθούν για επιθέσεις σε στρατιωτικούς και μη στρατιωτικούς στόχους θέτει σοβαρά ερωτήματα σχετικά με τους κανόνες πολέμου.

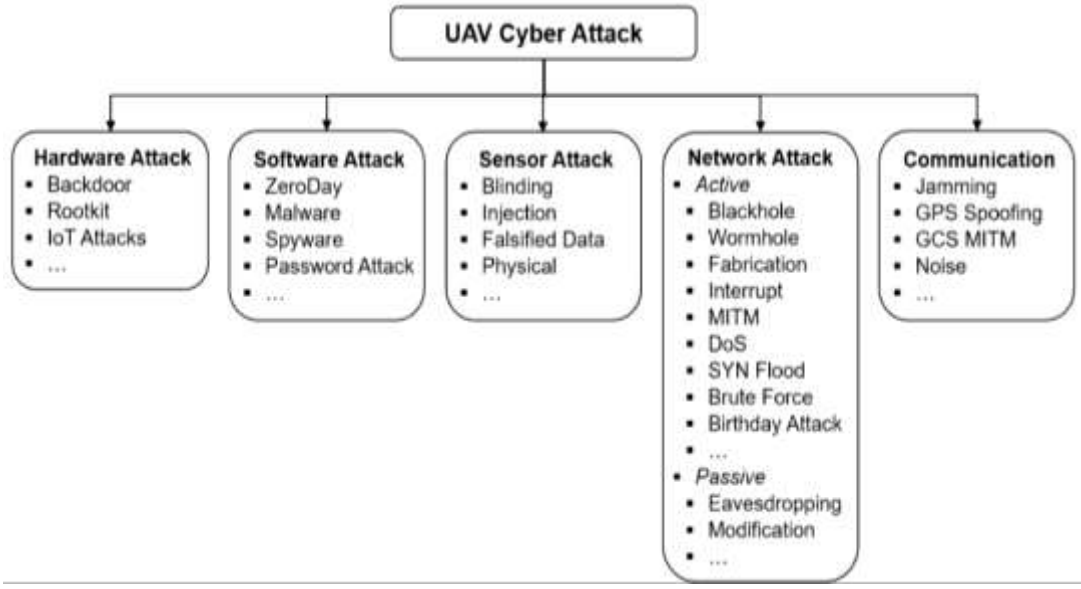
Η Ρωσό-Ουκρανική κρίση δείχνει τον καθοριστικό ρόλο που μπορούν να παίξουν τα drones στις σύγχρονες συγκρούσεις, αναδεικνύοντας τόσο τη δύναμη όσο και τους κινδύνους αυτής της τεχνολογίας [36].

Τρόποι Αντιμετώπισης των UAVs

Εξουδετέρωση UAVs μέσω hacking και ηλεκτρονικού πολέμου

Οι κυβερνοεπιθέσεις σε συστήματα UAVs συνιστούν σημαντικές απειλές για τη λειτουργικότητα και την ασφάλειά τους, στοχεύοντας σε διάφορα δομικά στοιχεία[Cosar, M. (2022). Cyber attacks on unmanned aerial vehicles and cyber security measures. The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 21, 258-265.], όπως υλικό, λογισμικό, αισθητήρες, δίκτυα και συστήματα επικοινωνίας. Κάθε φάση του κύκλου ζωής ενός UAV - ανάπτυξη, παραγωγή και συναρμολόγηση - απαιτεί ξεχωριστές αρχιτεκτονικές, οι οποίες μπορούν να εισάγουν ευπάθειες σε πολλαπλά επίπεδα. Αυτές οι ευπάθειες, ιδίως σε στοιχεία που είναι υπεύθυνα για τη λήψη κρίσιμων αποφάσεων, είναι ευάλωτες σε απειλές που θέτουν σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα των πληροφοριών.

Μεταξύ αυτών, οι δικτυακές επιθέσεις είναι οι πιο διαδεδομένες και διακρίνονται σε δύο κύριες κατηγορίες: **Ενεργητικές (Active)** και **Παθητικές (Passive).**



ΠΗΓΗ: Cyber attacks on unmanned aerial vehicles and cyber security measures

Οι ενεργητικές επιθέσεις αποσκοπούν στη διατάραξη των λειτουργιών μέσω της παραβίασης των αρχών ασφαλείας, ενώ οι παθητικές επιθέσεις επικεντρώνονται στην κρυφή πρόσβαση σε ευαίσθητες πληροφορίες χωρίς να επηρεάζεται η απόδοση του συστήματος. Οι επιθέσεις αυτές στοχεύουν τοπολογίες δικτύων, συστήματα επικοινωνίας, πρωτόκολλα και ανταλλαγές δεδομένων σε συστήματα UAV, συμπεριλαμβανομένων των σταθμών ελέγχου εδάφους (GCS) και των σμηνών UAV.

Τα πρωτόκολλα δρομολόγησης (Routing protocols), ένα κρίσιμο μέρος της αρχιτεκτονικής του δικτύου, διασφαλίζουν την ασφαλή και αποτελεσματική μετάδοση πακέτων δεδομένων. Ωστόσο, αποτελούν επίσης μια βασική ευπάθεια που αξιοποιείται σε επιθέσεις στον κυβερνοχώρο. Θέτοντας σε κίνδυνο τα επίπεδα μετάδοσης και τα πρωτόκολλα δρομολόγησης[37], οι επιτιθέμενοι μπορούν να εξαπολύσουν τόσο ενεργητικές όσο και παθητικές επιθέσεις, διακόπτοντας την επικοινωνία και θέτοντας σε κίνδυνο την αποστολή του UAV. Η αντιμετώπιση αυτών των προκλήσεων απαιτεί μια ολοκληρωμένη προσέγγιση για την εξασφάλιση ολόκληρου του συστήματος UAV έναντι πιθανών απειλών.

Ο παρακάτω πίνακας περιέχει τους τύπους κυβερνοεπιθέσεων κατά των UAVs.

Τύπος Επίθεσης	Όνομα	Ορισμός
Active	MITM	Χάκερ υποκλέπτει την αμφίδρομη επικοινωνία μεταξύ των κόμβων, δρομολογώντας όλες τις μεταδόσεις μέσω του εαυτού του. Αυτό επιτρέπει στον επιτιθέμενο να κρυφακούει, να τροποποιήσει δεδομένα, να κλέψει ευαίσθητες πληροφορίες όπως κωδικούς πρόσβασης και να υποδυθεί ένα από τα μέρη που επικοινωνούν.
Active	Worm Hole	Κακόβουλοι κόμβοι συνεργάζονται για τη δημιουργία ενός καναλιού επικοινωνίας υψηλής ποιότητας, το οποίο χρησιμοποιούν για να παρασύρουν τους γύρω κόμβους στην αποστολή πακέτων δεδομένων. Οι επιτιθέμενοι μπορούν να χειραγωγήσουν ή να απορρίψουν τα πακέτα, διαταράσσοντας το δίκτυο.
Active	Black Hole	Ένας αθέμιτος κόμβος τοποθετεί τον εαυτό του ως τη συντομότερη διαδρομή για επικοινωνία, στέλνοντας ψευδείς απαντήσεις δρομολόγησης. Μόλις τα πακέτα δεδομένων δρομολογηθούν μέσω αυτού, ο επιτιθέμενος μπορεί να τα διαγράψει, να τα τροποποιήσει ή να τα ανακατευθύνει, προκαλώντας ενδεχομένως επιθέσεις άρνησης παροχής υπηρεσιών ή υποκλέπτοντας δεδομένα.

1

Τύπος Επίθεσης	Όνομα	Ορισμός
Active	Fabrication	Αυτή η επίθεση περιλαμβάνει την εισαγωγή ψευδών μηνυμάτων δρομολόγησης για τη δημιουργία σύγχυσης στο δίκτυο, την αποστράγγιση πόρων ή τη διακοπή της λειτουργίας. Παραδείγματα περιλαμβάνουν τη διάσωση διαδρομών, τις επιθέσεις στέρησης ύπνου και τις επιθέσεις επανάληψης.
Active	Interrupt	Ο επιτιθέμενος μπλοκάρει τη μετάδοση πακέτων μεταξύ κόμβων τροποποιώντας τα μηνύματα δρομολόγησης, διακόπτοντας ουσιαστικά την επικοινωνία με τον κόμβο-στόχο.
Active	DoS	Αυτή η επίθεση υπερφορτώνει τους κόμβους και τους πόρους του δικτύου δημιουργώντας υπερβολική κίνηση, καταναλώνοντας εύρος ζώνης και εξαντλώντας τις δυνατότητες μνήμης, CPU ή αποθήκευσης.
Active	SYN Flood	Ένας τύπος επίθεσης DoS όπου ο επιτιθέμενος βομβαρδίζει το δίκτυο με υπερβολικά αιτήματα SYN, υπερφορτώνοντας την ικανότητα του συστήματος να επεξεργάζεται νόμιμη κυκλοφορία.
Active	Brute Force	Αυτή η επίθεση επιχειρεί επανειλημμένα διάφορους συνδυασμούς ονόματος χρήστη και κωδικού πρόσβασης σε ένα σύστημα ελεγχόμενης πρόσβασης για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση.
Active	Birthday Attack	Εκμεταλλευόμενος αλγόριθμους κατακερματισμού, ο επιτιθέμενος δημιουργεί ένα μήνυμα digest πανομοιότυπο με το αρχικό. Αυτό του επιτρέπει να αντικαταστήσει ένα νόμιμο μήνυμα με το δικό του χωρίς να εντοπιστεί, θέτοντας σε κίνδυνο την ακεραιότητα των επικοινωνιών.
Passive	Eavesdropping	Ο επιτιθέμενος παρακολουθεί και αναλύει την κυκλοφορία του δικτύου για να αντλήσει μη εξουσιοδοτημένες πληροφορίες, συχνά χωρίς να διαταράξει τη λειτουργία του δικτύου.

Τύπος Επίθεσης	Όνομα	Ορισμός
Passive	Modification	Τα πακέτα ανακατευθύνονται σε λανθασμένους προορισμούς, με αποτέλεσμα να κυκλοφορούν άσκοπα και τελικά να λήγουν. Αυτό προκαλεί συμφόρηση του δικτύου και σπαταλά τους πόρους του κόμβου προέλευσης, όπως ενέργεια και εύρος ζώνης, λόγω των επαναλαμβανόμενων επαναμεταδόσεων. Παράδειγμα: εσφαλμένη δρομολόγηση.

Εξουδετέρωση UAVs μέσω οπλικών συστημάτων

2 ΠΗΓΗ : https://armyrecognition.com/news/army-news/army-news-2024/eurosatory-2024-knds-presents-rapidfire-defense-system

Τα συστήματα αντι-UAV έχουν εξελιχθεί σημαντικά ως απάντηση στην αυξανόμενη απειλή[38] των μη επανδρωμένων αεροσκαφών, αξιοποιώντας τόσο παραδοσιακές όσο και καινοτόμες τεχνολογίες (laser) για την εξουδετέρωση εναέριων στόχων. Πολλά από αυτά τα συστήματα, που παρουσιάζονται σε διεθνείς εκθέσεις όπλων (π.χ Eurosatory), χρησιμοποιούν κινητικούς μηχανισμούς θανάτωσης, όπως όπλα, πυραύλους ή συνδυασμό και των δύο. Για παράδειγμα, η κινεζική NORINCO έχει προσαρμόσει το ναυτικό οπλικό σύστημα εγγύς βολής LD-2000 (CIWS) [39] για χρήση κατά UAV, στοχεύοντας μη επανδρωμένα αεροσκάφη με διατομή ραντάρ τουλάχιστον 0,1m² σε περιβάλλοντα ηλεκτρονικών αντιμέτρων. Παρομοίως, η ευρωπαϊκή εταιρεία Thales προσφέρει το σύστημα RAPIDFire[40], το οποίο συνδυάζει αντιαεροπορικά

πυροβόλα και πυραύλους STARStreak για την αντιμετώπιση απειλών UAV χαμηλού κόστους, με δυνατότητα σμήνους.

Πέρα από τις κινητικές λύσεις, υιοθετούνται πιο καινοτόμες προσεγγίσεις, συμπεριλαμβανομένων των όπλων κατευθυνόμενης ενέργειας (DEW). Τα συστήματα αυτά, όπως τα μικροκύματα υψηλής ισχύος (HPM) και τα λέιζερ, αχρηστεύουν τα UAV στοχεύοντας τα εσωτερικά ηλεκτρονικά τους συστήματα. Η γερμανική εταιρεία Diehl Defense ανέπτυξε το HPEMcounterUAS, το οποίο χρησιμοποιεί παλμούς HPM για να καταστήσει τα μη επανδρωμένα αεροσκάφη μη λειτουργικά, ακόμη και όταν εμπλέκονται σε σμήνη. Τα συστήματα που βασίζονται σε λέιζερ κερδίζουν επίσης έδαφος- το Silent Hunter της NORINCO, που παρουσιάστηκε στην IDEX 2017, χρησιμοποιεί λέιζερ μεταβλητής ισχύος για να καταστρέψει μικρά UAV χαμηλού ύψους σε αποστάσεις έως και 2 χιλιόμετρα. Ομοίως, η ισραηλινή Rafael Advanced Systems διαθέτει στην αγορά το Iron Beam, ένα λέιζερ υψηλής ισχύος σχεδιασμένο για την αντιμετώπιση εναέριων απειλών μικρής εμβέλειας και πυροβολικού.

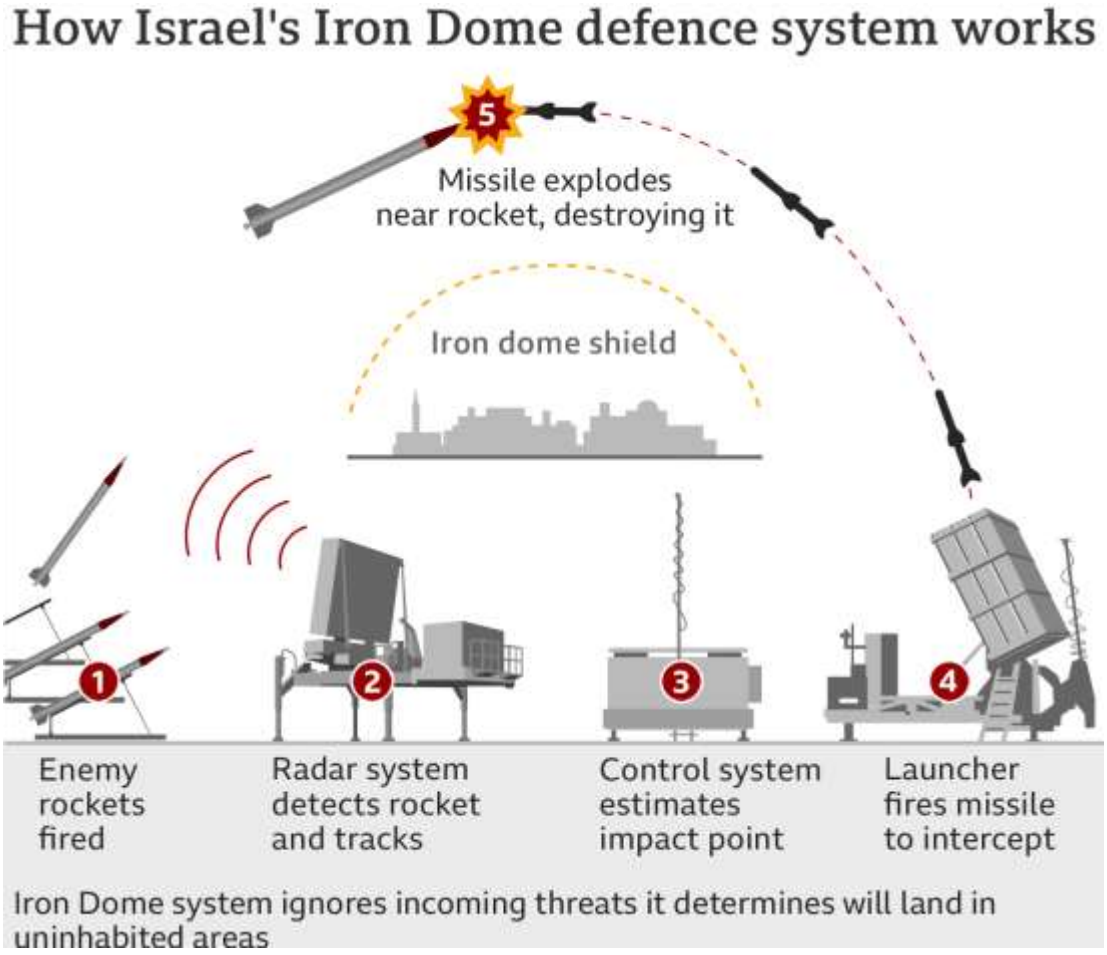
3 ΠΗΓΗ: https://armyrecognition.com/news/army-news/2023/defea-2023-soukos-robots-displays-minotaur-anti-drone-laser-weapon-systems

Τέλος, ειδική μνεία θα πρέπει να γίνει στο ελληνικής κατασκευαστής στρατιωτικό αμυντικό όχημα Μινώταυρος από την εταιρεία Soukos Robots, ένα σύστημα που έχει τη δυνατότητα να καταρρίπτει εχθρικά drones με laser. Το σύστημα έχει τη δυνατότητα να χτυπήσει στόχους σε απόσταση έως 80 χιλιόμετρα. Ο **Μινώταυρος** εκπέμπει μία δέσμη laser δημιουργώντας νέφος ιονισμού με αποτέλεσμα ότι εισέρχεται εντός της εμβέλειας να αναφλέγεται. Οι θερμοκρασίες που αναπτύσσονται εντός του «νέφους» ξεπερνούν τους 3.000 βαθμούς Κελσίου, ενώ η διάμετρος που δημιουργείται εντός του νέφος ιονισμού φτάνει τα 1.000 μέτρα.

Αυτές οι εξελίξεις καταδεικνύουν μια δυναμική αλλαγή στην τεχνολογία για την καταπολέμηση των UAV.

Anti-Drone Ασπίδα – Το Παράδειγμα του Iron Dome

Το Iron Dome είναι ένα από τα πιο προηγμένα συστήματα αντιπυραυλικής και αντι-drone άμυνας παγκοσμίως, σχεδιασμένο από την ισραηλινή εταιρεία Rafael Advanced Defense Systems σε συνεργασία με την Raytheon Technologies. Το σύστημα είναι σχεδιασμένο να εντοπίζει, να αναχαιτίζει και να εξουδετερώνει απειλές, όπως ρουκέτες, πυραύλους μικρού βεληνεκούς, όλμους (C-RAM), καθώς και πυραύλους κρουζ και μη επανδρωμένα αεροσκάφη (UAV). Σε λειτουργία από το 2011, ο Σιδηρούς Θόλος έχει αποδείξει σταθερά την αποτελεσματικότητά του αναχαιτίζοντας με επιτυχία πάνω από 5.000 πυραύλους με ποσοστό επιτυχίας που υπερβαίνει το 90%. Το σύστημα έχει σώσει αμέτρητες ζωές και έχει μειώσει σημαντικά τις υλικές ζημιές σε ζώνες συγκρούσεων [41].



ΠΗΓΗ: https://energiainteligenteufjf.com.br/tecnologia/dimensoes-da-tecnologia-nas-guerras

Τα βασικά χαρακτηριστικά του Iron Dome είναι:

- Ικανότητα πολλαπλών αποστολών: C-RAM, επιτρέποντας την προστασία τόσο των αναπτυγμένων δυνάμεων όσο και των κρίσιμων υποδομών.

- Προσαρμοστικότητα στις καιρικές συνθήκες: Λειτουργεί αξιόπιστα σε δυσμενείς καιρικές συνθήκες, όπως χαμηλά σύννεφα, βροχή, καταιγίδες σκόνης και ομίχλη.
- Ταυτόχρονη εμπλοκή: Δυνατότητα εντοπισμού και αναχαίτισης πολλαπλών απειλών ταυτόχρονα, εξασφαλίζοντας ολοκληρωμένη προστασία [42].
- Αποδοτικότητα κόστους: Η ικανότητά του να διακρίνει μεταξύ γνήσιων απειλών και μη κρίσιμων απειλών μειώνει τις περιττές εκτοξεύσεις αναχαιτιστών, μειώνοντας έτσι το λειτουργικό κόστος.
- Ευελιξία και κινητικότητα: Μπορεί να ενσωματωθεί σε διάφορες πλατφόρμες, συμπεριλαμβανομένων των φορτηγών και των πλοίων, και είναι μεταφερόμενο μέσω αεροσκαφών. Οι διαμορφώσεις περιλαμβάνουν το χερσαίο Iron Dome, το κινητό I-DOME και τη ναυτική παραλλαγή C-DOME.

Τα οφέλη που προκύπτουν από τη χρήσου συστήματος Iron Dome

- Τεχνολογία που σώζει ζωές: Το Iron Dome αναχαιτίζει τις εισερχόμενες απειλές και ελαχιστοποιεί τις απώλειες πολιτών και στρατιωτών [43].
- Προστασία των υποδομών: Αποτρέπει την πρόκληση ζημιών σε ζωτικά αστικά και βιομηχανικά περιουσιακά στοιχεία.
- Οικονομική αποδοτικότητα: Μειώνει τις περιττές δαπάνες πόρων μέσω της επιλεκτικής ανάπτυξης αναχαιτιστών.
- Επιχειρησιακή ευελιξία: Προσαρμόσιμη για αστική άμυνα, προωθημένες επιχειρησιακές βάσεις και κινητές δυνάμεις(I-DOME: A Mobile Variant).
- Επεκτασιμότητα και ενσωμάτωση: Μπορεί να ενσωματωθεί σε ευρύτερα δίκτυα αεράμυνας για ενισχυμένη πολυεπίπεδη προστασία.
- Παγκόσμια εφαρμογή: Αποδεδειγμένη απόδοση σε ποικίλα περιβάλλοντα το καθιστά πολύτιμο περιουσιακό στοιχείο για κάθε έθνος που αντιμετωπίζει εναέριες απειλές.

Συμπεράσματα

Η εξέλιξη του πολέμου έχει συνδεθεί άρρηκτα με την πρόοδο της τεχνολογίας (π.χ AI, ML) και τα UAVs αντιπροσωπεύουν μια από τις πιο σημαντικές καινοτομίες στον τομέα των σύγχρονων στρατιωτικών επιχειρήσεων. Από την αναγνώριση και την επιτήρηση έως τις στοχευμένες επιθέσεις, η χρήση των UAVs έχει αλλάξει ριζικά τη φύση της στρατιωτικής στρατηγικής, προσφέροντας αυξημένη ακρίβεια, χαμηλό κόστος, αποτελεσματικότητα και μείωση του κινδύνου για ανθρώπινες ζωές. Παράλληλα, η ανάπτυξη προηγμένων συστημάτων αεράμυνας, όπως το Iron Dome αποτελεί στρατηγική επένδυση για την ενίσχυση της εθνικής ασφάλειας κάθε χώρας. Παρά τις οικονομικές και τεχνικές προκλήσεις, η υιοθέτηση τέτοιων τεχνολογιών είναι απαραίτητη για την αντιμετώπιση των σύγχρονων απειλών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1 Ryan Bridley and Scott Pastor, https://smallwarsjournal.com/2022/08/19/, 2022
2 https://www.westernfrontassociation.com/world-war-i-articles/balloonatics-during-the-first-world-war-1914-1918/
3 "V-1 Cruise Missile." National Air and Space Museum, accessed June 11, 2022. https://airandspace.si.edu/collection-objects/v-1-cruise-missile/nasm_A19600341000.
4 Axe,D. (2021). Drone War Vietnam. Pen & Sword Books. https://books.google.gr/books?id=QwY0EAAAQBAJ
5 https://www.iwm.org.uk/history/a-brief-history-of-drones.
6 Aranzazu Suescun, Catalina & Cardei, Mihaela. (2016). Unmanned Aerial Vehicle Networking Protocols. 10.18687/LACCEI2016.1.S.078.
7 Finn, A., & Scheding, S. (2010). Developments and Challenges for Autonomous Unmanned Vehicles. Springer.
8 Manley, J. E. (2008). Unmanned Surface Vehicles, 15 Years of Development. Proceedings of the Association for Unmanned Vehicle Systems International.
9 https://www.navalnews.com/naval-news/2024/10/unmanned-surface-vehicles-usvs-as-both-game-changers-and-game-extenders/.
10 Todor Dimitrov, ASPECTS IN USAGE OF UNMANNED SURFACE VEHICLE IN UKRAINIAN WAR.
11 https://enterprise.dji.com/
12 Barnhart, R. K., Hottman, S. B., Marshall, D. M., & Shappee, E. (2012). Introduction to Unmanned Aircraft Systems. CRC Press.
13 https://www.thesoldiersproject.org/how-much-does-a-military-drone-cost/
14 Sönmez, Maria & Pelin, Cristina & Georgescu, Mihai & Pelin, George & Stelescu, Maria & Nituica (Vilsan), Mihaela & Stoian, George & Alexandrescu, Laurentia & Gurau, Dana. (2022). Unmanned Aerial Vehicles – Classification, Types of Composite Materials Used in Their Structure and Applications. 77-82. 10.24264/icams-2022.I.11.
15 Floreano, D., & Wood, R.J. (2015). Science, technology and the future of small autonomous drones. Nature, 521, 460-466.
16 https://www.uasolutions.ch/types-of-drones/
17 Meier, L., Tanskanen, P., Heng, L., Lee, G. H., Fraundorfer, F., & Pollefeys, M. (2015). PX4:A node-based multithreaded open source robotics framework for deeply embedded platforms. In 2015 IEEE International Conference on Robotics and Automation (ICRA) (pp. 6235-6240). IEEE.
18 Kochenderfer, M. J., Wheeler, T. A., & Wray, K. H. (2016). Algorithms for decision making. MIT Press.
19 Huang, H., Wang, L., & Li, Q. (2018). RTK-GPS and its application in precision agriculture. In 2018 International Conference on Machine Learning and Cybernetics (ICMLC) (pp. 200-205). IEEE.
20 Barnhart, R. K., Hottman, S. B., Marshall, D. M., & Shappee, E. (2012). Introduction to Unmanned Aircraft Systems. CRC Press.
21 Cheung, T. M. (2015). China's Drones:Airspace Dominance in the 21st Century. Journal of Strategic Studies, 38(5), 621-645.
22 Gunes, M. (2020). Turkey's Bayraktar TB2 and the Future of Drone Warfare. Middle East Policy, 27(4), 156-162.
23 Bendett, S. (2018). Russia's Military Drones A New Capability for the Kremlin's War Machine. War on the Rocks. Available at https://warontherocks.com.
24 Bock, P., & Kreps, S. (2015). The Rise of Drones in Israeli Military Strategy. Middle East Journal, 69(3), 359-375.
25 https://dronewars.net/who-has-armed-drones/
26 https://www.eurocontrol.int/system/satellite-communications-datalink
27 https://en.wikipedia.org/wiki/Radio_frequency
28 https://netlinetech.com/how-drones-are-being-controlled-and-the-way-to-neutralise-them/
29 Lin X, Yajnanarayana V, Muruganathan SD, Gao S, Asplund H, Maattanen HL, Bergstrom M, Euler S, Wang YPE (2018) The sky is not the limit:LTE for unmanned aerial vehicles. IEEE Commun Mag 56(4):204–210
30 Qazi S, Siddiqui AS, Wagan AI (Dec 2015) UAV based real time video surveillance over 4G LTE. In 2015 international conference on open source systems & technologies (ICOSST). IEEE, New York, pp 141–145
31 Nguyen HC, Amorim R, Wigard J, Kovacs IZ, Mogensen P (Sept 2017) Using LTE networks for UAV command and control link: a rural-area coverage analysis. In 2017 IEEE 86th vehicular tech-nology conference (VTC-Fall). IEEE, New York, pp 1–6
32 Guillen-Perez A, Sanchez-Iborra R, Cano MD, Sanchez-Aarnoutse JC, Garcia-Haro J (Nov 2016) WiFi networks on drones. In 2016 ITU kaleidoscope:ICTs for a sustainable world (ITU WT). IEEE,New York, pp 1–8
33 Jang JS, Liccardo D (2007) Small UAV automation using MEMS. IEEE Aerosp Electron Syst Mag 22(5):30–34
34 Kunertova Dominika (2023), The war in Ukraine shows the game-changing effect of drones depends on the game. ETH Zurich
35 Shahed Aviation Industries Research Center. (2022). Shahed-136 Tactical Specifications and Use in Modern Warfare. Journal of Advanced Military Systems.
36 United Nations Institute for Disarmament Research (UNIDIR). (2023). Drones in Conflict Zones:A Case Study of the Russia-Ukraine War. Geneva:UNIDIR Publications.

37	Cosar, M. (2022). Cyber Attacks on Unmanned Aerial Vehicles and Cyber Security Measures. The Eurasia Proceedings of Science Technology Engineering and Mathematics
38	Kobaszyńska-Twardowska, Anna & Łukasiewicz, J. & Sielicki, Piotr. (2022). Risk Management Model for Unmanned Aerial Vehicles during Flight Operations. Materials. 15. 2448. 10.3390/ma15072448.
39	http://www.armyguide.com/eng/product4174.html
40	https://www.thalesgroup.com/en/markets/defence-and-security/naval-forces/above-water-warfare/rapidfire
41	Rafael Advanced Defense Systems. (2021). Iron Dome:Multi-Mission Defense System. Available at https://www.rafael.co.il
42	Middle East Policy Council. (2020). The Strategic Role of the Iron Dome in Israel's Defense Strategy. Available at:https://www.mepc.org
43	Bendett, S. (2018). Russia's Military Drones:A New Capability for the Kremlin's War Machine. War on the Rocks. Available at https://warontherocks.com

Βιογραφικό Συντακτών

Ο Ιωάννης Σοφράς είναι απόφοιτος του τμήματος Ηλεκτρονικών Μηχανικών Τ.Ε της σχολής Τεχνολογικών Εφαρμογών του ΑΤΕΙ Πειραιά (2014). Είναι κάτοχος Μεταπτυχιακών Διπλωμάτων στις «Ψηφιακές Επικοινωνίες και Δίκτυα» του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς (2018), στην «Κρυπτογραφία, Ασφάλεια και Συστήματα Πληροφοριών» του τμήματος Στρατιωτικών Επιστημών της Στρατιωτικής Σχολής Ευελπίδων (2024), και κάτοχος Διπλώματος MicroMaster in CyberSecurity από το Rochester Institute of Technology (2017), καθώς και πιστοποιήσεων εξειδίκευσης. Είναι φοιτητής στο πρόγραμμα «Executive MBA» της Σχολής Οικονομικών και Πολιτικών Επιστημών, του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών (2024-2025). Εργάζεται επι μια δεκαετία ως Μηχανικός Κυβερνοασφάλειας & Ασφάλειας Πληροφοριών στον Τραπεζικό Τομέα.

Ο Ευάγγελος Γκούμας είναι απόφοιτος του τμήματος Μαθηματικών του Πανεπιστημίου Πατρών και είναι κάτοχος μεταπτυχιακού διπλώματος στην "Κρυπτογραφία, Ασφάλεια και Συστήματα Πληροφοριών" από τη Στρατιωτική Σχολή Ευελπίδων. Από το 2023, είναι διδακτορικός φοιτητής και μέλος της ομάδας Cryptography and Complexity Theory στο Τεχνολογικό Πανεπιστήμιο του Darmstadt στη Γερμανία, εστιάζοντας στην κβαντική κρυπτογραφία.

ΣΤΡΑΤΙΩΤΙΚΕΣ ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΕΠΑΥΞΗΜΕΝΗΣ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑΣ

Γεώργιος Σπύρου, Σμρος ΠΝ

Ιστορική αναδρομή

Η επαυξημένη πραγματικότητα (AR – Augmented Reality) αποτελεί συνέχεια της εικονικής πραγματικότητας (VR-Virtual Reality). Η ιστορία της ξεκινά το 1901, όταν πρώτος ο Frank Baum διατύπωσε μια ιδέα για το τι είναι η AR. Η ιδέα αυτή αφορούσε ένα είδος ηλεκτρονικών γυαλιών (Character Markers) που θα πρόβαλαν δεδομένα στον πραγματικό κόσμο [1] . Αξιοσημείωτα ορόσημα στην ιστορία της AR αποτελούν τα ακόλουθα:

- Το 1968 οι Ivan Sutherland και David Evans δημιούργησαν το Sword of Damocles. Πρόκειται για μια τρισδιάστατη συσκευή απεικόνισης που τοποθετείται στο κεφάλι του χρήστη, με σκοπό να επαυξήσει τη σκηνή με τρισδιάστατες πληροφορίες. Πετύχαινε με αυτό τον τρόπο να παρουσιάζει στον χρήστη μια εικόνα η οποία αλλάζει καθώς το κεφάλι του ή κινείται σε μια περιοχή.
- Το 1980 ο Steve Mann δημιούργησε το EyeTap. Το EyeTap ήταν η πρώτη κατασκευή που διέθετε υπολογιστικό σύστημα όρασης με κείμενο και γραφικές επικαλύψεις σε AR.

Εικόνα 1: Το EyeTap (αριστερή εικόνα) και Sword of Damocles (δεξιά εικόνα)

- Το 1992 οι Steven Feiner, Blair MacIntyre και Doree Seligmann παρουσίασαν το πρώτο άρθρο πάνω σε σύστημα AR. Το σύστημα ονομαζόταν KARMA (Knowledge-based Augmented Reality Maintenance Assistance) και χρησιμοποιούσε σύστημα HMD (head-mounted display) για την υποβοήθηση του χρήστη κατά τη συντήρηση ενός εκτυπωτή laser.

- Το 1995 ο Jun Rekimoto αναπτύσσει το πρώτο φορητό AR, το NaviCam, μια συσκευή που διαθέτει αναγνώριση markers και σχολιασμό του πραγματικού κόσμου
- Το 1999 η εταιρεία Total Immersion παρουσίασε το πρώτο λογισμικό για την ανάπτυξη εφαρμογών με υποστήριξη AR, το D'Fusion Studio. Την ίδια χρονιά δημιουργήθηκε η open-source βιβλιοθήκη AR από τον Hirokazu Kato, η ARToolKit. Αποτελεί τη βάση για πολλές εφαρμογές επαυξημένης πραγματικότητας και χρησιμοποιείται μέχρι και σήμερα.
- Το 2001 δημιουργήθηκε από τους Bob Kooper και Blair MacIntyre το πρώτο πρόγραμμα περιήγησης επαυξημένης πραγματικότητας, το Real-World Wide Web (RWWW), που υπερθέτει δεδομένα από τον Παγκόσμιο Ιστό στον πραγματικό κόσμο μέσω μιας HMD [2].
- Το 2010 η Microsoft δημιούργησε την Kinect, μια συσκευή που αποτέλεσε η βάση για την ανάπτυξη βιντεοπαιχνιδιών AR.
- Το 2015 η Microsoft δημιούργησε τη συσκευή Hololens η οποία συνδυάζει την VR και την AR. Η συσκευή είναι ένας ολοκληρωμένος υπολογιστής κι έχει πολλούς αισθητήρες.

Εικόνα 2: Η συσκευή Hololens της Microsoft (2015)

Ορισμός - Χαρακτηριστικά

Υπάρχουν πολλοί ορισμοί για την AR. Σύμφωνα με τον Tom Caudell: «Η AR είναι η αλληλεπίδραση των πολύ βελτιωμένων γραφικών, του ήχου κι άλλων αισθήσεων σ' ένα πραγματικό περιβάλλον και σε πραγματικό χρόνο» [3].

Επίσης ο Ronald Azuma ανέφερε ότι: «Η AR είναι μια παραλλαγή της εικονικής πραγματικότητας, αλλά δεν θα πρέπει να τις συγχέουμε, διότι η επαυξημένη συμπληρώνει τον πραγματικό κόσμο και δεν τον υποκαθιστά» [4].

Γενικότερα, η AR αποτελεί μια καινοτόμα ιδέα πάνω στα υπολογιστικά γραφικά. Όπως αναφέρεται και στην ονομασία της, η AR «επαυξάνει» πληροφορίες, δηλαδή δεν υποκαθιστά το πραγματικό περιβάλλον, αλλά το ενισχύει. Εμπλουτίζει τις ανθρώπινες αισθήσεις προσθέτοντας εικονικές πληροφορίες στον πραγματικό κόσμο με τη βοήθεια του υπολογιστή.

Σύμφωνα, λοιπόν, με όλα αυτά, την AR την καθορίζουν τρία βασικά χαρακτηριστικά:

- Συνδυάζει τον πραγματικό με τον εικονικό κόσμο
- Είναι διαδραστική σε πραγματικό χρόνο

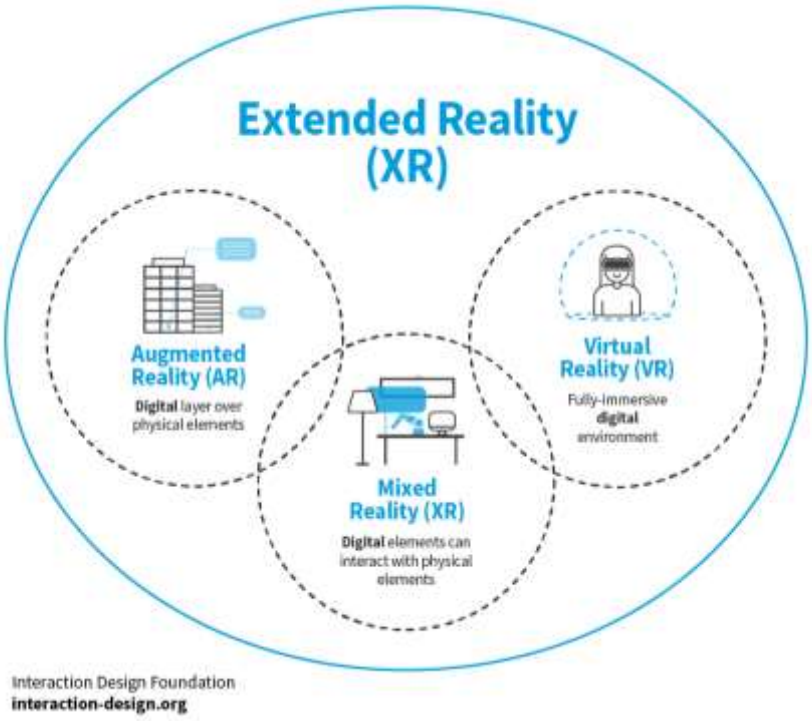
- Η πληροφορία καταχωρείται σε τρεις διαστάσεις.

Παρότι η AR αποτελεί σχετικά νέα τεχνολογία και δεν έχει γίνει αναλυτική περιγραφή των χαρακτηριστικών μιας AR εφαρμογής, μπορούμε να συμφωνήσουμε ότι τα πιο βασικά της χαρακτηριστικά μιας τέτοιας εφαρμογής είναι η διάδραση και η αλληλεπίδρασή μεταξύ:

- Χρήστη και εφαρμογής AR
- Χρηστών της εφαρμογής
- Εικονικού και πραγματικού περιβάλλοντος
- Χρήστη και εικονικού περιβάλλοντος
- Χρήστη και πραγματικού περιβάλλοντος

Το φάσμα της Εκτεταμένης Πραγματικότητας

Ο όρος της εκτεταμένη πραγματικότητα (Extended Reality – XR) χρησιμοποιείται για να καλύψει ένα ευρύ φάσμα «τεχνολογιών που τροποποιούν την πραγματικότητα προσθέτοντας ψηφιακά στοιχεία στο φυσικό ή πραγματικό περιβάλλον σε οποιονδήποτε βαθμό, θολώνοντας τη γραμμή μεταξύ του φυσικού και του ψηφιακού κόσμου» [5]. Η εκτεταμένη πραγματικότητα περιλαμβάνει την εικονική, την επαυξημένη και τη μικτή πραγματικότητα (Mixed Reality – MR) καθώς και κάθε άλλη τεχνολογία του ιδίου φάσματος, ακόμη κι αν δεν έχει αναπτυχθεί ακόμη.



Εικόνα 3: Το φάσμα της XR

Με την εικονική πραγματικότητα επιτυγχάνεται η αντικατάσταση του πραγματικού περιβάλλοντος του χρήστη, με ένα εικονικό που παράγεται και ελέγχεται πλήρως από τον υπολογιστή, δημιουργώντας έτσι την ψευδαίσθηση στους χρήστες ότι βρίσκονται σε πραγματικό κόσμο. Για τη δημιουργία μιας ρεαλιστικής εικονικής σκηνής, απαιτείται υψηλό επίπεδο λεπτομέρειας στα γραφικά και η απεικόνισή της να γίνεται σε πραγματικό χρόνο.

Αντίστοιχα, η επαυξημένη πραγματικότητα έχει σαν στόχο την επαύξηση (όχι αντικατάσταση) των στοιχείων του πραγματικού περιβάλλοντος, μέσω της χρήσης αισθητήρων ήχου, εικόνας, βίντεο και άλλων πολυμέσων, με συνθετικές πληροφορίες παραγόμενες από ένα υπολογιστικό σύστημα. Με τον τρόπο αυτό, τα στοιχεία του πραγματικού περιβάλλοντος δεν αποκρύπτονται εντελώς, αλλά εμπλουτίζονται με εικονικά στοιχεία. Τα εικονικά αντικείμενα δεν απαιτούν απαραίτητα υψηλά επίπεδα γραφικών. Η ρεαλιστικότητά τους περιορίζεται μόνο από τις παραμέτρους της εφαρμογής

Τέλος, η μικτή πραγματικότητα λειτουργεί όπως η AR, με το επιπλέον χαρακτηριστικό ότι μια αλληλεπίδραση του χρήστη με ένα φυσικό αντικείμενο είναι δυνατό να φέρει μια αλλαγή σε κάποια ψηφιακό αντικείμενο. Θα μπορούσαμε να πούμε ότι η μικτή πραγματικότητα έχει σαν στόχο την ανάμειξη του φυσικού με τον πραγματικό κόσμο, σε έναν ενιαίο κόσμο.

Παραδείγματα Μη Στρατιωτικών Εφαρμογών

Η εφαρμογή Pokémon Go το 2016 έφερε την AR στα κινητά ενός πολύ μεγάλου αριθμού του ανθρώπινου πληθυσμού. Ακόμη, AR συναντά κανείς πλέον και στην κατηγορία των social media, σε εφαρμογές όπως το Instagram και το Snapchat.

Η τεχνολογία AR όμως είναι πολύ μεγαλύτερη από αυτή των εφαρμογών κοινωνικής δικτύωσης και των παιχνιδιών, με πολλές χρήσεις σε βιομηχανικούς και εκπαιδευτικούς τομείς, την αρχαιολογία, τον τουρισμο, την ιατρική, μέχρι και σε στρατιωτικούς τομείς. Ορισμένα παραδείγματα μη στρατιωτικών εφαρμογών της AR είναι τα παρακάτω:

Αρχαιολογία

Στον τομέα της αρχαιολογίας, η AR χρησιμοποιείται με σκοπό την ενίσχυση των αρχαιολογικών ερευνών[6]. Για παράδειγμα, το VITA (Visual Interaction Tool for Archaeology) αποτελεί μια αρχαιολογική εφαρμογή που χρησιμοποιεί την AR, για να επιτρέψει σε αρχαιολόγους να επεξεργαστούν και να μελετήσουν τα αποτελέσματα ανασκαφών από το σπίτι ή το εργαστήριο, χωρίς να απαιτείται η παρουσίαση τους στον χώρο των ανασκαφών [7].

Βιομηχανία

Στον τομέα της βιομηχανίας κατά την εκτέλεση των εργασιών συντήρησης και επισκευής των μηχανημάτων, ορισμένες εταιρείες δίνουν στο τεχνικό προσωπικό τους εξοπλισμό με τεχνολογίες AR. Πρόκειται για ακουστικά και γυαλιά AR, τα οποία δίνουν

συγκεκριμένες οδηγίες και δύνανται να επισημαίνουν πιθανές διορθώσεις και περιοχές που μπορεί να περιέχουν προβλήματα [8].

Εκπαίδευση

Η χρήση της Η/Υ, διαδραστικών πινάκων και διαδικτυακών αιθουσών έχει γίνει ευρέως διαδεδομένη σε πολλά σχολεία και εκπαιδευτικά ιδρύματα. Η τελευταία τάση είναι οι καθηγητές και οι εκπαιδευτικοί να «επαυξάνουν» την μαθησιακή εμπειρία του μαθητή με τη χρήση εφαρμογών AR. Για παράδειγμα, η εφαρμογή Aurasma χρησιμοποιείται σε αίθουσες διδασκαλίας, έτσι ώστε οι μαθητές να μπορούν να μάθουν νέα πράγματα αλληλοεπιδρώντας με τα εικονικά αντικείμενα που εμφανίζονται από την εφαρμογή [8].

Επιχειρήσεις (Logistics)

Το AR παρουσιάζει μια ποικιλία ευκαιριών για την αύξηση της αποδοτικότητας και της εξοικονόμησης κόστους σε πολλούς τομείς της επιχειρηματικής εφοδιαστικής. Η εταιρεία DHL για παράδειγμα δίνει στους υπαλλήλους αποθηκών της «έξυπνα» γυαλιά με τεχνολογία AR, οι φακοί των οποίων εμφανίζουν στους εργαζόμενους τη συντομότερη διαδρομή που πρέπει να ακολουθήσουν μέσα σε μια αποθήκη, για να εντοπίσουν ένα συγκεκριμένο αντικείμενο [8].

Ιατρική

Από τη λειτουργία του εξοπλισμού μαγνητικής τομογραφίας μέχρι την εκτέλεση πολύπλοκων χειρουργικών επεμβάσεων, η τεχνολογία AR έχει τη δυνατότητα να ενισχύσει το βάθος και την αποτελεσματικότητα της ιατρικής εκπαίδευσης. Φοιτητές ιατρικής μπορούν να χρησιμοποιήσουν τεχνολογία AR, για να πραγματοποιήσουν μια χειρουργική επέμβαση σε ελεγχόμενο περιβάλλον, μειώνοντας τα ποσοστά κινδύνου κατά την εκπαίδευση των εν δυνάμει χειρουργών [8].

Τουρισμός

Η τεχνολογία AR μπορεί να χρησιμοποιηθεί σε έναν αρχαιολογικό χώρο με την επαύξηση οθονών ή εκθεμάτων με την βοήθεια ενός smartphone. Στο εξωτερικό περιβάλλον, τα αξιοθέατα μπορούν να επικαλυφθούν από εικονικές πληροφορίες χρησιμοποιώντας τεχνολογία ΕΠ και με μία κινητή συσκευή που διαθέτει κάμερα οι τουρίστες έχουν την δυνατότητα να περιηγηθούν σε ιστορικούς χώρους και να ενημερωθούν για τα γεγονότα και τα αξιοθέατα που βλέπουν μέσω αυτών των εικονικών πληροφοριών. Παράδειγμα μιας τέτοιας εφαρμογής αποτελεί η Archeoguide [6].

Παραδείγματα Στρατιωτικών Εφαρμογών

Εκπαίδευση (εξομοιώσεις - προσομοιώσεις)

Η χρήση του AR στη στρατιωτική εκπαίδευση φαίνεται ιδιαίτερα αποτελεσματική στην προετοιμασία των στρατιωτών για σενάρια πραγματικού κόσμου. Οι εφαρμογές AR προσομοιώνουν σενάρια μάχης, αστικούς πολέμους και περίπλοκα περιβάλλοντα αποστολών επιτρέποντας στους στρατιωτικούς να συμμετέχουν σε ρεαλιστικές και διαδραστικές ασκήσεις εκπαίδευσης. Μεταξύ άλλων, οι στρατιώτες μπορούν να

εξασκηθούν στη λήψη αποφάσεων υπό πίεση, τους τακτικούς ελιγμούς και την ομαδική εργασία, ενώ λαμβάνουν ανατροφοδότηση σε πραγματικό χρόνο. Τέλος, η εκπαίδευση με χρήση της AR ελαχιστοποιεί τους κινδύνους και το κόστος σε σχέση με τις πραγματικές ασκήσεις.

Εικόνα 4: Ομαδική εικονική μάχη και χειριστής

Εφαρμογές προσομοιώσεων χρησιμοποιούν, όλοι οι κλάδοι των ενόπλων δυνάμεων των Η.Π.Α. Ο στρατός ξηράς για παράδειγμα, χρησιμοποιεί την τεχνολογία της εικονικής πραγματικότητας, για να προετοιμάσει τους στρατιώτες για αποστολές σε συγκεκριμένες περιοχές, όπως το Αφγανιστάν. Οι στρατιώτες μπορούν να προετοιμάζονται για την εκτέλεση των αποστολών τους, δοκιμάζοντας όλα όσα έχουν μάθει, σε μια εφαρμογή AR η οποία αναπαριστά πιστά την τοποθεσία της περιοχής στην οποία πρόκειται να επιχειρήσουν. Σύμφωνα με πολλά ερευνητικά δεδομένα, οι εκπαιδευόμενοι μπορούν να μαθαίνουν να διαχειρίζονται αποτελεσματικά το άγχος τους και να έχουν βέλτιστα αποτελέσματα, όταν εξασκούνται σε εικονικά περιβάλλοντα [9]. Ακόμη, υπάρχουν και παραδείγματα χρήσης της εικονικής πραγματικότητας από την πολεμική αεροπορία, όπως οι προσομοιωτές πτήσης.

Παρότι οι περιπτώσεις χρήσης της AR μπορεί να διαφέρουν για κάθε σώμα και οι εφαρμογές της μπορεί ακόμα να μην έχουν αναπτυχθεί πλήρως, δεν υπάρχουν αμφιβολίες ότι η AR πρόκειται για μια τεχνολογία που θα αλλάξει ριζικά τον τρόπο λειτουργίας του αμυντικού τομέα στο άμεσο μέλλον.

Τηλεπαρουσία

Για να μειωθούν οι κίνδυνοι που ενέχει η φυσική παρουσία στρατιωτικού προσωπικού σε συγκεκριμένες τοποθεσίες, αναπτύχθηκαν εφαρμογές τηλεπαρουσίας. Οι πολεμικές επιχειρήσεις είναι εξαιρετικά επικίνδυνες, δεδομένου ότι το προσωπικό είναι πολλές φορές εκτεθειμένο σε εχθρικά πυρά, κινδύνους από νάρκες, παγίδες κ.ο.κ.. Για την αποφυγή τραυματισμών και απωλειών, δημιουργήθηκαν οχήματα απομακρυσμένης λειτουργίας όπως τα drones.

Ένα drone τηλεχειρίζεται από κάποιον χειριστή που δεν βρίσκεται επί του σκάφους. Τα τελευταία χρόνια, τα drones έχουν αποδειχθεί ανεκτίμητο εργαλείο για στρατιωτικές επιχειρήσεις. Με το κατάλληλο λογισμικό AR τα drone μπορούν να μετατραπούν σε ένα υπέρτατο εργαλείο επιτήρησης, παρέχοντας σε πραγματικό χρόνο τη δυνατότητα αναγνώρισης αντικειμένων και δημιουργίας εξελιγμένου συστήματος παρακολούθησης ανθρώπων, αντικειμένων και στρατιωτικών οχημάτων.

Παράδειγμα Heads-Up Display (HUD) για πιλότους

Επαύξηση πληροφορίας - AR για πλοήγηση

Το Heads-Up Display (HUD) είναι το τυπικό παράδειγμα χρήσης της τεχνολογίας AR για στρατιωτικές εφαρμογές της αεροπορίας. Τα κράνη των πιλότων διαθέτουν μια διάφανη οθόνη, η οποία εμφανίζει εικονικές πληροφορίες σε επικάλυψη με το

πραγματικό περιβάλλον. Για πολλά χρόνια, τα στρατιωτικά αεροσκάφη και ελικόπτερα χρησιμοποιούσαν HUDs και στο κράνος (Helmet Mounted Sights-HMS), ώστε να υπερθέσουν διανυσματικά γραφικά στο οπτικό πεδίου του πιλότου. Εκτός από την παροχή βασικών πληροφοριών πτήσης και πλοήγησης, τα γραφικά αυτά πολλές φορές καταγράφουν το περιβάλλον, παρέχοντας έναν τρόπο στόχευσης των όπλων του αεροσκάφους. Για παράδειγμα, ο πυργίσκος σε ένα πολεμικό ελικόπτερο μπορεί να είναι συνδεδεμένος με την οθόνη που προσαρμόζεται στο κράνος του πιλότου, έτσι ώστε να μπορεί να στοχεύει με το πυροβόλο απλά κοιτάζοντας το στόχο [10].

Οι Head-Mounted Displays (HMDs) χρησιμοποιούνται κυρίως από τα στρατεύματα εδάφους, με σκοπό να τους παρέχουν κρίσιμες πληροφορίες, σχετικές με το πλησίον περιβάλλον και τη θέση του εχθρού [8]. Χρησιμοποιώντας λύσεις AR, τα στρατεύματα μπορούν να έχουν πρόσβαση σε διαδραστικούς χάρτες και ενδείξεις πλοήγησης απευθείας μέσα στο οπτικό τους πεδίο. Τα τοπογραφικά δεδομένα και οι συντεταγμένες GPS, υπερτίθενται στο πραγματικό περιβάλλον, βοηθώντας τους στρατιώτες στην ακριβή πλοήγηση, την αναγνώριση στόχων και τον σχεδιασμό της αποστολής.

Επίγνωση της κατάστασης και οπτικοποίηση δεδομένων

Η επίγνωση της κατάστασης είναι μια κρίσιμη πτυχή των στρατιωτικών επιχειρήσεων. Η χρήση τεχνολογίας AR μπορεί να βοηθήσει τους στρατιώτες να κατανοήσουν καλύτερα το περιβάλλον τους επικαλύπτοντας κρίσιμες πληροφορίες, όπως δεδομένα εδάφους, εχθρικές θέσεις και θέσεις φιλικών στρατευμάτων, στο οπτικό τους πεδίο. Οι εφαρμογές επαυξημένης πραγματικότητας παρέχουν ενημερώσεις και ευφυΐα σε πραγματικό χρόνο, βελτιώνοντας την ικανότητα των διοικητών να λαμβάνουν ενημερωμένες αποφάσεις γρήγορα. Αυτή η βελτιωμένη επίγνωση της κατάστασης εξασφαλίζει ταχύτερη απόκριση στις μεταβαλλόμενες συνθήκες, μειώνοντας την ευπάθεια στο πεδίο της μάχης.

Στόχευση και χτυπήματα ακριβείας

Η τεχνολογία AR έχει επαναστατήσει τον τρόπο στόχευσης και την ακρίβεια στα χτυπήματα ακριβείας του αυστραλιανό στρατό. Οι εφαρμογές AR επιτρέπουν στους στρατιώτες να εγκλωβίζουν στόχους με ακρίβεια και αποτελεσματικότητα, μειώνοντας τις παράπλευρες ζημιές και ελαχιστοποιώντας τους κινδύνους για τους αμάχους. Τα συστήματα εγκλωβισμού στόχων που βασίζονται σε AR μπορούν επίσης να ενσωματώνουν δεδομένα από αισθητήρες που βρίσκονται σε drones και άλλες επιχειρησιακές μονάδες, παρέχοντας μια ολοκληρωμένη εικόνα του πεδίου της μάχης και ενισχύοντας την αποτελεσματικότητα των βολών.

Εφαρμογές εκπαίδευσης στρατιωτικών ιατρών

Η εκπαίδευση και η συντήρηση των δεξιοτήτων του στρατιωτικών ιατρών και νοσηλευτών, οι οποίοι θα παρέχουν βοήθεια σε τραυματίες στο πεδίο της μάχης, είναι ιδιαίτερης σημασίας για τις ένοπλες δυνάμεις. Παρότι οι εκπαιδευτές αυτών των ομάδων είναι εξαιρετικοί, οι προσομοιώσεις των τραυμάτων στο πεδίο της μάχης είναι απλές και στατικές όπως για παράδειγμα ένα κομμάτι ταινίας με εγγεγραμμένο τον τύπο του τραύματος, χωρίς φυσική αναπαράσταση του ίδιου του τραύματος.

Με τη χρήση της AR, ειδικά μετά την έκρηξη στα φορητά ακουστικά AR, μπορεί να επέλθει ριζική αλλαγή στον τρόπο με τον οποίο συμβαίνει σήμερα η εκπαίδευση Tactical Combat Casualty Care (TC3). Σε μια άσκηση, καθώς ένας ασκούμενος πλησιάζει έναν τραυματία θα βλέπει μια προσομοίωση πληγής να προβάλλεται σε αυτόν. Ταυτόχρονα, μέσω των ακουστικών AR, θα ακούει την απόκριση των τραυματιών [11]. Έτσι, τα εργαλεία AR προσφέρουν ένα νέο και δυνητικά πολύτιμο εργαλείο για την εκπαίδευση των στρατιωτικών ιατρών και νοσηλευτών μέσω της οπτικής και ακουστικής αναπαράστασης σε αυτούς των πληγών και της απόκρισης του τραυματία, ενώ εξακολουθούν να βρίσκονται και να λειτουργούν σε πραγματικό περιβάλλον.

Συμπεράσματα

Η επαυξημένη πραγματικότητα αποτελεί ένα τεχνολογικό επίτευγμα, το οποίο ήδη έχει επεκταθεί σε πολλούς τομείς της ανθρώπινης καθημερινότητας. Πέραν όμως των εφαρμογών που έχει η τεχνολογίας στην καθημερινότητα και την εργασία των ανθρώπων, ιδιαίτερο ενδιαφέρον παρουσιάζουν οι προοπτικές της στην αμυντική βιομηχανία. Σύγχρονες ένοπλες δυνάμεις, όπως των ΗΠΑ, έχουν ήδη αρχίσει να εκμεταλλεύονται τα οφέλη της AR, κάτι που αναμένεται να ακολουθήσουν αρκετές χώρες τα επόμενα χρόνια.

ΑΝΑΦΟΡΕΣ

1	Frank Baum. (1996). The Master Key. Project Gutenberg. https://www.gutenberg.org/ebooks/436
2	Oxford Economis. (2001). AVIATION: The Real World Wide Web (RWWW)
3	Cassella , D. (2009). Digital Trends. https://www.digitaltrends.com/gaming/what-is-augmented-reality-iphone-apps-games-flash-yelp-android-ar-software-and-more
4	Azuma, R., Baillot, Y., Behringer, R., Feiner, S., Julier, S., & MacIntyre, B. (2001). Recent advances in augmented reality. IEEE Computer Graphics and Applications, 21(6), 34–47. https://doi.org/10.1109/38.963459
5	Tremosa, L. (2023). Beyond AR vs. VR: What is the Difference between AR vs. MR vs. VR vs. XR?. Interaction Design
6	V. Vlahakis (2002), "Archeoguide: An Augmented Reality Guide for Archaeological Sites" in IEEE Computer Graphics and Applications, vol. 22, no. 05, pp. 52-60, 2002. doi: 10.1109/MCG.2002.1028726
7	Benko H., Ishak E.W., Feiner S., (2004), “VITA: visual interaction tool for archaeology (demo)”, In Proceedings of the 2004
8	Arnaldi B., Guitton P., Moreau G., (2018), “Virtual reality and augmented reality myths and realities”, Newark John Wiley & Sons Ann Arbor, Michigan Proquest, pp. 1-60.
9	Bouchard, S., Guitard, T., Bernier, F., & Robillard, G. (2011). Virtual Reality and the Training of Military Personnel to Cope with Acute Stressors. In Studies in computational intelligence (pp. 109–128). https://doi.org/10.1007/978-3-642-17824-5_6
10	Wanstall, B. (1989). HUD on the Head for Combat Pilots. Interavia, 44, pp. 334-338.

11 Taylor, G., Deschamps, A., Tanaka, A., Nicholson, D., Bruder, G., Welch, G., & Guido-Sanz, F. (2018). Augmented reality for tactical combat casualty care training. In Lecture notes in computer science (pp. 227–239). https://doi.org/10.1007/978-3-319-91467-1_19

12 Γκουρουμπίνου, Α.-Μ. (2018). Εικονική vs επαυξημένη πραγματικότητα. http://repository.teiwest.gr/xmlui/handle/123456789/6828

13 Sutherland, I. E. (1968, December). A head-mounted three dimensional display. In Proceedings of the December 9-11, 1968, fall joint computer conference, part I (pp. 757-764). https://dl.acm.org/doi/pdf/10.1145/1476589.1476686.

14 Tremosa, L. (2023, July 25). Beyond AR vs. VR: What is the Difference between AR vs. MR vs. VR vs. XR?. Interaction Design

15 Yardley, R. J., Thie, H. J., Schank, J. F., Galegher, J., & Riposo, J. (2003). Use of Simulation for Training in the U.S. Navy Surface Force. RAND NATIONAL DEFENSE RESEARCH INSTITUTE. https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1770.pdf

Βιογραφικό συντάκτη

Ο Σημαιοφόρος Γεώργιος Σπύρου ΠΝ γεννήθηκε στο Μαρούσι Αττικής το 1999. Φοίτησε στη Σχολή Ναυτικών Δοκίμων και ονομάστηκε Σημαιοφόρος το 2021. Υπηρέτησε αρχικά στη Φ/Γ Ύδρα και τη Φ/Γ Ψαρά της Διοίκησης Φρεγατών. Στη συνέχεια διετέλεσε επιτελής στο Αρχηγείο Στόλου. Φοίτησε στο Τμήμα Αναλυτών / Προγραμματιστών της Σχολής Προγραμματιστών Ηλεκτρονικών Υπολογιστών του Στρατού Ξηράς, από το οποίο αποφοίτησε επιτυχώς το 2024.

ΠΛΕΥΡΙΚΗ ΚΙΝΗΣΗ: ΤΕΧΝΙΚΕΣ, ΜΕΘΟΔΟΛΟΓΙΕΣ ΚΑΙ ΒΕΛΤΙΣΤΕΣ ΠΡΑΚΤΙΚΕΣ ΑΜΥΝΑΣ

Διονύσιος Τσίπας, Υπολοχαγός(ΠΖ)

Εισαγωγή

Στη σύγχρονη εποχή, ο ολοένα και αυξανόμενος βαθμός συνδεσιμότητας και η μαζική παραγωγή δεδομένων έχουν καταστήσει πολυπλοκότερα, αλλά και πιο ευάλωτα τα δίκτυα των επιχειρήσεων και των οργανισμών. Με την εμφάνιση του Internet of Things (IoT) και την εξάπλωση των διασυνδεδεμένων συσκευών, τα δεδομένα παράγονται από διαφορε- τικές πηγές, δημιουργώντας ένα δυναμικό αλλά και διασυνδεδεμένο ψηφιακό περιβάλλον. Ωστόσο, τις προσφερόμενες ευκαιρίες για καινοτομία και βελτιστοποίηση των διαδικασιών συνοδεύουν νέες ευπάθειες προς εκμετάλλευση, όσον αφορά στην ασφάλεια των πληροφοριακών συστημάτων. Ανάμεσα σε αυτές, περιλαμβάνονται και οι επιθέσεις πλευρικής κίνησης, τις οποίες αξιοποιούν οι κακόβουλοι για να πλοηγηθούν αθέατοι εντός των δικτύων, να εκμεταλλευτούν τις προσφερόμενες ευπάθειες και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε κρίσιμες πληροφορίες.

Εικόνα 1: Cyber Kill Chain

Φάσεις της Πλευρικής Κίνησης

Αναγνώριση

Κατά τη φάση της αναγνώρισης συλλέγονται πληροφορίες από τον κακόβουλο, όσον αφορά την τοπολογία του δικτύου, τα χαρακτηριστικά χρηστών και των χρησιμοποιούμενων συσκευών, ώστε να ανακαλυφθούν ευπάθειες προς εκμετάλλευση. Επιπλέον, εξετάζεται η υποδομή του δικτύου ενδιαφέροντος, έτσι ώστε να αποκαλυφθούν τα ιεραρχικά μοντέλα που υλοποιούνται, οι συμβάσεις ονοματοδοσίας (host naming conventions) και τα λειτουργικά συστήματα (OSs) που χρησιμοποιούνται, επιστρατεύοντας διαφορετικές τεχνικές, ώστε να παραμείνουν το δυνατόν ανεντόπιστες οι κινήσεις των κακόβουλων [7]. Συνήθως κατά την αρχική πρόσβαση γίνονται προσπάθειες για χαρτογράφηση του δικτύου, των χρησιμοποιούμενων διευθύνσεων (IPs), ονόματα τομέων και υποτομέων (Domain names), τύποι και εκδόσεις τεχνολογιών και φυσικά οποιουδήποτε μέτρου ασφαλείας χρησιμοποιεί η υποδομή ενδιαφέροντος, όπως τείχη προστασίας (Firewalls), συστήματα ανίχνευσης εισχωρήσεων (IDS) κλπ [14]. Τα παραπάνω είναι προαπαιτούμενα, ώστε οι κακόβουλοι να σχεδιάσουν τις κινήσεις τους στο δίκτυο και να αποφύγουν οποιοδήποτε τροχοπέδι θα μπορούσε να τους αποτρέψει. Κάτι τέτοιο είναι εφικτό να υλοποιηθεί, αξιοποιώντας εργαλεία όπως το Netstat, ipconfig, powershell, ARPshell κ.α.

- Netstat: Εργαλείο με το μπορούν να συλλεχθούν πληροφορίες για τις τρέχουσες συνδέσεις δικτύου της συσκευής. Χρησιμοποιώντας αυτή την εντολή ο επιτηθέμενος μπορεί να κατανοήσει τις διασυνδέσεις σε ένα δίκτυο, τις διαδρομές που χρησιμοποιεί για να στέλνει και να λαμβάνει πληροφορίες, ακόμα και πιο τεχνικές πληροφορίες όπως πρωτόκολλα και πόρτες που εγκαθιδρύονται οι δίαυλοι επικοινωνίας. [10]
- Local Routing Tables: Σε τέτοιου είδους πίνακες είναι αποθηκευμένες πληροφορίες, όπως δρομολόγηση (route) και διασυνδέσεις δικτύων.
- Ipconfig/ifconfig: Με αυτές τις εντολές δίνεται η δυνατότητα να γίνουν αντιληπτές πληροφορίες για τις διαμορφώσεις του δικτύου και να συλλεχθούν δεδομένα διευθύνσεων άλλων δικτυακών συσκευών.
- Address Resolution Protocol cache: Σε αυτή τη μνήμη αποθηκεύονται οι αντιστοιχήσεις των διευθύνσεων IP και και φυσικών διευθύνσεων (MAC). Η γνώση τέτοιου είδους πληροφορίας δίνει τη δυνατότητα να στοχοποι- ηθούν συγκεκριμένα end points στο δίκτυο και να αποφευχθούν τυχόντες αμυντικοί μηχανισμοί.
- PowerShell: Πρόκειται για μια γλώσσα scripting υψηλής ευελιξίας και ένα περιβάλλον γραμμής εντολών, το οποίο χρησιμοποιείται από κακόβουλους χρήστες για τον εντοπισμό λογαριασμών με προνομιακά δικαιώματα (administrative privileges). Με αυτόν τον τρόπο, οι επιτιθέμενοι αποκτούν τη δυνατότητα να αξιοποιήσουν ένα ευρύ φάσμα εργαλείων για την εκτέλεση αξιολογήσεων ευπάθειας και χαρτογράφησης δικτύων, προκειμένου να

εκμεταλλευτούν τυχόν ευπάθειες που θα προκύψουν από τη συλλογή πληροφοριών.

- Nmap: Πρόκειται για ένα δωρεάν και ανοιχτού κώδικα εργαλείο με το οποίο είναι εφικτή η ανίχνευση δικ- τύου (εύρεση συνδεδεμένων συσκευών). Μπορούν να υλοποιηθούν έλέγχοι ασφάλειας (αναγνώριση ευπαθειών, έλεγχος θυρών), ταυτοποίηση λειτουργικών συστημάτων και έλεγχος δικτυακών υπηρεσιών. Χρησιμοποιείται για την αναγνώριση ανοιχτών θυρών και τον εντοπισμό των υπηρεσιών που εκτελούνται σε αυτές και είναι εξίσου αποτελεσματικό σε σκαναρίσματα για ευπάθειες των hosts.

Εικόνα 2: Phases of Lateral Movement

Εξαγωγή Διαπιστευτηρίων και Κλιμάκωση Προνομίων

Με την ολοκλήρωση της προηγούμενης φάσης ο εισβολέας θα πρέπει να αποκτήσει πρόσβαση σε διαπιστευτήρια ή να κλιμακώσει τα προνόμια στο σύστημα το οποίο έχει ήδη παραβιαστεί. Συνεπώς, επικεντρώνεται στην απόκτηση αυτών των πληροφοριών μέσω τεχνικών κοινωνικής μηχανικής (social engineering), καταχρηστική ονοματοδοσία ιστοτόπων με ορθογραφικά λάθη (typo Squatting) και επιθέσεις ψαρέματος (phishing). Επιπλέον τεχνικές της ΠΚ αποτελούν [4]:

- Καταγραφείς Πληκτρολογήσεων (Keyloggers): Ο επιτιθέμενος χρησιμοποιεί μολυσμένα αρχεία, κακόβουλα link ή και τεχνικές ηλεκτρονικού ψαρέματος (phishing) για μολύνουν τον νόμιμο χρήστη και να του αποσπάσουν κάθε πληροφορία που πληκτρολογεί [16].
- Pash-the-Hash (PtH): Στην επίθεση αυτή, ο κακόβουλος χρήστης συλλαμβάνει έναν κατακερματισμένο κωδικό πρόσβασης και τον χρησιμοποιεί για να αποκτήσει πρόσβαση σε άλλες συσκευές ή υπηρεσίες σε ένα δίκτυο. Ο στόχος είναι η εκμετάλλευση των διαδικασιών αυθεντικοποίησης των λειτουργικών συστημάτων, κυρίως στα Windows.
- Pass-the-Ticket (PtT): Χρησιμοποιώντας εργαλεία όπως το Mimikatz για την εξαγωγή των Kerberos au- thentication tickets ο επιτιθέμενος αποκτά πρόσβαση σε ένα δίκτυο και αυθεντικοποιείται, χωρίς να έχει στη διάθεσή του τον κωδικό πρόσβασης ενός χρήστη.

Φυσικά αυτές οι τεχνικές εμπίπτουν στην γενικότερη κατηγορία της Απόκτησης Διαπιστευτηρίων (Credential Access), όπως αναφέρεται στο MITRE ATT&CK. Ο στόχος του επιτιθέμενου είναι η απόκτηση έγκυρων ονομάτων χρήστη και κωδικών

πρόσβασης σε συστήματα, δίκτυα και ευαίσθητες πληροφορίες. Η καταγραφή πληκτρολογήσεων (keylogging) και η εξαγωγή διαπιστευτηρίων (credential dumping) είναι δύο κοινές τενικές που χρησιμοποιούνται για την κλοπή διαπιστευτηρίων. Στην πρώτη περίπτωση περιλαμβάνεται η καταγραφή των πληκτρολογήσεων που κάνει ο χρήστης, ενώ στη δεύτερη η εκμετάλλευση αφορά στη διαδικασία εξαγωγής αποθηκευμένων κωδικών πρόσβασης από ένα σύστημα το οποίο έχει προσβληθεί [1].

Η πρόσβαση σε έγκυρα διαπιστευτήρια μπορεί να προσφέρει στον επιτιθέμενο σημαντικό πλεονέκτημα, επιτρέποντας του να δρα εντός του δικτύου χωρίς να εντοπίζεται, καθώς εμφανίζεται ως νόμιμος χρήστης. Για την αποτροπή αυτών

των επιθέσεων θα πρέπει να επιβληθούν αυστηρές πολιτικές ασφαλείας τουλάχιστον ως προς την διαχείρηση και αλλαγή κωδικών πρόσβασης, πολυπαραγοντικός έλεγχος ταυτότητας (MFA), απομόνωση συστημάτων και υιοθέτηση της αρχής της παροχής των ελάχιστων δικαιωμάτων σε κάθε συσκευή εντός δικτύου. Παράλληλα, η παρακολούθηση και η ανάλυση μη συνηθισμένης δραστηριότητας και ο τακτικός έλεγχος των αρχείων καταγραφής του συστήματος (logs) μπορούν να συμβάλλουν στην έγκαιρη ανίχνευση της χρήσης κλεμένων διαπιστευτηρίων από κάποιο κακόβουλο [12].

Απόκτηση πρόσβασης

Η αναγνώριση και παράκαμψη των υπαρχώντων μέτρων ασφαλείας μπορεί να συνεχιστεί, έως ότου επιτευχθεί η παραβίαση του στόχου. Ο επιτιθέμενος διεξάγει συνεχώς αναγνωριστικές ενέργειες εντός δικτύου, προσπαθώντας να κατανοήσει τη δομή, τα σημεία αδυναμίας και τις δυνατότητες της παρεχόμενης ασφάλειας. Σε αυτό το σημείο είναι σημαντικό να αναγνωριστεί ο ρόλος της ανθρώπινης εμπλοκής στην περίπλοκη εξέλιξη των κυβερνοεπιθέσεων. Δηλαδή, παρόλο που πολλές επιθέσεις γίνονται με αυτοματοποιημένα εργαλεία, ο ανθρώπινος παράγοντας εξακολουθεί να διαδραματίζει καθοριστικό ρόλο. Ειδικά σε πιο εξελιγμένες επιθέσεις, οι άνθρωποι είναι αυτοί που λαμβάνουν αποφάσεις για το πώς θα ξεπεραστούν τα εμπόδια ασφαλείας. Αυτό έχει εφαρμογή ιδιαίτερα στις χρησιμοποιούμενες από τους οργανισμούς εφαρμογές μηχανικής μάθησης, που χρησιμοποιούνται για να ενισχύσουν την ασφάλειά τους. Οι επιτιθέμενοι μπορούν να προσαρμόζουν τις τακτικές τους, ειδικά όταν εντοπίζουν μηχανισμούς που βασίζονται σε μηχανική μάθηση, ώστε να τα παρακάμψουν. Παρ'όλα αυτά οι ενέργειες των κακόβουλων μπορούν να εντοπίστούν και να αντιμετωπιστούν εαν ο οργανισμός διαθέτει ένα ολοκληρωμένο και προσεκτικά σχεδιασμένο σχέδιο ασφάλειας.

Επιπροσθέτως, το Mimikatz αποτελεί ένα από τα πιο γνωστά εργαλεία ανοιχτού κώδικα, διακεκριμένο για την αποτελεσματικότητά του στις δοκιμές διείσδυσης (penetration testing). Αρχικά δημιουργήθηκε από τον ηθικό χάκερ Benjamin Delpy [5] για να αναδείξει μια αδυναμία στα πρωτόκολλα αυθεντικοποίησης των Windows, αλλά έκτοτε έχει γίνει ένα βασικό εργαλείο για την προσομοίωση πραγματικών επιθέσεων και τον έλεγχο της ασφάλειας συστημάτων και δικτύων.

Με τη χρήση αυτού του εργαλείου δίνεται η δυνατότητα να εξαχθούν τα εισιτήρια Kerberos και άλλα διαπιστευτήρια αυθεντικοποίησης από έναν σταθμό εργασίας Windows, συμπεριλαμβανομένων των κωδικών πρόσβασης, οι οποίοι μπορούν να χρησιμοποιηθούν για μη εξουσιοδοτημένη πρόσβαση σε συστήματα και δίκτυα. Αυτό το καθιστά ένα ισχυρό εργαλείο στα χέρια των επιτιθέμενων, αλλά ταυτόχρονα αποτελεί και ένα σημαντικό εργαλείο για τους ειδικούς ασφάλειας (ethical hackers), καθώς τους βοηθά να εντοπίζουν ευπάθειες στα συστήματά τους και να ενισχύουν την ασφάλειά τους με τις κατάλληλες διορθωτικές ενέργειες.

Το εργαλείο αυτό στοχεύει στη διαδικασία Local Security Authority Subsystem Service (LSASS)- Sigle Sign- On, η οποία διαχειρίζεται την ασφάλεια και την αυθεντικοποίηση των χρηστών στα Windows. ΄Οταν το LSASS βρίσκεται στη μνήμη του συστήματος, αποθηκεύει διάφορες πληροφορίες που σχετίζονται με τους χρήστες και την ταυτοποίησή τους, όπως κωδικούς πρόσβασης και token αυθεντικοποίησης. Το Mimikatz εκμεταλλεύεται αυτό το γεγονός για να αποκτήσει πρόσβαση στα διαπιστευτήρια των χρηστών και να τα εξάγει. Μπορεί να ανακτήσει δεδομένα όπως κρυπτογραφημένους κωδικούς (hashes), ή ακόμα και κωδικούς σε απλό κείμενο (cleartext), που επιτρέπουν στον επιτιθέμενο να μιμηθεί τον πραγματικό χρήστη και να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα.Το Mimicatz ή αλλιώς kiwi λειτουργεί ως εξής:

- Αναγνώριση Ευπαθειών: Χρησιμοποιώντας το local exploit suggester του Metasploit, μπορούν να εν- τοπιστούν ευπάθειες στο σύστημα στόχο που είναι επιρρεπείς προς εκμετάλλευση. Το Metasploit είναι ένα εργαλείο που χρησιμοποιείται για τη δοκιμή ευπάθειών και τη διείσδυση σε συστήματα.
- Αύξηση Προνομίων: Χρησιμοποιώντας την εκμετάλλευση bypass uac dotnet profiler, είναι εφικτή η αύξηση των προνόμίων (privillege escalation), δηλαδή η απόκτηση πρόσβασης με υψηλότερα δικαιώματα (administrator) στο σύστημα. ΄Επειτα, μεταφέρεται το εκτελέσιμο αρχείο kiwi στη στοχοθετημένη μηχανή. Το kiwi είναι ένα εργαλείο που χρησιμοποιείται για την εξαγωγή κωδικών πρόσβασης από τη μνήμη.
- ΄Ελεγχος Προνομίων: Πραγματοποιείται έλεγχος προνομίων χρησιμοποιώντας την εντολή privilege::debug σε ένα σύστημα shell, προκειμένου να διασφαλιστεί ότι το εκτελέσιμο kiwi λειτουργεί σωστά με τα αναγκαία δικαιώματα.
- Εξαγωγή Πληροφοριών Διαπιστευτηρίων: Εκτελώντας την εντολή kiwi cmd sekurlsa::logonPasswords, μπορούν να εξάχθούν πληροφορίες διαπιστευτηρίων. Αυτές οι πληροφορίες περιλάμβαναν τους κωδικούς πρόσ- βασης σε κρυπτογραφημένη μορφή (SHA1 και NTLM hashes) του συνδεδεμένου χρήστη.
- Σπάσιμο Κωδικών Πρόσβασης: Τέλος, χρησιμοποιείται το εργαλείο hashcat μαζί με τους εξαγόμενους κωδικούς πρόσβασης σε κρυπτογραφημένη μορφή, ώστε να σπάσουν οι κωδικοί πρόσβασης και να αποκτηθούν οι πραγματικές τιμές τους. [6]

Διαπιστώθηκε ότι όταν το Windows Defender ήταν ενεργό, κατάφερε να ανιχνεύσει αποτελεσματικά το κακόβουλο λογισμικό κατά τη διάρκεια της μεταφοράς του φορτίου (payload) Meterpreter στο στοχοθετημένο σύστημα. Ομοίως το ίδιο συνέβει και για το εκτελέσιμο του MimiKatz. Συνεπώς, από το [6] προκύπτει ότι επιβεβαιώνεται η αποτελεσ- ματικότητα του Windows Defender στην προστασία από κακόβουλο λογισμικό και την ικανότητά του να ανιχνεύει και να καταγράφει επιθέσεις που χρησιμοποιούν εργαλεία όπως το Meterpreter και το Mimikatz. Το εργαλείο Mimikatz αποτελεί μία από τις ισχυρότερες πλατφόρμες για την κλοπή κωδικών πρόσβασης παγκοσμίως. ΄Εχει μετατραπεί σε ένα σημαντικό εργαλείο για post-exploitation και χρησιμοποιείται από κακόβουλους οι οποίοι στοχεύουν σε συστή- ματα που βασίζονται σε Microsft, από ειδικούς που εκτελούν τεστ διείσδυσης (pentesters) και γενικότερα ειδικούς ασφάλειας για την αξιολόγηση ασφάλειας και την αναβάθμιση των προνομίων σε λειτουργικά συστήματα Windows. Τη συνεχή αναβάθμιση του λειτουργικού συστήματος των Windows ακολουθεί και η ανάπτυξη νέων εκδόσεων του Mimikatz, ώστε να διασφαλίζεται τη συμβατότητά και την αποτελεσματικότητά του. Είναι σημντικό να σημειωθεί ότι συγκεκριμένες εκδόσεις του Mimikatz έχουν ενσωματωθεί σε κακόβουλα πακέτα απειλών, όπως το NotPetya και το BadRabbit, καταδεικνύοντας κατ αυτό τον τρόπο την εφαρμογή του σε ευρείας κλίμακας κυβερνοεπιθέσεις. [11]

Πλέον, το Mimikatz περιλαμβάνεται σε όλες τις πρόσφατες εδόσεις των διανομών Kali Linux, καθώς και στο Metasploit framework, ένα γνωστό εργαλείο για την αξιολόγηση τρωτών σημείων και στην εκμετάλλευση τους [1]Το Mimikatz έχει αναγνωριστεί ευρέως ως η κύρια επιλογή για την παραγωγή πλαστών εισητηρίων Kerberos και την εκμετάλλευση των σχετικών ευπαθειών. Αν και το Mimikatz δεν προορίζεται για κακόβουλη χρήση, οι προηγούμενες δυνατότητες του το καθιστούν εργαλείο διπλής χρήσης, καθώς μπορεί να αξιοποιηθεί τόσο για κακόβουλες ενέργειες, όπως η κλοπή διαπιστευτηρίων και η αναβάθμιση προνομίων, όσο και για θεμιτούς σκοπούς ασφάλειας, όπως η ανίχνευση και η αντιμετώπιση τρωτών σημείων σε δίκτυα. Είναι κρίσιμο να σημειωθεί ότι οι ισχυρές λύσεις ασφάλειας για τερματικά σημεία παίζουν καθοριστικο ρόλο στην προστασία από πιθανή κατάχρηση τέτοιων εργαλείων σε περιβάλλοντα δικτύου [17].

Πλευρική Κίνηση σε Συστήματα Windows: Μέθοδοι και Στρατηγικές Επιθέσεων

Ο κύριος σκοπός των επιτιθέμενων που εφαρμόζουν τεχνικές πλευρικής κίνησης (lateral movement) είναι να διαπεράσουν το προστατευμένο δίκτυο, χρησιμοποιώντας διάφορα εργαλεία για να αποκτήσουν πλήρη απομακρυσμένο έλεγχο των συστημάτων-στόχων. Για να το πετύχουν, μπορεί να αξιοποιήσουν εργαλεία απομακρυσμένης πρόσβασης ή να εκμεταλλευτούν ευάλωτα συστήματα που έχουν ήδη παραβιαστεί. Αυτό τους επιτρέπει να κινούνται πλευρικά σε διάφορους κόμβους του δικτύου, γεγονός που είναι απαραίτητο για τη διατήρηση της ανωνυμίας τους μετά την πρόσβαση. Οι τεχνικές που περιλαμβάνονται σε αυτή τη στρατηγική, όπως

ενημερώνονται στη βάση δεδομένων ανοικτού κώδικα MITRE, ποικίλλουν και αναλύονται ενδεικτικά ως εξής:

Οι εισβολείς συχνά επικεντρώνονται σε συστήματα Windows που βρίσκονται σε εταιρικά ή οικιακά δίκτυα (SOHO), εκμεταλλευόμενοι απομακρυσμένες υπηρεσίες για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε κόμβους του δικ- τύου. Αυτή η εκμετάλλευση βασίζεται στη δυνατότητα αξιοποίησης ευπαθειών που υπάρχουν στα στοχευμένα συστή- ματα, οι οποίες μπορεί να προέρχονται από σφάλματα στον πηγαίο κώδικα των εφαρμογών, προβλήματα σε υπηρεσίες των Windows ή αδυναμίες στον πυρήνα του λειτουργικού συστήματος των Windows. Αυτές οι αδυναμίες μπορούν να επιτρέψουν την εκτέλεση κακόβουλου λογισμικού και την πρόσβαση στο δίκτυο από απόσταση χωρίς εξουσιοδότηση. Για να αξιολογήσει την ευπάθεια ενός στοχευμένου συστήματος, ένας επιτιθέμενος συνήθως εφαρμόζει διάφορες γνωστές τεχνικές σάρωσης δικτυακών υπηρεσιών. Αυτές οι μέθοδοι είναι σχεδιασμένες να εντοπίζουν παρωχημένα ή μη ενημερωμένα λειτουργικά συστήματα, καθώς και την απουσία σύγχρονων συστημάτων ανίχνευσης εισβολών (IDS) και προγραμμάτων antivirus. Οι κόμβοι εξυπηρετητών (server-nodes), λόγω της μεγάλης τους αξίας, συχνά γίνονται κύριος στόχος επιθέσεων πλευρικής κίνησης (LM). Αφού αποκτήσει αρχική πρόσβαση σε ένα δίκτυο, ο επιτιθέμενος συνήθως περιπλανιέται σε διάφορα συστήματα, αναβαθμίζοντας σταδιακά τα προνόμιά του, με τους servers να είναι συχνά ο τελικός του στόχος. Οι επιτιθέμενοι, προκειμένου να διευκολύνουν την πρόσβασή τους σε ένα δίκτυο, χρησιμοποιούν μεθόδους που τους επιτρέπουν να συλλέγουν πληροφορίες σχετικά με το περιβάλλον. Η σάρωση θυρών (port scanning) τους επιτρέπει να εντοπίζουν ποιες θύρες είναι ανοιχτές σε έναν υπολογιστή ή διακομιστή, παρέχοντας στοιχεία για τις υπηρεσίες που εκτελούνται. Η αξιολόγηση ευπαθειών (vulnerability assessment) αφορά τη χρήση εργαλείων που αναλύουν το λογισμικό και τις ρυθμίσεις για να εντοπίσουν τρωτά σημεία που μπορούν να εκμεταλλευτούν[17].

Αφού αποκτήσουν πρόσβαση σε ένα σύστημα, οι επιτιθέμενοι εγκαθιστούν αυτά τα εργαλεία για να συλλέγουν δεδομένα σχετικά με τις υπηρεσίες που τρέχουν στο δίκτυο, καθώς και για τις ευπάθειες ή τις ακατάλληλες ρυθμίσεις που μπορεί να υπάρχουν. Με αυτόν τον τρόπο, μπορούν να σχεδιάσουν στρατηγικές επιθέσεις, εκμεταλλευόμενοι τις αδυναμίες της υποδομής του δικτύου και να διεισδύσουν σε συστήματα με μεγαλύτερη ευκολία.

Ανάμεσα στις πιο συχνά χρησιμοποιούμενες διαδικασίες σάρωσης δικτύου για δοκιμές διείσδυσης σε περιβάλ- λοντα Windows/Active Directory (AD), σύμφωνα με την ενημερωμένη λίστα MITRE ATT&CK, περιλαμβάνεται το CrackMapExec (CME). Αυτό το εργαλείο δοκιμών διείσδυσης έχει αναπτυχθεί σε Python και αξιοποιεί τα ενσωματωμένα πρωτόκολλα του Active Directory, επιτρέποντας τη συγκέντρωση πληροφοριών που κυμαίνονται από διευθύνσεις IP μέχρι την κλοπή διαπιστευτηρίων από το SAM. [2] Πιο συγκεκριμένα, το CME λειτουργεί εντοπίζοντας τους καταγεγραμμένους χρήστες και εξερευνώντας τις κοινοποιήσεις του Service Message Block (SMB) που σχετίζον- ται με το Windows AD. Επιπλέον, αυτό το εργαλείο επιτρέπει την εκτέλεση PowerShell και Python scripts για την εκτέλεση επιθέσεων

brute force διαπιστευτηρίων. Τέτοιες τεχνικές περιλαμβάνουν την εικασία κωδικών πρόσβασης σε συστήματα όπου δεν είναι γνωστά τα νόμιμα διαπιστευτήρια, καθώς και το password spraying [8], το οποίο περιλαμ- βάνει τη χρήση ενός μόνο αναμενόμενου ονόματος χρήστη για την προσπάθεια ανακάλυψης έγκυρων λογαριασμών. Οι επιτιθέμενοι συχνά χρησιμοποιούν λίστες κωδικών πρόσβασης και γνωστές λέξεις-κλειδιά σε μια προσπάθεια να παραβιά- σουν έγκυρους λογαριασμούς χρηστών στο στοχευμένο δίκτυο. Επίσης, δύο σημαντικές ομάδες κυβερνοκατασκοπείας, οι BackdoorDiplomacy και Chimera, έχουν ταυτοποιηθεί να εκμεταλλεύονται ευπάθειες σε διαδικτυακά εκτεθειμένες συσκευές, όπως διακομιστές ιστού (web servers), για κακόβουλες δραστηριότητες. Η ομάδα APT BackdoorDiplomacy χρησιμοποιεί το rootkit Moriya για την εγκατάσταση μιας παθητικής πίσω πόρτας, που επιτρέπει στους επιτιθέμενους να παρακολουθούν την εισερχόμενη κίνηση στο παραβιασμένο σύστημα [15]. Αυτές οι επιθέσεις συχνά περιλαμβάνουν τεχνικές LM σε ένα δίκτυο για την εγκατάσταση προσαρμοσμένων implants, όπως το Turian, που προορίζονται για την εξαγωγή ευαίσθητων δεδομένων από αφαιρούμενα μέσα, με στόχους όπως η επίτευξη ανταγωνιστικού πλεονεκτήματος, το οικονομικό όφελος ή πολιτικά κίνητρα. Οι ομάδες αυτές αξιοποιούν συχνά εργαλεία αναγνώρισης ανοιχτού κώδικα, με στόχο οργανισμούς για συλλογή πληροφοριών. Φαίνεται ότι δίνουν έμφαση σε διπλωματικούς οργανισμούς στην Ασία και την Αφρική, καθώς έχουν εξαπολύσει πολυάριθμες επιθέσεις με κακόβουλο λογισμικό κλοπής διαπιστευτηρίων εναντίον των Υπουργείων Εξωτερικών, ενώ σπανιότερα στοχεύουν μεγάλες πολυεθνικές τηλεπικοινωνιακές εταιρείες. Επιπλέον, η ομάδα Chimera στοχεύει σε ευαίσθητα δεδομένα, όπως έγγραφα για Ολοκληρωμένα Κυκλώματα (ICs), Κιτ Ανάπτυξης Λογισμικού (SDKs), σχέδια ICs και πηγαίο κώδικα, τα οποία είναι κρίσιμα και χρήσιμα για κρατικούς φορείς, αποκτώντας τα μέσω προηγμένων τακτικών και τεχνικών διείσδυσης. Πρόσφατα, η βορειοκορεατική ομάδα APT APT37 κυκλοφόρησε μια νέα έκδοση του κακόβουλου λογισμικού RokRat, το οποίο βασίζεται σε υποδομές cloud για την κλοπή δεδομένων και την αποστολή τους σε υπηρεσίες cloud [3].

Προστασία από επιθέσεις Πλευρικής Κίνησης - Βέλτιστες Πρακτικές

Για την προστασία ενός οργανισμού από επιθέσεις, είναι σημαντικό να εφαρμόζονται μια σειρά από μέτρα ασ- φαλείας που θα δυσκολέψουν την κίνηση των επιτιθέμενων εντός του δικτύου και θα διευκολύνουν την ανίχνευση επιθέσεων,όπως προτείνεται από το National Cyber Security Centre [9].

- Προστασία διαπιστευτηρίων: Τα διαπιστευτήρια χρηστών, ειδικά των διαχειριστών, πρέπει να προστατεύονται επαρκώς ώστε να αποφεύγεται η κατάχρησή τους από επιτιθέμενους. Οι κωδικοί δεν πρέπει να αποθηκεύονται σε μορφή απλού κειμένου, και τα hash των κωδικών πρέπει να προστατεύονται. Επιπλέον, τα διαπιστευτήρια θα πρέπει να χρησιμοποιούνται μόνο σε εγκεκριμένες συσκευές που προσφέρουν την κατάλληλη ασφάλεια, κατά προτίμηση με υποστήριξη αποθήκευσης διαπιστευτηρίων σε υλικό (hardware-backed).

- Καλές πρακτικές ταυτοποίησης: Η ταυτοποίηση πρέπει να είναι εύκολη για τον χρήστη αλλά δύσκολη για έναν επιτιθέμενο. Συνιστάται η χρήση διαχειριστών κωδικών για την αποφυγή αποθήκευσης διαπιστευτηρίων σε μη ασφαλείς μορφές, όπως απλό κείμενο. Η χρήση πολλαπλών παραγόντων ταυτοποίησης (MFA) είναι σημαν- τική για υπηρεσίες που είναι εκτεθειμένες στο διαδίκτυο και για λογαριασμούς υψηλού κινδύνου. Επιπλέον, προτείνονται εναλλακτικές μέθοδοι ταυτοποίησης, όπως βιομετρικά δεδομένα και έξυπνες κάρτες.
- Προστασία λογαριασμών υψηλών δικαιωμάτων: Οι διαχειριστικοί λογαριασμοί θα πρέπει να χρησι- μοποιούνται μόνο για τις απαραίτητες εργασίες και να είναι κλειδωμένοι για άλλες χρήσεις, όπως το browsing και η χρήση email. Προτείνεται η χρήση ξεχωριστών λογαριασμών για καθημερινές εργασίες και για εργασίες διαχείρισης.
- Αρχή ελάχιστων δικαιωμάτων: Η αρχή των ελάχιστων δικαιωμάτων απαιτεί οι χρήστες και οι λογα- ριασμοί να έχουν πρόσβαση μόνο σε ό,τι είναι απολύτως απαραίτητο για την εκτέλεση των καθηκόντων τους.΄Ενα σύστημα ιεράρχησης δικαιωμάτων μπορεί να περιορίσει τη χρήση λογαριασμών με πλήρη δικαιώματα και να ελαχιστοποιήσει την έκθεση σε κινδύνους.
- Ασφάλιση συσκευών και συστημάτων: ΄Ολες οι συσκευές του οργανισμού πρέπει να ενημερώνονται τακτικά και να εφαρμόζονται τα διαθέσιμα patches. Επίσης, η χρήση allow lists για τον περιορισμό των εφαρμογών που μπορούν να εκτελεστούν, καθώς και η ενεργοποίηση τοπικών firewalls, είναι απαραίτητες πρακτικές.
- Δικτυακή διαίρεση και παρακολούθηση: Η διαίρεση του δικτύου σε τμήματα δυσχεραίνει την κίνηση των επιτιθέμενων. Τα τμήματα του δικτύου που δεν χρειάζεται να επικοινωνούν μεταξύ τους πρέπει να διαχωρί- ζονται, ενώ παράλληλα, η παρακολούθηση του δικτύου είναι κρίσιμη για την ανίχνευση πιθανών επιθέσεων. Η καταγραφή των logs και η τακτική ανάλυσή τους βοηθά στην ανίχνευση ύποπτης δραστηριότητας.
- Χρήση honeypots: Τα honeypots μπορούν να χρησιμοποιηθούν ως παγίδες για τους επιτιθέμενους, παρέχοντας μια επιπλέον μέθοδο ανίχνευσης εισβολών. Ενώ είναι χρήσιμα, πρέπει να εφαρμοστούν με προσοχή λόγω του κινδύνου που ενέχουν αν χρησιμοποιηθούν λανθασμένα.

Η εφαρμογή αυτών των πρακτικών συμβάλλει στην ενίσχυση της ασφάλειας ενός οργανισμού, δίνοντας παράλληλα χρόνο για να αντιμετωπιστεί έγκαιρα μια πιθανή επίθεση.

Επίλογος

Η πλευρική κίνηση αποτελεί μια κρίσιμη φάση στις στρατηγικές επιθέσεων που εφαρμόζονται σε σύγχρονα δίκτυα. Οι επιτιθέμενοι, εκμεταλλευόμενοι ευπάθειες και ελλείψεις ασφαλείας, επιχειρούν να επεκτείνουν την πρόσβασή τους και να διατηρήσουν τον έλεγχο στοχοποιημένων συστημάτων. Η κατανόηση των φάσεων της

πλευρικής κίνησης, σε συνδυασμό με την υιοθέτηση βέλτιστων πρακτικών ασφαλείας, μπορεί να συμβάλει ουσιαστικά στην ανίχνευση και αποτροπή τέτοιων επιθέσεων.

Η εφαρμογή παραδοσιακών αλλά και προηγμένων τεχνικών προστασίας, όπως η τακτική ενημέρωση λογισμικού, η ενίσχυση πολιτικών ασφαλείας, η παρακολούθηση δικτύων και η χρήση εργαλείων ανίχνευσης ευπαθειών, μπορεί να μειώσει σημαντικά τον κίνδυνο παραβίασης. Ωστόσο, η πραγματική καινοτομία στη σύγχρονη ασφάλεια δικτύων έρχεται μέσω της ενσωμάτωσης τεχνικών μηχανικής μάθησης (ML). Οι αλγόριθμοι ML επιτρέπουν την αναγνώριση ανωμαλιών σε πραγματικό χρόνο και την αυτόματη ανίχνευση επιθέσεων που είναι δύσκολο να εντοπιστούν με παραδοσιακές μεθόδους. Η δυνατότητα του ML να μαθαίνει και να προσαρμόζεται στις εξελισσόμενες απειλές μπορεί να προσφέρει στους οργανισμούς ένα δυναμικό και προληπτικό εργαλείο για την ανίχνευση προηγμένων επιθέσεων, όπως η πλευρική κίνηση και οι στοχευμένες επιθέσεις σε κρίσιμους πόρους.

Επιπλέον, η εφαρμογή στρατηγικών για την επιχειρησιακή συνέχεια (business continuity) αποτελεί αναπόσπαστο μέρος της συνολικής στρατηγικής ασφάλειας. Η καλή διαχείριση της επιχειρηματικής συνέχειας εξασφαλίζει ότι, ακόμη και στην περίπτωση παραβίασης, οι οργανισμοί μπορούν να ανακάμψουν γρήγορα και να συνεχίσουν τις κρίσιμες λει- τουργίες τους χωρίς σοβαρές διακοπές. Με τη συνδυαστική χρήση του ML και των στρατηγικών αντοχής (cybersecurity tolerance), οι οργανισμοί δεν περιορίζονται μόνο στην αποτροπή επιθέσεων αλλά είναι επίσης καλύτερα προετοιμασ- μένοι για τη διαχείριση και την αποκατάσταση συστημάτων μετά από ένα συμβάν. Η δυνατότητα να ελέγχουν και να αναλύουν τις ευπάθειες των συστημάτων σε πραγματικό χρόνο, να αναγνωρίζουν υποκείμενες τάσεις επίθεσης και να αναπτύσσουν ταυτόχρονα σχέδια αποκατάστασης, διασφαλίζει ότι τα οργανωτικά δεδομένα παραμένουν προστατευμένα και η λειτουργία του οργανισμού συνεχίζεται απρόσκοπτα.

Συνεπώς, είναι απαραίτητη η συνεχής επαγρύπνηση και η διαρκής ενασχόληση με το ζήτημα της ασφάλειας, προκειμένου οι οργανισμοί να παραμένουν ένα βήμα μπροστά από τις εξελισσόμενες απειλές και να διασφαλίζουν την ακεραιότητα και τη συνέχεια των κρίσιμων λειτουργιών τους.

Αναφορές

1 Mitre attack. https://attack.mitre.org, October 2024. Accessed: 2024-10-08.

2 Raj Chandel. Lateral movement on active directory using crackmapexec. https://www.hackingarticles. in/lateral-movement-on-active-directory-crackmapexec, 2020. Accessed: October 22, 2024.

3 Cyware News. Chimera group now targeting cloud services. https://social.cyware.com/news/ chimera-group-now-targeting-cloud-services-4db01161, 2023. Accessed: 2024-10-10.

4 Ravi Das. Common lateral movement techniques and how to prevent them. https://www.techtarget. com/searchsecurity/tip/Common-lateral-movement-techniques-and-how-to-prevent-them. Accessed: 2024-09-26.

5 Benjamin Delpy. Mimikatz: A tool for manipulating windows security. https://github.com/gentilkiwi/ mimikatz, 2024. Accessed: 2024-10-22.

6 Shahrukh Iqbal. Attacking windows 10 using mimikatz. https://shahrukhiqbal24.medium.com/ attacking-windows-10-using-mimikatz-824c73eb9f3d, 2021. Medium article, Accessed: 2024-10-22.

7 What is Lateral Movement? https://www.illumio.com/cybersecurity-101/lateral-movement. Accessed: 2024-09-10.

8 MITRE ATT&CK. T1110.003 - password spraying. https://attack.mitre.org/techniques/T1110/003/, 2023. Accessed: 2024-10-10.

9 National Cyber Security Centre. Preventing lateral movement. Online resource, 2023. Accessed: 2024-10-22. . Available: https://hellanicus.lib.aegean.gr/handle/11610/26758. Accessed 2024

10 Netstat command in Linux. https://www.geeksforgeeks.org/netstat-command-linux/. Accessed: 2024- 09-10.

11 Danny Palmer. Bad rabbit ransomware spread using leaked nsa eternalromance exploit, researchers confirm. ZDNet, October 2017. Accessed: 2024-10-09.

12 Daniel Petri. Pass the Hash Attack Defense: AD Security 101 https://www.semperis.com/blog/ how-to-defend-against-pass-the-hash-attack/. Accessed: 2024-10-08.

13 Rapid7. Metasploit: The penetration testing framework, 2024. Accessed: 2024-10-22.

14 Penetration Testing:Methodology, Scope and Types of Pentests. https://www.illumio.com/ cybersecurity-101/lateral-movement. Accessed: 2024-09-10.

15 TheSec Master. How backdoordiplomacy apt group uses turian back- door to carry out cyber espionage campaign. https://thesecmaster.com/ how-backdoordiplomacy-apt-group-usesturian-backdoor-to-carryout-cyber-espionage-campaign, 2023. Accessed: 2024-10-10.

16 Τσίπας Δ. Βιβλιογραφική επισκόπηση επιθέσεων σε μη επανδρωμένα αεροσκάφη και μια μελέτη περίπτωσης. Master's thesis, Πανεπιστήμιο Αιγαίου, 2022

17 S. Altini, "Detecting Lateral Movement in MS Windows through Supervised MachineLearning," September 2023. Online

Βιογραφικό συντάκτη

Ο Υπολοχαγός Διονύσιος Τσίπας αποφοίτησε από τη Στρατιωτική Σχολή Ευελπίδων (ΣΣΕ) το 2018, ως Ανθυπολοχαγός Πεζικού (ΠΖ). Είναι απόφοιτος του Σχολείου Βασικής Εκπαίδευσης Αλεξιπτωτιστή (ΣΒΕΑ), Joint Terminal Attack Controller (JTAC) του Κέντρου Αεροπορικής Τακτικής (ΚΕΑΤ) και του Σχολείου Παροχής Α' Βοηθειών στο Πεδίο της Μάχης (TCCC). Έχει ολοκληρώσει όλα τα προβλεπόμενα στο βαθμό του σχολεία και έχει υπηρετήσει στη Σάμο και στη Λέρο. Είναι κάτοχος μεταπτυχιακού τίτλου σπουδών (MSc) του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων (Πανεπιστήμιο Αιγαίου-Πολυτεχνική Σχολή) με τίτλο «Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων» και αυτή την περίοδο φοιτεί στην Σχολή Προγραμματιστών Ηλεκτρονικών Υπολογιστών (ΣΠΗΥ) στο τμήμα Προγραμματιστών και Αναλυτών.

ΤΕΧΝΙΚΕΣ ΚΑΙ ΕΡΓΑΛΕΙΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΗΣ ΕΥΦΥΪΑΣ ΣΤΟ ΠΥΡΟΣΒΕΣΤΙΚΟ ΣΩΜΑ

Κωνσταντίνος Μαρκούτης,

Εισαγωγή

Εφαρμογή εργαλείων και τεχνικών Επιχειρηματικής Ευφυΐας

Το Πυροσβεστικό Σώμα είναι ιδιαίτερο Σώμα Ασφαλείας, με αρμοδιότητα που εκτείνεται σε όλη την Επικράτεια. Στο πλαίσιο της αποστολής του, συμμετέχει στην αντιμετώπιση κάθε έκτακτης ανάγκης που προκύπτει σε περίοδο ειρήνης ή πολέμου, και σε συνεργασία με τις συναρμόδιες αρχές και υπηρεσίες, συμβάλλει στην εξασφάλιση της πολιτικής προστασίας και της πολιτικής άμυνας της Χώρας.

Από αυτόν τον ορισμό, προκύπτει ότι το Πυροσβεστικό Σώμα έχει αναλάβει ένα πλήθος αρμοδιοτήτων, οι οποίες δημιουργούν αυξημένες απαιτήσεις για λήψη γρήγορων και σωστών αποφάσεων σε σύντομο χρονικό διάστημα.

Το Πυροσβεστικό Σώμα είναι ένας από τους πυλώνες σταθερότητας της χώρας μας και έχει αναλάβει ένα πλήθος καθηκόντων που αφορούν την προστασία ανθρώπων και αγαθών.

Σε αυτές προκλήσεις, η επιχειρηματική ευφυΐα μπορεί να συνεισφέρει δίνοντας λύσεις και απαντήσεις σε δύσκολες καταστάσεις αλλά και στην αποδοτικότερη οργάνωση του Σώματος.

Ορισμός επιχειρηματικής ευφυΐας [2]

Η επιχειρηματική ευφυΐα είναι ένα σύνολο στρατηγικών και τεχνικών, οι οποίες συλλέγουν, αποθηκεύουν και αναλύουν τα δεδομένα τα οποία παράγονται από τις δραστηριότητες ενός οργανισμού.

Τι είναι η επιχειρηματική ευφυΐα [3]

Είναι ένα σύνολο προγραμμάτων και διαδικασιών, με τις οποίες συλλέγουμε, επεξεργαζόμαστε, και παρουσιάζουμε δεδομένα.

Αυτή η ανάλυση αφορά ιστορικά και τρέχοντα δεδομένα και οδηγεί στη λήψη στρατηγικών για έναν οργανισμό αποφάσεων.

Η παρουσίαση των αποτελεσμάτων γίνεται με αναφορές οι οποίες περιέχουν δείκτες, γραφήματα και χάρτες ώστε οι χρήστες να έχουν μια γενική ή ειδική εικόνα ανάλογα με τη θέση και τα καθήκοντα που έχουν στον οργανισμό για τον οποίο εργάζονται.

Λήψη αποφάσεων με ανάλυση δεδομένων επιχειρηματικής ευφυΐας

Ένα από τα μεγαλύτερα πλεονεκτήματα της χρήσης τεχνικών και εργαλείων επιχειρηματικής ευφυΐας στο Πυροσβεστικό Σώμα είναι η δυνατότητα λήψης αποφάσεων βάσει ιστορικών δεδομένων και δεδομένων πραγματικού χρόνου.

Βελτίωση στη διαχείριση συμβάντων [4]

Οι πλατφόρμες επιχειρηματικής ευφυΐας συλλέγουν και αναλύουν δεδομένα, όπως ιστορικά περιστατικά πυρκαγιάς και πλημμύρας, καιρικές συνθήκες και κτιριακές δομές. Χρησιμοποιώντας αυτά τα δεδομένα, οι πυροσβεστικές υπηρεσίες μπορούν να προβλέψουν καλύτερα πού και πότε είναι πιθανό να εκδηλωθούν συμβάντα, βοηθώντας τους να ιεραρχήσουν τους πόρους και το προσωπικό πιο αποτελεσματικά.

Η ικανότητα πρόγνωσης και μοντελοποίησης των δεδομένων είναι ιδιαίτερα κρίσιμη για τη διαχείριση συμβάντων, καθώς επιτρέπει στις υπηρεσίες να προβλέπουν μελλοντικούς κινδύνους και να αναπτύσσουν πόρους (οχήματα και προσωπικό) πιο αποτελεσματικά.

Στην περίπτωση πυρκαγιάς, έχοντας πρόσβαση σε δεδομένα όπως οι πλησιέστεροι κρουνοί, κτίρια ενδιαφέροντος, και παρουσία επικίνδυνων υλικών μαζί με ανάλυση ιστορικών δεδομένων εμφάνισης πυρκαγιών μπορεί να είναι ζωτικής σημασίας για τη λήψη αποφάσεων σε δευτερόλεπτα που μπορεί να σώσουν ζωές και περιουσίες

Βελτιστοποίηση των απόκριση κλήσεων έκτακτης ανάγκης

Όταν χρησιμοποιηθούν μαζί με αντίστοιχα εργαλεία άλλων σωμάτων και υπηρεσιών, όπως Αστυνομία ή Ε.Κ.Α.Β., τα εργαλεία επιχειρηματικής ευφυΐας επιτρέπουν την επικοινωνία και συντονισμό προσωπικού και πόρων κατά τη διάρκεια καταστάσεων έκτακτης ανάγκης.

Αυτή η ολοκληρωμένη προσέγγιση ελαχιστοποιεί τους χρόνους απόκρισης και διασφαλίζει ότι το σωστό προσωπικό και οχήματα αναπτύσσονται γρήγορα και αποτελεσματικά μειώνοντας την πιθανότητα απωλειών.

Διαχείριση κινδύνου – Πρόληψη πυρκαγιάς [5]

Η διαχείριση κινδύνων αποτελεί στόχο της πυροσβεστικής υπηρεσίας, και τα εργαλεία επιχειρηματικής ευφυΐας είναι απαραίτητα για τη βελτίωση της αξιολόγησης και μετριασμού τους.

Οι σύγχρονες πλατφόρμες επιχειρηματικής ευφυΐας χρησιμοποιούν εξελιγμένους αλγόριθμους και αναλύσεις για την ερμηνεία μεγάλου όγκου δεδομένων, παροχή λεπτομερών πληροφοριών στις πυροσβεστικές υπηρεσίες σχετικά με ενδεχόμενους κινδύνους των περιοχών ευθύνης τους και πληροφορίες για τον διαθέσιμο εξοπλισμό τους

Διαχείριση και συντήρηση πυροσβεστικού εξοπλισμού

Ο πυροσβεστικός εξοπλισμός, όπως σωλήνες και μάνικες, οχήματα και ο εξοπλισμός ατομικής προστασίας υφίστανται συνεχή φθορά. Τα εργαλεία επιχειρηματικής ευφυΐας επιτρέπουν στις υπηρεσίες να εφαρμόζουν προγνωστικά χρονοδιαγράμματα συντήρησης παρακολουθώντας την απόδοση του εξοπλισμού σε πραγματικό χρόνο. Αυτό διασφαλίζει ότι όλος ο εξοπλισμός λειτουργεί όπως πρέπει και μειώνει την πιθανότητα βλάβης ή δυσλειτουργίας κατά τη διάρκεια μιας επιχείρησης.

Προφίλ κινδύνου ανά περιοχή

Τα συστήματα επιχειρηματικής ευφυΐας μπορούν να συλλέγουν και να αναλύουν δεδομένα σχετικά με περιστατικά πυρκαγιάς, δημογραφικά στοιχεία της περιοχής ευθύνης τους, τύπους κτιρίων, ακόμη και οικονομικούς και κοινωνιολογικούς παράγοντες για τον προσδιορισμό των περιοχών που διατρέχουν τον υψηλότερο κίνδυνο για εμφάνιση πυρκαγιάς. Αυτά τα δεδομένα επιτρέπουν στις πυροσβεστικές υπηρεσίες να δημιουργούν στοχευμένα προγράμματα πρόληψης πυρκαγιών που εστιάζουν στην εκπαίδευση των κατοίκων σχετικά με την πυρασφάλεια, διενέργεια επιθεωρήσεων σε περιοχές υψηλού κινδύνου και μεγαλύτερη διάθεση πόρων για την πρόληψη συμβάντων. Αναλύοντας προηγούμενα περιστατικά και δημογραφικά δεδομένα, οι πυροσβεστικές υπηρεσίες μπορούν να αναπτύξουν προγράμματα πυρασφάλειας που αντιμετωπίζουν συγκεκριμένες προκλήσεις, όπως κατοικίες με μεγάλο πληθυσμό, παλιά και ενδεχομένως ηλεκτρικά συστήματα μη καλώς συντηρημένα ή έλλειψη συναγερμών πυρκαγιάς.

Αυτή η προληπτική προσέγγιση όχι μόνο μειώνει τον αριθμό των περιστατικών πυρκαγιάς, αλλά και ενισχύει την ανθεκτικότητα της περιοχής σε ακραίες καταστάσεις.

Μοντέλα Πρόβλεψης Κινδύνου

Μια άλλη πτυχή της λειτουργίας των συστήματα επιχειρηματικής ευφυΐας στη διαχείριση κινδύνων είναι η δημιουργία μοντέλων πρόβλεψης κινδύνου. Αυτά τα μοντέλα χτίζονται αναλύοντας μοτίβα από προηγούμενα περιστατικά και εφαρμόζοντάς τα για την πρόβλεψη μελλοντικών συμβάντων. Για παράδειγμα, εάν ορισμένες καιρικές συνθήκες ή τύποι κτιρίων σχετίζονται με υψηλότερη πιθανότητα πυρκαγιάς, αυτά τα συστήματα μπορούν να επισημάνουν αυτούς τους παράγοντες και να προτρέψουν το Πυροσβεστικό Σώμα να λάβει προληπτικά μέτρα, επιθεωρήσεις, συμβουλές στους ιδιοκτήτες των κτιρίων σχετικά με αναβαθμίσεις πυρασφάλειας ή αύξηση της ευαισθητοποίησης των πολιτών με ημερίδες για ενημέρωση για έκτακτες καταστάσεις.

<u>Επιχειρησιακή αποτελεσματικότητα</u> [4]

Η επιχειρησιακή αποτελεσματικότητα αποτελεί κύριο ζητούμενο για το Πυροσβεστικό Σώμα, καθώς επηρεάζει άμεσα την ικανότητά του να ανταποκρίνεται αποτελεσματικά σε καταστάσεις έκτακτης ανάγκης. Τα εργαλεία επιχειρηματικής ευφυΐας επιτρέπουν

στις Πυροσβεστικές Υπηρεσίες να εξορθολογήσουν τις λειτουργίες τους ενσωματώνοντας διάφορες πηγές δεδομένων, αυτοματοποίηση διοικητικών εργασιών και βελτίωση του επιχειρησιακού συντονισμού.

Κεντρικά συστήματα δεδομένων

Οι πλατφόρμες επιχειρηματικής ευφυΐας ενσωματώνουν δεδομένα από διάφορες πηγές, όπως GPS, μετεωρολογικές προβλέψεις, εφαρμογές πυρασφάλειας, και εργαλεία παρακολούθησης προσωπικού, για να παρέχουν μια ολιστική εικόνα των επιχειρήσεων.

Έλεγχος αποδοτικότητας

Οι πυροσβεστικές υπηρεσίες μπορούν να χρησιμοποιήσουν συστήματα επιχειρηματικής ευφυΐας για να αξιολογήσουν τις επιχειρήσεις των Πυροσβεστικών Υπηρεσιών με βάση δεικτών επιδόσεων (KPI), όπως χρόνοι απόκρισης, επιτυχής επίλυση συμβάντων, και αξιοποίηση πόρων. Παρέχοντας ένα dashboard αυτών των μετρήσεων σε πραγματικό χρόνο, τα συστήματα επιχειρηματικής ευφυΐας επιτρέπουν στις Πυροσβεστικές Υπηρεσίες να παρακολουθούν συνεχώς τις επιδόσεις τους και να εντοπίζουν τομείς στους οποίους μπορούν να γίνουν βελτιώσεις.

Αυτοματοποίηση διοικητικών εργασιών

Ένα άλλο πλεονέκτημα των εργαλείων επιχειρηματικής ευφυΐας είναι η ικανότητά τους να αυτοματοποιούν διοικητικές εργασίες, απελευθερώνοντας το προσωπικό από τη γραφειοκρατία για να επικεντρωθεί σε πυροσβεστικές επιχειρήσεις. Για παράδειγμα, αντί να εισάγουν χειροκίνητα δεδομένα σε αναφορές περιστατικών, Τα εργαλεία επιχειρηματικής ευφυΐας μπορούν αυτόματα να δημιουργήσουν και να κατηγοριοποιήσουν αυτά τα δεδομένα, σε έτοιμες αναφορές και στη συνέχεια η διοίκηση του Πυροσβεστικού Σώματος να έχει πρόσβαση, να αναλύσει πληροφορίες και να αξιολογήσει το αποτέλεσμα.

Αυτή η αυτοματοποιημένη διαδικασία μπορεί να επεκταθεί και στη συντήρηση του εξοπλισμού. Ο εξοπλισμός πυρόσβεσης υφίσταται σημαντική φθορά κατά τη διάρκεια των επιχειρήσεων, και η τακτική συντήρηση είναι απαραίτητη για να διασφαλιστεί ότι λειτουργεί σωστά κατά τη διάρκεια συμβάντων. Οι πλατφόρμες επιχειρηματικής ευφυΐας μπορούν να παρακολουθούν τη χρήση και την απόδοση του εξοπλισμού, και να επισημάνουν όταν απαιτείται συντήρηση ή αλλαγή. Αυτή η προσέγγιση έγκαιρης συντήρησης βοηθά στην πρόληψη βλαβών του εξοπλισμού και του υλικού και διασφαλίζει ότι όλα τα εργαλεία είναι σε άριστη κατάσταση όταν χρειάζονται.

Προϋπολογισμός και κατανομή πόρων

Το Πυροσβεστικό Σώμα λειτουργεί υπό αυστηρούς δημοσιονομικούς περιορισμούς και η αποτελεσματική κατανομή των πόρων είναι ζωτικής σημασίας για να διασφαλιστεί

ότι μπορεί να συνεχίσει να παρέχει υπηρεσίες υψηλής ποιότητας χωρίς υπερβολικές δαπάνες. Τα εργαλεία επιχειρηματικής ευφυΐας βοηθούν τις Διευθύνσεις να βελτιστοποιήσουν τους προϋπολογισμούς τους, παρέχοντας πληροφορίες σχετικά με το πού δαπανώνται τα χρήματα και εντοπίζοντας τομείς όπου μπορεί να επιτευχθεί εξοικονόμηση κόστους.

Προϋπολογισμός βάσει εργαλείων κατανομής πόρων

Τα συστήματα επιχειρηματικής ευφυΐας επιτρέπουν στις Διευθύνσεις να αναλύουν λεπτομερώς τα λειτουργικά τους έξοδα, από το κόστος προσωπικού έως τις αγορές εξοπλισμού και συντήρηση εγκαταστάσεων. Με τον εντοπισμό μοτίβων στις δαπάνες, η διοίκηση μπορούν να λαμβάνει πιο στοχευμένες αποφάσεις σχετικά με το πού να κατανείμει τους πόρους που έχουν χορηγηθεί. Για παράδειγμα, εάν οι αναφορές δείξουν ότι ένας συγκεκριμένος Πυροσβεστικός Σταθμός αντιμετωπίζει συχνότερα αστικά περιστατικά, θα πρέπει να έχει τον κατάλληλο εξοπλισμό για να ανταποκριθεί η δύναμη του Σταθμού σε τέτοιου είδους συμβάντα. Ομοίως, τα συστήματα επιχειρηματικής ευφυΐας μπορούν να παρακολουθούν το κόστος εκπαίδευσης και να βοηθούν τα τμήματα να αξιολογούν την απόδοση τους στο πεδίο.

Συνεργασία Υπηρεσιών

Σε καταστάσεις έκτακτης ανάγκης, η απρόσκοπτη συνεργασία μεταξύ διαφορετικών υπηρεσιών. όπως η πυροσβεστική, η αστυνομία και το Ε.Κ.Α.Β. είναι απαραίτητη. Τα εργαλεία επιχειρηματικής ευφυΐας διευκολύνουν την επικοινωνία ενσωματώνοντας δεδομένα από πολλαπλές πηγές και καθιστώντας τα διαθέσιμα σε όλους τους εμπλεκόμενους σε πραγματικό χρόνο.

Όταν εμπλέκονται πολλοί οργανισμοί στην αντιμετώπιση ενός περιστατικού, τα συστήματα επιχειρηματικής ευφυΐας διασφαλίζουν ότι όλοι έχουν πρόσβαση στις ίδιες πληροφορίες. Για παράδειγμα, κατά τη διάρκεια μιας πυρκαγιάς, η Πυροσβεστική Υπηρεσία μπορεί να χρειαστεί να συντονιστεί με την Αστυνομία για να διαχειριστεί την κυκλοφορία και να διασφαλίσει την ασφάλεια των πολιτών. Η ύπαρξη μιας κοινής πλατφόρμας όπου τα δεδομένα ενημερώνονται σε πραγματικό χρόνο επιτρέπει σε όλους τους οργανισμούς να συνεργάζονται αποτελεσματικά. Σε καταστάσεις έκτακτης ανάγκης με περιστατικά μεγάλης κλίμακας, όπως πυρκαγιές ή φυσικές καταστροφές, η επιχειρηματική ευφυΐα μπορεί επίσης να βελτιώσει τον συντονισμό σε περιφερειακό ή εθνικό επίπεδο.

Δυνατότητα Διαβάθμισης

Ο διαχειριστής του συστήματος μπορεί να εκχωρήσει διαφορετικό επίπεδο δυνατοτήτων στους χρήστες. Ανάλογα με τα καθήκοντα και το βαθμό τους. Ο υπεύθυνος ενός τμήματος ή γραφείου έχει πλήρη πρόσβαση στον αντίστοιχο φάκελο του τμήματος του για να μπορεί σε αυτόν τον φάκελο να παράγει αναφορές, να διαβάζει αναφορές συναδέλφων, να στέλνει αναφορές στους ανώτερους του και γενικά

να επεξεργάζεται και να παράγει πληροφορία. Αντίστοιχα, ο Διοικητής του θα μπορεί να διαβάζει μόνο τις αναφορές που παράγει και δουλεύει το τμήμα το οποίο διοικεί.

Δημιουργία ομάδων

Υπάρχει η δυνατότητα να δημιουργηθούν ομάδες, στις οποίες θα έχουν πρόσβαση οι χρήστες ανάλογα με την υπηρεσία που διατελούν. Με αυτόν τον τρόπο επιτυγχάνεται στόχευση της πληροφορίας σε ομάδες χρηστών ανάλογα με τα καθήκοντά τους.

Δημιουργία βαθμών

Υπάρχει η δυνατότητα να οριστούν βαθμοί, και να αποδοθούν στους χρήστες του συστήματος με τα αντίστοιχα δικαιώματα. Ανάλογα με το βαθμό που έχει ο κάθε χρήστης θα έχει πρόσβαση σε διαφορετικό επίπεδο πληροφορίας και δυνατοτήτων στο σύστημα. Έτσι επιτυγχάνεται διαβάθμιση της πληροφορίας.

Παραδείγματα χρήσης εργαλείων επιχειρηματικής [6]

.

Χρήση εργαλείων επιχειρηματικής ευφυΐας από την Πυροσβεστική Υπηρεσία της Virginia των Ηνωμένων Πολιτειών Αμερικής

Στόχος χρήσης εργαλείων επιχειρηματικής ευφυΐας

Η Πυροσβεστική Υπηρεσία της Virginia των Ηνωμένων Πολιτειών Αμερικής έχει αναγνωρίσει από το 2020 την ανάγκη να χρησιμοποιεί τα πιο σύγχρονα εργαλεία για πετύχει τους στόχους της και σύμφωνα με τον Dr. Evgeniy Ivanov, διευθυντή τμήματος έρευνας της Πυροσβεστικής Υπηρεσίας της Virginia, «να αναγνωριστεί η Πυροσβεστική Υπηρεσία της Virginia ως ηγέτης στην πυρόσβεση, με τη δυνατότητα να προβλέπει αναδυόμενα και απαιτητικά περιβάλλοντα, να αναπτύξει τις ικανότητες των μελών της, και να καλλιεργήσει το αίσθημα της ασφάλειας ανάμεσα στην κοινότητα».

Τι σημαίνει επιχειρηματική ευφυΐα για την Πυροσβεστική Υπηρεσία

Σύμφωνα με τον ίδιο, τα δεδομένα μιας Πυροσβεστικής Υπηρεσίας καλύπτουν όλους τους λειτουργικούς τομείς εσωτερικά και εξωτερικά, όπως για παράδειγμα ανθρώπινο δυναμικό, πυροσβεστικές επιχειρήσεις, επιθεωρήσεις, ασφάλεια, οικονομικά, κ.α. Επιπλέον, η ικανότητα χρήσης εργαλείων επιχειρηματικής ευφυΐας θα βοηθήσει την Υπηρεσία να εξερευνήσει όλα αυτά τα δεδομένα με δομημένο τρόπο. Έτσι, θα δώσει τη δυνατότητα σε όλους τους διευθυντές που επιβλέπουν αυτούς τους τομείς να λαμβάνουν τεκμηριωμένες αποφάσεις, και να βελτιώσουν τις διαδικασίες για να πετύχουν τους στόχους τους.

Τα στοιχεία που απαρτίζουν τη χρήση επιχειρηματικής ευφυΐας

Η χρήση επιχειρηματικής ευφυΐας μπορεί να γίνει πετυχημένα με το συνδυασμό τριών στοιχείων: Τα εργαλεία επιχειρηματικής ευφυΐας, την εκπαίδευση στη χρήση τους, και τους αναλυτές, οι οποίοι θα μετουσιώσουν τα δυο προηγούμενα στοιχεία σε λύσεις μέσω αναφορών και ταμπλό (dashboards)

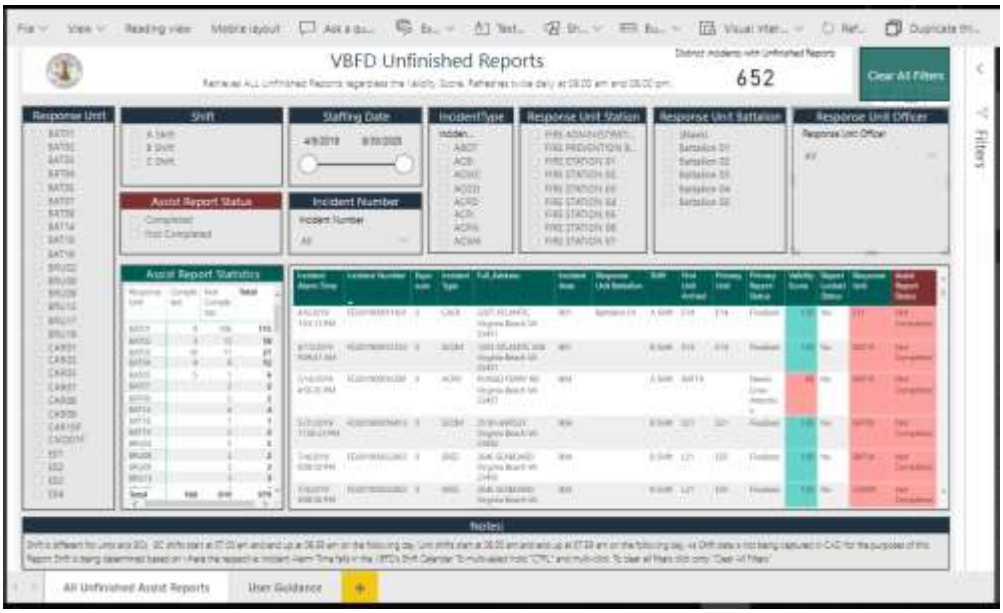
Στην περίπτωση της Πυροσβεστικής Υπηρεσίας της Virginia, η ομάδα επιχειρηματικής ευφυΐας στεγάζεται στο γραφείο Έρευνας και Ανάλυσης. Απαρτίζεται από δυο αναλυτές του πολιτικού προσωπικού, ο ένας ασχολείται με την έρευνα και ο άλλος είναι διαχειριστής της Βάσης Δεδομένων της Υπηρεσίας, και επιβλέπονται από έναν επιπυραγό, οποίος επιβλέπει και προσφέρει την επιχειρησιακή εμπειρία.

Πυροσβεστικό Σώμα

Η Πυροσβεστική τους Υπηρεσία χρησιμοποιεί τρείς αναφορές, που περιγράφονται στις επόμενες παραγράφους.

Εντοπισμός μη ολοκληρωμένων αναφορών

Ένας επιπυραγός επιθυμεί να βλέπει τις αναφορές οι οποίες δεν έχουν ολοκληρωθεί. Χωρίς τη χρήση εργαλείων επιχειρηματικής ευφυΐας, κάποιος από τη διεύθυνση πληροφορικής θα παρήγαγε αυτήν την πληροφορία, η οποία θα έφτανε μόνο στον επιπυραγό. Με τη χρήση εργαλείων επιχειρηματικής ευφυΐας, αυτή η πληροφορία μπορεί να κοινοποιηθεί σε περισσότερους ανθρώπους, οι οποίοι πρέπει να είναι ενήμεροι. Το συγκεκριμένο ταμπλό (dashboard) δημιουργήθηκε μετά από συζητήσεις ανάμεσα στην επιχειρησιακή ομάδα, για τον προσδιορισμό της μη ολοκληρωμένης αναφοράς, και έχει την παρακάτω μορφή, όπως φαίνεται στην επόμενη εικόνα

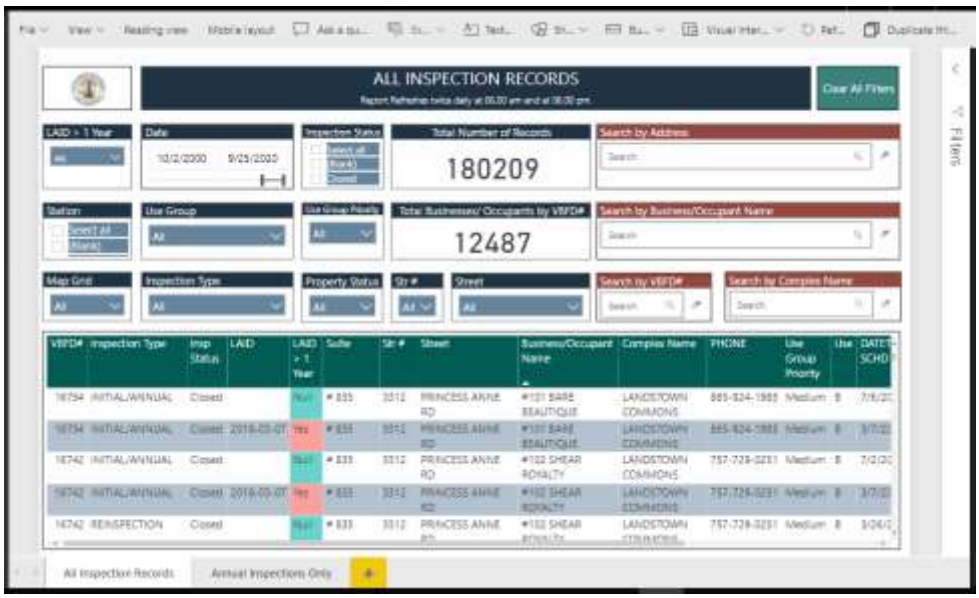


Dashboard με μη ολοκληρωμένες αναφορές της Πυροσβεστικής Υπηρεσίας της Virginia (Staff, F. (2024) Is your department business intelligent? FirefighterNation. Διαθέσιμο από: https://www.firefighternation.com/firerescue/is-your-department-business-intelligent/ (Προσπελάστηκε: 5 Οκτωβρίου 2024))

Εντοπισμός επιθεωρήσεων πυρασφάλειας

Όλοι γνωρίζουν πόσο σημαντικές είναι οι επιθεωρήσεις για την πυρασφάλεια για την προστασία των επιχειρήσεων. Ταυτόχρονα, αυτή η διαδικασία προσφέρει χρήματα στον δημόσιο τομέα. Συνεπώς η καταγραφή των επιθεωρήσεων πυρασφάλειας με έξυπνο και αποδοτικό τρόπο είναι απαραίτητη. Η Πυροσβεστική τους Υπηρεσία έχει δημιουργήσει ένα dashboard το οποίο αποτελείται από δυο καρτέλες, η μια δείχνει τις εγγραφές των επιθεωρήσεων πυρασφάλειας και η άλλη τις ετήσιες επιθεωρήσεις. Επιπλέον γίνεται ένας έλεγχος αν η τελευταία επιθεώρηση πυρασφάλειας είναι παλαιότερη του ενός έτους. Αυτό θα ήταν ένας τρόπος να δοθεί προτεραιότητα για επιθεώρηση σε αυτές τις επιχειρήσεις. Ένας άλλος τρόπος με τον οποίο μπορεί να δοθεί προτεραιότητα για επιθεώρηση είναι ανάλογα με τη σημασία τους για την ασφάλεια του κοινού. Για αυτόν τον λόγο έχουν δημιουργήσει το πεδίο “Use Group priority” (Προτεραιότητα ομάδας κοινού) στο οποίο έχουν δώσει τις τιμές “High”, “Medium”, και “Low” («Υψηλή», «Μέτρια», και «Χαμηλή» αντίστοιχα).

Για παράδειγμα, τα εκπαιδευτικά ιδρύματα έχουν υψηλή προτεραιότητα, οι χώροι εστίασης μέτρια προτεραιότητα και οι ιδιωτικές κατοικίες χαμηλή προτεραιότητα για επιθεώρηση πυρασφάλειας. Εν τέλει, αυτό το ταμπλό (dashboard) μπορεί να χρησιμοποιηθεί από τον Υπάλληλο της Πυροσβεστικής Υπηρεσίας ο οποίος διεξάγει επιθεώρηση πυρασφάλειας για να δημιουργήσει μια λίστα με επιθεωρήσεις ανάλογα με την προτεραιότητα προς επιθεώρηση, ανά χρόνο ή μήνα, να εντοπίσει χώρους στους οποίους δεν έχει γίνει επιθεώρηση, ή η επιθεώρηση είναι ημιτελής, και όλα αυτά με χρήση ηλεκτρονικών μέσων, χωρίς απαραίτητα να χρησιμοποιεί κάποιο έντυπο, όπως φαίνεται στην επόμενη εικόνα.

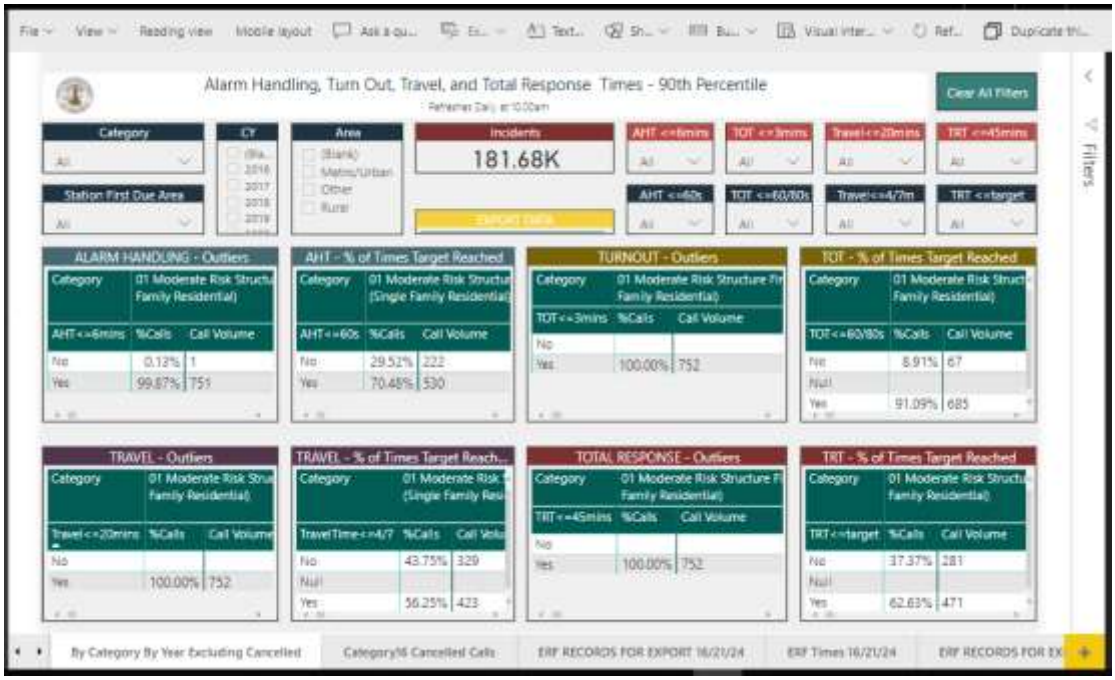


Dashboard με επιθεωρήσεις πυρασφάλειας της Πυροσβεστικής Υπηρεσίας της Virginia Staff, F. (2024) Is your department business intelligent? FirefighterNation. Διαθέσιμο από: https://www.firefighternation.com/firerescue/is-your-department-business-intelligent/ (Προσπελάστηκε: 5 Οκτωβρίου 2024))

Αυτοματοποίηση διαδικασίας υπολογισμού χρόνου απάντησης

Η διαδικασία υπολογισμού χρόνου απάντησης είναι ιδιαίτερα απαιτητική και χρονοβόρα. Χωρίς τη χρήση εργαλείων επιχειρηματικής ευφυΐας, αυτός ο υπολογισμός θα απαιτούσες κάθε φορά τον υπολογισμό από τη βάση δεδομένων του χρόνου μεταφοράς στο σημείο και του χρόνου απάντησης για όλα τα συμβάντα.

Στη συνέχεια θα έπρεπε κανείς να υπολογίσει αυτούς τους χρόνους ανά ημερολογιακό έτος, ανά πιθανότητα κινδύνου, ανά περιοχή, κ.λ.π. Όλοι αυτοί οι υπολογισμοί θα έπρεπε να γίνονται κάθε φορά που απαιτείται αυτή η πληροφορία. Με τη χρήση εργαλείων επιχειρηματικής ευφυΐας, αυτή η διαδικασία μπορεί να γίνει μία φορά και στη συνέχεια αυτή η πληροφορία να ανανεώνεται αυτόματα, και κατά απαίτηση, όπως φαίνεται στην επόμενη εικόνα.



Dashboard με χρόνους απάντησης της Πυροσβεστικής Υπηρεσίας της Virginia (Staff, F. (2024) Is your department business intelligent? FirefighterNation. Διαθέσιμο από: https://www.firefighternation.com/fireresc ue/is-your-department-business-intelligent/ (Προσπελάστηκε: 5 Οκτωβρίου 2024))

Συμπεράσματα

Αδιαμφισβήτητα, το έργο του Πυροσβεστικού Σώματος είναι ιδιαίτερα σημαντικό, αλλά και πολύπλοκο. Τα μέλη του καλούνται να πάρουν σημαντικές αποφάσεις σε σύντομο χρονικό διάστημα, είτε βρίσκονται στο πεδίο και επιχειρούν είτε βρίσκονται στο γραφείο

και λαμβάνουν αποφάσεις. Από την ανάλυση των τεχνικών και των εργαλείων της επιχειρηματικής ευφυΐας, όπως προκύπτει και από τις πηγές, η επιχειρηματική ευφυΐα μπορεί να βοηθήσει τόσο στο τεχνικό μέρος. προσφέροντας ταχύτητα και ακρίβεια στην επεξεργασία δεδομένων, με στόχο τη λήψη αποτελεσματικότερων αποφάσεων, όσο και σε διοικητικό, δίνοντας πρόσβαση στην πληροφορία στους κατάλληλους ανθρώπους, εύκολα και με ακρίβεια.

Αναφορές

1	Αποστολή του Πυροσβεστικού Σώματος (2016) Αποστολή - Αρμοδιότητες - Πυροσβεστικό Σώμα Ελλάδος. Διαθέσιμο από: https://www.fireservice.gr/el_GR/apostole-armodiotetes (Προσπελάστηκε: 2 Οκτωβρίου 2024).
2	Frankenfield, J. (χωρίς ημερομηνία) What is Business Intelligence (BI)? types, benefits, and examples, Investopedia. Διαθέσιμο από: https://www.investopedia.com/terms/b/business-intelligence-bi.asp (Προσπελάστηκε: 5 Οκτωβρίου 2024).
3	Team, P.B. (2024) What is business intelligence: Microsoft Power bi, What Is Business Intelligence | Microsoft Power BI. Διαθέσιμο από: https://powerbi.microsoft.com/en-us/what-is-business-intelligence (Προσπελάστηκε: 2 Οκτωβρίου 2024).
4	FirePlus (2021) Ranking a firefighting operation's Business Intelligence: Provident FirePlus, Provident FirePlus | Provident FirePlus. Διαθέσιμο από: https://www.providentfireplus.com/ranking-firefighting-operations-business-intelligence (Προσπελάστηκε: 5 Οκτωβρίου 2024).
5	Data and Business Intelligence Guidance (2023) NFCC. Διαθέσιμο από: https://nfcc.org.uk/our-services/community-risk-programme/data-and-business-intelligence-guidance/ (Προσπελάστηκε: 5 Οκτωβρίου 2024).
6	Staff, F. (2024) Is your department business intelligent? FirefighterNation. Διαθέσιμο από: https://www.firefighternation.com/firerescue/is-your-department-business-intelligent/ (Προσπελάστηκε: 5 Οκτωβρίου 2024).

Βιογραφικό συντάκτη

Ο Υποπυραγός Κωνσταντίνος Μαρκούτης είναι απόφοιτος του Τμήματος Πληροφορικής του Πανεπιστημίου Πειραιά με Κατεύθυνση στα Διαδικτυακά και Υπολογιστικά Συστήματα ΚΑΙ κάτοχος Μεταπτυχιακού τίτλου στα Προηγμένα Συστήματα Πληροφορικής του ιδίου Πανεπιστημίου. Από το 2014 έως το 2022 συμμετείχε σε έργα επιχειρηματικής ευφυΐας στο δημόσιο και ιδιωτικό τομέα, στην Ελλάδα και στο εξωτερικό, σε χώρους όπως δημόσιοι φορείς, τραπεζικός, τηλεπικοινωνιακός, φαρμακευτικός, ασφαλιστικός. Σήμερα υπηρετεί στη Διεύθυνση Πληροφορικής του Πυροσβεστικού Σώματος.

ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Ολοκλήρωση Επιμορφωτικών Προγραμμάτων Η/Υ ΔΙΜΑ και ΦΠ

Στις 14 Ιουν 24 και 21 Ιουν 24 ολοκληρώθηκαν τα Επιμορφωτικά Προγράμματα για το Πολιτικό Προσωπικό του ΥΠΕΘΑ με ΔΙΜΑ και ΦΠ: «Βασικό Επίπεδο Γνώσεων Υπολογιστικών Φύλλων Excel Ι», «Βασικές Δεξιότητες Βάσεων Δεδομένων Access», «Βασικό Επίπεδο Γνώσεων Επεξεργασίας Κειμένου Word Ι», Η εκπαίδευση εκάστου είχε διάρκεια μία εβδομάδα και συμμετείχαν συνολικά σε αυτά 26 Μόνιμοι Υπάλληλοι..

Επίσκεψη της 143 Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών στο ΚΕΠΥΕΘΑ και το ΚΕΠΥΕΣ

Στις 25 Ιουνίου 2024 πραγματοποιήθηκε επίσκεψη της 143ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών της ΣΠΗΥ, στο ΚΕΠΥΕΘΑ και το ΚΕΠΥΕΣ. Οι σπουδαστές της Σχολής ενημερώθηκαν για την αποστολή και το έργο των δύο Μονάδων και είχαν την ευκαιρία να γνωρίσουν τη δομή και τη λειτουργία των πληροφοριακών συστημάτων που υποστηρίζουν.

Παρουσίαση Πτυχιακών Εργασιών της 143ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών

Στις 26 Ιουνίου 2024 πραγματοποιήθηκε στη ΣΠΗΥ, παρουσίαση πτυχιακών εργασιών της 143ης Εκπαιδευτικής Σειράς Αναλυτών-Προγραμματιστών, παρουσία του Δκτή του ΚΕΠΥΕΣ Συνταγματάρχη (ΕΠ) Αντωνίου Κόγια. Οι εργασίες των σπουδαστών αφορούσαν την ανάπτυξη εφαρμογών διαδικτύου και τεχνητής νοημοσύνης. Στο περιθώριο της εκδήλωσης τιμήθηκαν με αναμνηστική πλακέτα, από το Δκτή της ΣΠΗΥ, Συνταγματάρχη (ΕΠ) Δημήτριο Ντόντο, ο Ταξχος εα κ. Χρήστος Κολαΐτης και ο καθηγητής κ. Παυλάτος Χρήστος προς αναγνώριση της πολυετούς συνεισφοράς τους στο εκπαιδευτικό έργο της Σχολής. Παρόντες στην παρουσίαση πλην του Δκτή του ΚΕΠΥΕΣ και του Δκτή της ΣΠΗΥ, ήταν εκπρόσωποι και επιτελείς του ΚΕΠΥΕΣ, του ΚΕΤΑΚ, του ΓΕΝ/Ε3, της ΣΠΗΥ, καθώς και καθηγητές της Σχολής.

Αποφοίτηση της 143ης Εκπαιδευτικής Σειράς Αξιωματικών Αναλυτών-Προγραμματιστών

Στις 28 Ιουνίου 2024 πραγματοποιήθηκε στη ΛΑΕΔ, η αποφοίτηση της 143ης Εκπαιδευτικής Σειράς Αξκών Αναλυτών-Προγραμματιστών της ΣΠΗΥ, παρουσία του Υδντή του ΓΕΣ/ΔΔΒ-ΕΠ Ταξιάρχου Γρηγορίου Γκουτζέλη, ο οποίος απένειμε τα πτυχία στους αποφοιτήσαντες.

Στην ίδια τελετή τιμήθηκε με αναμνηστική πλακέτα, από το Δκτή της ΣΠΗΥ, Συνταγματάρχη (ΕΠ) Δημήτριο Ντόντο, ο Συνταγματάρχης ε.α. Ιωάννης Καλαϊτζάκης προς αναγνώριση της πολυετούς πολύτιμης συνεισφοράς του στο εκπαιδευτικό έργο της Σχολής.

Στην τελετή παρευρέθηκαν επιτελείς του του ΓΕΣ/ΔΔΒ-ΕΠ, του ΓΕΝ/Β2, του ΓΕΑ//Γ5, της ΣΠΗΥ, καθώς και καθηγητές της Σχολής.




Ολοκλήρωση Επιμορφωτικών Προγραμμάτων Η/Υ ΔΙΜΑ και ΦΠ

Στις 27 Σεπ 24 και 11 Οκτ 24 ολοκληρώθηκαν τα Επιμορφωτικά Προγράμματα Η/Υ ΔΙΜΑ και ΦΠ «Χειρισμός Η/Υ, Διαχείρισης Αρχείων, Περιήγησης στο Διαδίκτυο και Χρήσης Ηλεκτρονικού Ταχυδρομείου», «Βασικό Επίπεδο Γνώσεων Υπολογιστικών Φύλλων Excel Ι», «Εφαρμογή παρουσιάσεων Power Point», «Βασικό Επίπεδο Γνώσεων Επεξεργασίας Κειμένου, Word Ι, για άτομα κωφά και βαρήκοα, με διερμηνέα νοηματικής γλώσσας», για το Πολιτικό Προσωπικό του ΥΠΕΘΑ. Η εκπαίδευση κάθε σεμιναρίου διήρκησε μία εβδομάδα και συμμετείχαν συνολικά σε αυτά 65 Μόνιμοι Υπάλληλοι. Ολοκλήρωση Επιμορφωτικών Προγραμμάτων Η/Υ ΔΙΜΑ και ΦΠ.


Εσωτερικοί Αγώνες Bowling ΣΠΗΥ

Στις 24 Οκτ 24 πραγματοποιήθηκαν για πρώτη φορά αγώνες Bowling της ΣΠΗΥ. Στους αγώνες συμμετείχαν στελέχη και σπουδαστές της Σχολής. Στους νικητές απονεμήθηκαν έπαθλα.



Ολοκλήρωση Επιμορφωτικών Προγραμμάτων Η/Υ ΔΙΜΑ και ΦΠ

Στις 25 Οκτ 24 ολοκληρώθηκε το Επιμορφωτικό Πρόγραμμα Η/Υ ΔΙΜΑ και ΦΠ, «Υπηρεσίες Διαδικτύου Επίπεδο Ι», για το Πολιτικό Προσωπικό του ΥΠΕΘΑ. Η εκπαίδευση του κάθε προγράμματος διήρκησε μία εβδομάδα και συμμετείχαν συνολικά 32 Μόνιμοι Υπάλληλοι.

Αποφοίτηση Σχολείου Διαχειριστών Πληροφοριακών Συστημάτων (Β΄ ΕΣ 2024)

Στις 25 Οκτ 24, στην έδρα της Σχολής, πραγματοποιήθηκε η τελετή αποφοίτησης του Σχολείου Διαχειριστών Πληροφοριακών Συστημάτων (Β΄ ΕΣ 2024). Συνολικά αποφοίτησαν έντεκα (11) στελέχη του ΣΞ, τέσσερα (4) του ΠΝ, τρία (3) της ΠΑ, δύο (2) ΝΟΜ του ΓΕΕΘΑ, δύο (2) του ΓΕΕΦ και ένας (1) Πολιτικός Υπάλληλος

Ολοκλήρωση Επιμορφωτικών Προγραμμάτων Η/Υ ΔΙΜΑ, για το Πολιτικό Προσωπικό του ΥΠΕΘΑ

Στις 25 Οκτ 24 ολοκληρώθηκε το Επιμορφωτικό Πρόγραμμα Η/Υ ΔΙΜΑ, «Υπηρεσίες Διαδικτύου Επίπεδο Ι, Εισαγωγή Και Ασφάλεια Διαδικτύου». Στις 15 Νοε 24, ολοκληρώθηκαν τα Επιμορφωτικά Προγράμματα Η/Υ ΔΙΜΑ, «Υπηρεσίες Διαδικτύου Επίπεδο ΙΙ», «Προχωρημένο Επίπεδο Γνώσεων Υπολογιστικών Φύλλων EXCEL ΙΙ» και με ΦΠ «Εφαρμογή παρουσιάσεων Power Point». Στις 29 Νοε 24, ολοκληρώθηκε το Επιμορφωτικό Πρόγραμμα Η/Υ ΔΙΜΑ, «Βασικές Δεξιότητες Βάσεων Δεδομένων Access». Η διάρκεια των εκπαιδευτικών προγραμμάτων ήταν μία εβδομάδα έκαστο και συμμετείχαν συνολικά 76 Μόνιμοι Πολιτικοί Υπάλληλοι.

Συμμετοχή των σπουδαστών του Τμήματος Αναλυτών – Προγραμματιστών 144 ΕΣ της ΣΠΗΥ στο 14ο e-Government Forum

Οι σπουδαστές του Τμήματος Αναλυτών – Προγραμματιστών της ΣΠΗΥ παρακολούθησαν το 14ο e-Government Forum, που πραγματοποιήθηκε το διήμερο 06-07 Νοε 2024 στο Ξενοδοχείο Divani Caravel της Αθήνας. Βασικός θεματικός τίτλος του συνεδρίου ήταν «Η Τεχνητή Νοημοσύνη προ των Πυλών της Δημόσιας Διοίκησης: Προετοιμασία, Αξιοποίηση, Οφέλη». Οι σπουδαστές είχαν την ευκαιρία να ενημερωθούν για τις σύγχρονες τάσεις των εφαρμογών της πληροφορικής στη δημόσια διοίκηση, με έμφαση στην ενσωμάτωση της τεχνητής νοημοσύνης σε αυτές.

Συμμετοχή των σπουδαστών της ΣΠΗΥ σε ομιλία με θέμα, ‘’Η Επιχειρησιακή Διάσταση του Κυβερνοχώρου και οι Υβριδικές Απειλές’’

Στις 15 Νοεμβρίου 2024, ο Data Protection Officer του Υπουργείου Ψηφιακής Διακυβέρνησης Κος Αθανάσιος Κοσμόπουλος, πραγματοποίησε διάλεξη με θέμα ‘’Η Επιχειρησιακή Διάσταση του Κυβερνοχώρου και οι Υβριδικές Απειλές’’. Οι σπουδαστές της σχολής ενημερώθηκαν για τις σύγχρονες απειλές στον κυβερνοχώρο και τη στρατηγική αντιμετώπισης τους.

Ολοκλήρωση Επιμορφωτικού Προγράμματος Η/Υ με Φ.Π, για το Πολιτικό Προσωπικό του ΥΠΕΘΑ

Στις 29 Νοε 24 ολοκληρώθηκε το Επιμορφωτικό Πρόγραμμα Η/Υ «Υπηρεσίες Διαδικτύου Επίπεδο ΙΙ: Εισαγωγή και Ασφάλεια Πληροφοριακών Συστημάτων». Η διάρκεια του Επιμορφωτικού Προγράμματος Η/Υ ήταν μία εβδομάδα και συμμετείχαν συνολικά εννέα (9) Μόνιμοι Πολιτικοί Υπάλληλοι.

Ολοκλήρωση Σεμιναρίου Υπασπιστών Διοίκησης επ΄ ωφελεία της ΑΣΔΥΣ

Στις 05 Δεκ 24 ολοκληρώθηκε το Σεμινάριο Υπασπιστών Διοίκησης επ΄ ωφελεία της ΑΣΔΥΣ διάρκειας μίας ημέρας.

Ολοκλήρωση Σχολείου ΧΕΜΕ

Στις 06 Δεκ 24 ολοκληρώθηκε το Σχολείο Χειριστών Επιστρατευτικής Μηχανογραφικής Εφαρμογής «ΕΦΕΔΡΟΣ» (ΧΕΜΕ). Εκπαιδεύτηκαν 28 στελέχη στο χειρισμό των λειτουργιών υποστήριξης των διαδικασιών της επιστράτευσης.

Όροι Συνεργασίας

Σκοπός

Το περιοδικό «ΗΛΕΚΤΡΟΝΙΟ» εκδίδεται από τη ΣΠΗΥ κάθε εξάμηνο με σκοπό την προώθηση πληροφοριών σχετικά με τις εξελίξεις στο χώρο της πληροφορικής και τις εφαρμογές της.

Η θεματολογία του περιοδικού περιλαμβάνει κείμενα σχετικά με:

- επιστημονικές εργασίες
- εφαρμογές της πληροφορικής
- νέες μεθοδολογίες και τεχνικές
- την ιστορική εξέλιξη της πληροφορικής
- τις δραστηριότητες της Σχολής

Τα κείμενα που δημοσιεύονται εκφράζουν τον συντάκτη και δεν απηχούν απαραίτητα τις απόψεις της Σχολής.

Τα προς δημοσίευση άρθρα θα πρέπει να πληρούν τους παρακάτω κανόνες:

- Τα κείμενα δεν θα πρέπει να υπερβαίνουν τις 5.000 λέξεις. Επιπλέον θα πρέπει να περιλαμβάνουν επαρκή τεκμηρίωση και βιβλιογραφία.
- Η υποβολή των κειμένων θα πρέπει να γίνεται σε ηλεκτρονική επεξεργάσιμη μορφή στη διεύθυνση ηλεκτρονικού ταχυδρομείου sphy_3@army.gr.
- Οι συντάκτες των άρθρων θα πρέπει να υποβάλλουν και ένα σύντομο βιογραφικό (με φωτογραφία προαιρετικά) το οποίο θα προστίθεται στο τέλος του κειμένου.
- Τα κείμενα δεν θα πρέπει να περιλαμβάνουν διαβαθμισμένες πληροφορίες.