Τεύχος 15 | Σεπτέμβριος 2024
ISSN 2732-7701

eΆλληλον

Χτίζοντας το μέλλον

Ένθετο Α:
Κυβερνοασφάλεια: Προκλήσεις και Προοπτικές στην Ψηφιακή Εποχή

Ένθετο Β:
Ασφάλεια και Ανθεκτικότητα

Ένθετο Γ:
Το Βήμα των Ομιλητών μας
Ενεργειακή Μετάβαση

ΜΗΝΥΜΑ ΕΚΔΟΤΗ

Άγγελος Παγκράτης
Ιδρυτής και Πρόεδρος ΔΕ της ΑΛΛΗΛΟΝ, Εκδότης του e-Άλληλον
Πρώην Επιτετραμμένος της ΕΕ στις ΗΠΑ και πρώην πρέσβης της ΕΕ στην Αργεντινή και στον Παγκόσμιο Οργανισμό Εμπορίου
Angelos Pangratis | LinkedIn

Αγαπητά μέλη, φίλοι και φίλες της ΑΛΛΗΛΟΝ,

Με την έναρξη του νέου ακαδημαϊκού έτους, η πρόοδος της ΑΛΛΗΛΟΝ συνεχίζεται δυναμικά. Το προηγούμενο έτος έκλεισε με δύο πολύ επιτυχημένες εκδηλώσεις: Η πρώτη, που πραγματοποιήθηκε στις αρχές Ιουνίου σε συνεργασία με τη Μόνιμη Ελληνική Αντιπροσωπεία (ΜΕΑ) Γενεύης, επικεντρώθηκε αποκλειστικά σε συναντήσεις speed mentoring. Η συμμετοχή των νέων ήταν εξαιρετική. Παράλληλα, αυτή η πρωτοβουλία εμβάθυνε τη συνεργασία μας με τη ΜΕΑ Γενεύης και την Ελληνική Διπλωματική Ακαδημία. Η δεύτερη εκδήλωση έγινε τον Ιούλιο σε συνεργασία με την Ideagen και το ACS. Η ΑΛΛΗΛΟΝ συμμετείχε με ένα εξαιρετικό πάνελ ομιλητών για την ενεργειακή μετάβαση στην Ελλάδα. Τα βίντεο των συνεντεύξεων έχουν ήδη συγκεντρώσει δεκάδες χιλιάδες προβολές στο YouTube, επιβεβαιώνοντας την απήχηση και τη σημασία του θέματος.

Οι προτεραιότητες που παρουσιάζονται στα ένθετα του περιοδικού μας θα αποτελέσουν και τους άξονες των επικείμενων εκδηλώσεών μας. Στο τρέχον τεύχος, **το Ένθετο Α** είναι αφιερωμένο στην Κυβερνοασφάλεια. Συνιστώ την σε βάθος μελέτη των άρθρων και του μηνύματος του προσκεκλημένου εκδότη μας, Ελευθέριου Αθουσάκη. Η Κυβερνοασφάλεια θα είναι και θέμα μελλοντικής μας εκδήλωσης με κάποιο πανεπιστήμιο. Το **Ένθετο Β** έχει ως κεντρικό θέμα την Ασφάλεια και Ανθεκτικότητα. Είναι συνέχεια του αντίστοιχου ενθέτου του προηγούμενου τεύχους. Σας προτρέπω να ξεκινήσετε την ανάγνωση από το μήνυμα του προσκεκλημένου εκδότη μας, Γεώργιου Κουκάκη. Ήδη προβλέπουμε για την Άνοιξη μια εκδήλωση σχετικά με την ελληνική αμυντική βιομηχανία.

Το Ένθετο Γ είναι το Βήμα των Ομιλητών μας και επικεντρώνεται, για ακόμα μία φορά, στο ζήτημα της Ενεργειακής Μετάβασης όπου ήδη έχουμε κάνει σημαντικές εκδηλώσεις. Συνιστώ να μελετήσετε το σημείωμα του εκδότη στο ένθετο αυτό, καθώς και τις δύο παρουσιάσεις που αποτελούν πραγματικά ιστορικά ντοκουμέντα. Στο πλαίσιο της ενεργειακής μετάβασης, αναδύεται ένα καίριο ερώτημα: Γιατί η Ελλάδα είναι η μόνη χώρα στην περιοχή της και στην Ευρωπαϊκή Ένωση που δεν αξιοποιεί τον φυσικό της πλούτο φυσικού αερίου; Το ερώτημα αυτό εγείρει και ένα τεράστιο **ζήτημα δημοκρατίας**, καθώς τόσο σημαντικές αποφάσεις για το μέλλον της χώρας θα πρέπει να λαμβάνονται με τη μεγαλύτερη δυνατή συναίνεση και υποστήριξη της κοινωνίας και ίσως με δημοψήφισμα. Σίγουρα όχι αποφάσεις που λαμβάνονται πίσω από κλειστές πόρτες και με αδιαφανή συμφέροντα. Στο προηγούμενο τεύχος του περιοδικού είχαμε τονίσει σαν συμπέρασμα την ανάγκη διαμόρφωσης μιας διακομματικής Εθνικής Στρατηγικής, τουλάχιστον εν μέρει εμπνευσμένης από το επιτυχημένο παράδειγμα της Νορβηγίας, η οποία καταφέρνει να συνδυάσει την πράσινη μετάβαση με την πλήρη εκμετάλλευση των ενεργειακών της αποθεμάτων, προς όφελος των πολιτών της, καλύπτοντας ένα μεγάλο μέρος των αναγκών σε φυσικό αέριο της ΕΕ. Τα στοιχεία που δημοσιεύουμε στο παρόν τεύχος επιβεβαιώνουν εκ νέου αυτό το συμπέρασμα.

Ευχαριστούμε θερμά όλους όσους συνέβαλαν στη δημιουργία του τεύχους αυτού. Με τη στήριξή τους, συνεχίζουμε να χτίζουμε γέφυρες γνώσης και συνεργασίας για ένα καλύτερο αύριο.

Άγγελος Παγκράτης

Impressum

ΕΚΔΟΤΗΣ:
ΑΛΛΗΛΟΝnet
Άγγελος Παγκράτης

ΤΑΧΥΔΡΟΜΙΚΗ ΔΙΕΥΘΥΝΣΗ:
ΑΛΛΗΛΟΝNet
Εθνική Οδός Λευκίμης 6, Κέρκυρα, Ελλάδα

ΑΡΧΙΣΥΝΤΑΚΤΗΣ:
Χρήστος Μπεζιρτζόγλου

ΣΥΝΤΑΚΤΙΚΗ ΟΜΑΔΑ:
Φιλαρέτη Πάκα

ΣΥΜΒΟΥΛΕΥΤΙΚΗ ΟΜΑΔΑ:
Δημήτρης Ηλιόπουλος,
Κλεάνθης Γαβριηλίδης,
Όλγα Κοσμίδου

ΟΜΑΔΑ ΕΠΙΚΟΙΝΩΝΙΑΣ:
Αλέξανδρος Παγκράτης

ΓΡΑΦΙΣΤΙΚΗ ΕΠΕΞΕΡΓΑΣΙΑ & ΕΠΙΜΕΛΕΙΑ ΕΞΩΦΥΛΛΟΥ:
Χριστίνα Μπαγκάκη

EMAIL ΕΠΙΚΟΙΝΩΝΙΑΣ:
periodiko@allilonet.gr

ΙΣΤΟΣΕΛΙΔΑ:
https://allilonnet.com/

Linkedin:
https://www.linkedin.com/company/allilon/

ISSN: 2732-7701

COVER & BACKCOVER:
shared by creators on pexels.com (royalty free)

ΠΕΡΙΕΧΟΜΕΝΑ

Γενικά Άρθρα

«Λαμπάδια έχοντες διαδώσουσιν άλλήλοις»

(Οι φέροντες τις δάδες τις μεταλαμπαδεύουν ο ένας στον άλλον). Φράση από την «Πολιτεία» του Πλάτωνος, στη μετατροπή της εισόδου στο Πανεπιστήμιο του Yale.

Το περιοδικό υποστηρίζει και προωθεί τους στόχους της ΑΛΛΗΛΟΝ με τα γενικά, τα θεματικά (ένθετα) και άλλα άρθρα του κάθε τεύχους. Οι κύριοι στόχοι της ΑΛΛΗΛΟΝ είναι:

1ος στόχος: Να υποστηρίζει ατομικά τις προσπάθειες των μελών μας και ιδίως των νέων μας που προετοιμάζονται και αγωνίζονται για ένα καλύτερο επαγγελματικό μέλλον.

2ος στόχος: Να κτίζει συνοχή και πνεύμα εθελοντισμού, αλληλεγγύης και αλληλοϋποστήριξης μεταξύ των μελών της καθώς και με άλλους φορείς με τους οποίους συνεργάζεται στην Ελλάδα και στο εξωτερικό.

3ος στόχος: Να συμβάλει, μέσα σε ένα διεθνές πλαίσιο τεχνολογικής επιτάχυνσης, αλλά και τριβών, συγκρούσεων και ανατροπών στην απαραίτητη προετοιμασία και προσαρμογή, μελών και συνεργατών και, ευρύτερα, στην πρόοδο και ανθεκτικότητα της Ελλάδας και του Ελληνισμού.

Η μετα-κοινωνία απειλεί τη δημοκρατία

Κωνσταντίνος Παπαλίτσας
Structural Civil Engineer, MEng, MSc | Project Manager, MSc | e-tutor
Konstantinos Papalitsas | LinkedIn

Περίληψη

Ζούμε στην εποχή της τεχνολογικής εξέλιξης. Τα τελευταία χρόνια με τη ραγδαία ανάπτυξη της τεχνολογίας έχει αλλάξει άρδην ο τρόπος που χρησιμοποιούμε το διαθέσιμο χρόνο μας (εργασία, διασκέδαση κλπ) καθώς έχει μεταβληθεί σημαντικά ο τρόπος που αλληλεπιδρούμε μεταξύ μας. Η τηλεργασία σε τομείς όπως η πληροφορική, η εκπαίδευση αλλά ακόμη και η ιατρική (τηλεϊατρική) έχει δώσει άλλη υπόσταση στο επιδιωκόμενο και πολυσυζητημένο work-life balance.

Τα τεχνολογικά επιτεύγματα που επηρεάζουν όλο και μεγαλύτερα τμήματα του πληθυσμού είναι σε θέση πλέον να καθορίζουν διάφορες εκφάνσεις της προσωπικής αλλά και της επαγγελματικής μας ζωής και μέσα σε όλο αυτό το κλίμα ευρύτερων αλλαγών αλλάζει σταδιακά και η ίδια η κοινωνία.

Στη σημερινή εποχή, όσο ποτέ άλλοτε, ακούμε και διαβάζουμε συνεχώς όλο και περισσότερες λέξεις με το πρόθεμα μετά- στην αρχή τους. Χαρακτηριστικά παραδείγματα είναι η μετα-πολιτική, ο μετα-πολιτισμός, η μετα-τεχνολογία, τα μετα-δεδομένα κ.α. Επιπλέον ενδεικτικό παράδειγμα αποτελεί η πασίγνωστη πλατφόρμα Facebook η οποία μετονομάστηκε σε Meta θέλοντας να καταδείξει τη μετά-βαση σε ένα νέο ψηφιακό περιβάλλον δραστηριοτήτων το λεγόμενο Metaverse. Το πρόθεμα μετά- περιγράφει μια αλλαγή από ένα περιβάλλον σε κάποιο άλλο και αυτό μπορεί να έχει είτε θετικά, είτε αρνητικά αποτελέσματα ανάλογα τη χρήση που του κάνει κάποιος. Εξάλλου οι τρεις βασικές λέξεις που χρησιμοποιούνται ευρέως με το συγκεκριμένο πρόθεμα είναι οι λέξεις μετάβαση, μεταβολή και μετατροπή οι οποίες αμφότερες αντιπροσωπεύουν τροποποιήσεις προς το μέλλον.

Είναι προφανές ότι η παραπάνω εξέλιξη εάν συνδυαστεί με ελεγχόμενη και στοχευμένη ανάπτυξη μπορεί να βελτιώσει σημαντικά την ποιότητα ζωής των ανθρώπων, την οποία υποτίθεται ότι πρέπει να υπηρετούν όλα αυτά τα μετα-στοιχεία. Οι προβληματισμοί ξεκινούν από το σημείο που το εν λόγω πρόθεμα χρησιμοποιείται ώστε να οδηγήσει τις εξελίξεις προς ορισμένη κατεύθυνση, καθώς κανένας δεν μπορεί να εγγυηθεί προς το παρόν ότι οι πραγματοποιούμενες διεργασίες αποσκοπούν στο ευρύτερο κοινωνικό συμφέρον.

Στον τομέα της τεχνολογίας για παράδειγμα το επερχόμενο metaverse δεν είναι κάτι μονοδιάστατα ορισμένο καθώς εκμεταλλευόμενοι τις δυνατότητες της τεχνητής νοημοσύνης (A.I.) μπορούμε να δημιουργήσουμε διαφορετικές εκδοχές του ανάλογα με τις επιθυμίες του εκάστοτε χρήστη. Αυτή η δυναμική τεχνολογική δυνατότητα που οδηγεί στη δημιουργία πολλών εναλλακτικών metaverses συγχέει ακόμη περισσότερο την κατάσταση σχετικά με τη χρησιμότητα όλων αυτών των διεργασιών.

Εάν δηλαδή το πρόθεμα μετά- εκτός από την πρόοδο προς το μέλλον αρχίσει να αντιπροσωπεύει δυναμικές καταστάσεις που μετα-βάλλονται από αρχάριους χρήστες τότε τι μας εξασφαλίζει ότι δεν μπορεί να δημιουργηθούν εναλλακτικές μορφές μεταπολιτικής, εναλλακτικοί μεταπολιτισμοί, εναλλακτικές μετατεχνολογίες και τελικά να μεταβούμε σταδιακά σε νέες μορφές κοινωνιών που θα ονομαστούν μετα-κοινωνίες;

Απειλείται η Δημοκρατία;

Η δημιουργία μετακοινωνιών με τη σειρά της εάν δεν γίνει πάνω σε συγκεκριμένες αρχές και αξίες φαντάζει τρομακτική και μπορεί να γίνει ακόμη χειρότερη στη περίπτωση που μέσω αυτού του δαιδαλώδους συστήματος αρχίσουν να αμφισβητούνται βασικές αρχές του πολιτεύματος που έχει εγκαθιδρυθεί στην πλειοψηφία των χωρών παγκοσμίως, της ίδιας της Δημοκρατίας.

Ήδη έχουν ακουστεί εκφράσεις όπως ο μετ-άνθρωπος, ένα υβρίδιο που κανείς δεν ξέρει πως θα συμπεριφερθεί όταν θα κληθεί να αντιμετωπίσει ηθικά και κοινωνικά ζητήματα όπως η αγάπη, το ενδιαφέρον, ο σεβασμός ή ακόμα και θεμελιώδη ζητήματα του δημοκρατικού πολιτεύματος όπως η αρχή της πλειοψηφίας, η ελευθερία της έκφρασης, η ισότητα, ο σεβασμός στη διαφορετικότητα, η δικαιοσύνη κ.α. Η μετά-βαση βέβαια έχει ήδη ξεκινήσει καθώς η συντριπτική πλειοψηφία των ανθρώπων παγκοσμίως χρησιμοποιεί τεχνολογικές συσκευές με κυρίαρχο το κινητό τηλέφωνο (smartphone) το οποίο έχει γίνει προέκταση του σώματός μας. Η υπερβολική του χρήση μας έχει καταστήσει ήδη πρώιμους μετανθρώπους καθώς πλήθος αντιδράσεών μας βασίζονται στη λειτουργία και τις δυνατότητες των συσκευών αυτών. Φαντάζει τρομερά δύσκολο να μπορέσει κάποιος να δράσει στη σύγχρονη εποχή χωρίς τη χρήση αυτών των τεχνολογικών εργαλείων, η οποία σταδιακά κανονικοποιήθηκε και πλέον θεωρείται αυτονόητη. Η συνεχής αλληλεπίδραση όμως των ανθρώπων με τα εργαλεία αυτά μέσω της διευκόλυνσης των καθημερινών λειτουργιών που τα τελευταία προσφέρουν, δημιουργεί τεράστια ποσά δεδομένων (big data) των οποίων η διαχείριση δύναται να καθορίσει μελλοντικές αλλαγές στην ίδια την κοινωνία.

Η δημοκρατικότητα της κοινωνίας εξελίσσεται δυναμικά και απαιτεί ευρεία συμμετοχή κάτι που είναι αντίθετο με τη λογική διαχείρισης των big data όπου επιχειρείται τυποποίηση των πάντων μέσω κατηγοριοποίησης. Επιπρόσθετα εάν εξετάσουμε σε βάθος τα meta data, θα διαπιστώσουμε πως η ευρεία χρήση τους κατευθύνει το χρήστη σε προαποφασισμένες ενέργειες, γεγονός που έχει ως αποτέλεσμα να συρρικνώνεται η δυνατότητα πρωτοβουλιών, ελεύθερης δημιουργίας και έκφρασης. Όλα τα παραπάνω δύνανται να αλλοιώσουν ένα από τα βασικά χαρακτηριστικά του δημοκρατικού πολιτεύματος που είναι η δυνατότητα επιλογής στη διαδικασία λήψης αποφάσεων και ως εκ τούτου να θέσουν εν αμφιβόλω την ανθρώπινη συμμετοχή σε μια διαρκώς μεταβαλλόμενη κοινωνία όπου τα τεχνολογικά επιτεύγματα έχουν πλέον τον πρώτο λόγο σχεδόν σε όλες τις εκφάνσεις της.

Τα τεχνολογικά επιτεύγματα δηλαδή συμμετέχουν ενεργά στη διαμόρφωση των προσωπικών απόψεων του καθενός γύρω από πάσης φύσεως θέματα και οι επικείμενες αντιδράσεις μπορούμε να πούμε ότι είναι πλέον περισσότερο ατομικές παρά συλλογικές όπως ορίζει η βασική αρχή της συμμετοχικής δημοκρατίας. Συνυπολογίζοντας δε ότι η διαχείριση των εφαρμογών και των δεδομένων απαιτεί εξειδικευμένες γνώσεις οφείλουμε να βάλουμε στη συζήτηση και την ακούσια ή εκούσια περιθωριοποίηση στις πλατιάς μάζας των πολιτών-χρηστών η οποία πλήττει κάθε έννοια ισότητας.

Κίνδυνος είναι η παραπάνω κατάσταση σε συνδυασμό με την πολυδιαφημιζόμενη μεταπολιτική να οδηγήσει σε μια νέα μορφή μετα-δημοκρατίας η οποία θα χαρακτηρίζεται από αλλοίωση των ηθικών αρχών και της ελεύθερης διακίνησης των ιδεών.

Τελικά υπάρχει λύση;

Σύμφωνα λοιπόν με τα παραπάνω το μέλλον προβλέπεται αρκετά δυσοίωνο όμως σε καμία περίπτωση η εξέλιξη δεν πρέπει να σταματήσει. Ο άνθρωπος από τη φύση του πάντα επιδίωκε την πρόοδο και την εξέλιξη και κάπως έτσι δημιουργήθηκαν οι πρώτες πολιτισμένες κοινωνίες που στη συνέχεια μέσω αρχών και κανόνων

μετασχηματίστηκαν σε δημοκρατικές. Πολλές φορές μάλιστα η εξέλιξη είναι αναπόφευκτη παρά τη σθεναρή αντίδραση κάποιων κοινωνικών ομάδων, καθώς η γενική ανάγκη για πρόοδο και βελτίωση της κοινωνικής ζωής πάντοτε υπερίσχυε των όποιων προσωπικών ενστάσεων μπορεί να έχει κάποιος ως άτομο.

Η ανάγκη αυτή λοιπόν είναι σχεδόν σίγουρο ότι θα οδηγήσει τον άνθρωπο στο επόμενο στάδιο, δημιουργώντας μια νέα μορφή κοινωνίας (μετά-κοινωνίας ή κάτι παρόμοιο), αρκεί η τελευταία να στηριχθεί σε ισχυρές βάσεις και αρχές με τις οποίες διακατέχονται οι δημοκρατικές κοινωνίες των ανεπτυγμένων κρατών.

Τον τρόπο για να γίνει αυτό τον δείχνει το ίδιο το δημοκρατικό πολίτευμα το οποίο έχει ως θεμελιώδη αρχή του κράτους δικαίου τη διάκριση των εξουσιών (Νομοθετική, Δικαστική, Εκτελεστική). Δυστυχώς μέχρι στιγμής οι απλοί πολίτες δεν έχουν λόγο για όλες τις παραπάνω προαναφερόμενες εξελίξεις και το γεγονός αυτό ενέχει τον κίνδυνο να παίρνονται αποφάσεις εκτός δημοκρατικών θεσμών. Η κατάσταση χειροτερεύει καθώς η πληροφορία είναι μεν μόνο ένα κλικ μακριά μας εκδημοκρατίζοντας την πρόσβαση στη γνώση αλλά από την άλλη η αυξημένη πληροφόρηση οδηγεί νομοτελειακά και σε αυξημένη παραπληροφόρηση.

Οι εφαρμογές τεχνητής νοημοσύνης και η ανεξέλεγκτη ανάπτυξη της τεχνολογίας συγχέουν ακόμη περισσότερο το τοπίο καθώς γίνεται όλο και πιο δύσκολο για τον καθένα μας να διαχωρίσουμε το πραγματικό από το κατασκευασμένο. Έτσι έννοιες όπως η αγάπη, το ενδιαφέρον, η τέχνη, η ηθική, οι αξίες κλπ κινδυνεύουν να χαθούν στη δίνη της τεχνητής παραπληροφόρησης και έτσι να τείνουν μειούμενα τα βασικά στοιχεία προόδου μιας δημοκρατικής κοινωνίας που είναι η εμπιστοσύνη και η συνεργασία μεταξύ των μελών της.

Κατ' αυτόν τον τρόπο γίνεται αντιληπτό ότι είναι δυνατόν μελλοντικά χαθεί η διάδραση μεταξύ τεχνολογικών εργαλείων και ανθρώπου ώστε να σταματήσει ο τελευταίος να είναι το επίκεντρο των δημοκρατικών διεργασιών. Δεν αποκλείεται δηλαδή οι τρεις δημοκρατικές εξουσίες να αποκτήσουν τέτοια εξάρτηση από την τεχνολογία και να εκχωρήσουν την πλειοψηφία των αρμοδιοτήτων τους σε αυτή ώστε σε λίγα χρόνια κανείς να μη μπορεί να αποκλείσει το γεγονός πως η θέσπιση και η εφαρμογή των νόμων και των κανονισμών καθώς και οι αποφάσεις τη δικαιοσύνης δεν θα είναι καθαρά και μόνο αποτέλεσμα λειτουργίας αλγορίθμων.

Εάν όμως οι τρεις δημοκρατικές εξουσίες λειτουργήσουν ανεξάρτητα και σε συνδυασμό με τη θέσπιση καθολικά αποδεκτών ανεξάρτητων αρχών, μέσα στα πλαίσια μιας κοινωνίας πανανθρώπινων αξιών τότε είναι δυνατή η δημιουργία ενός θεσμικού πλαισίου που θα ενσωματώσει όλες αυτές τις αλλαγές με τρόπο ωφέλιμο για τους πολίτες και ταυτόχρονα να γίνει σταδιακά αποδεκτό από όλους αποτελώντας το απόλυτο δημοκρατικό εχέγγυο υπέρ της δικαιοσύνης και της ισότητας.

Άλλωστε η ίδια η λέξη δημοκρατία (χωρίς το πρόθεμα μετά-) αποτελεί σύνθεση των λέξεων δήμος, που παραπέμπει στην κοινωνία, και κράτος, που παραπέμπει στην δύναμη και την κυριαρχία, γεγονός που καταδεικνύει τον τρόπο με τον οποίο πρέπει πάντα να θεσμοθετούνται οι κοινωνικές αλλαγές στα δημοκρατικά πολιτεύματα.

Κλείνοντας, λαμβάνοντας υπόψη ότι η τεχνολογική εξέλιξη είναι ένα ακόμη ανθρώπινο κατασκεύασμα όπως είναι το χρήμα, τα κράτη, οι εκκλησίες, οι Ανώνυμες Εταιρείες κλπ, χρησιμοποιείται και αυτή με τη σειρά της ώστε να αναπτύξει νέους δεσμούς μεταξύ των μελών μιας κοινωνίας. Συνεπώς θα πρέπει να την αντιμετωπίσουμε με το βασικό ερώτημα που αντιμετωπίζουμε όλα τα προαναφερθέντα ανθρώπινα κατασκευάσματα: Κατά πόσο η τεχνολογική εξέλιξη και πρόοδος διευκολύνει τη ζωή των ανθρώπων και εάν τους κάνει πιο ευτυχισμένους;

Χρήση της Ευρωπαϊκής Πρωτοβουλίας Πολιτών για τη δημιουργία ενός Ευρωπαϊκού Δήμου και την προώθηση αλλαγών στην Ευρώπη

Χρήστος Μπεζιρτζόγλου
Μέντορας Καριέρας ΑΛΛΗΛΟΝ
Στέλεχος Ευρωπαϊκής Επιτροπής
Christos Bezirtzoglou | Linkedin

Περίληψη

Η Ευρώπη και η Ελλάδα βρίσκονται σε ένα σταυροδρόμι. Οι ερχόμενοι μήνες θα είναι καθοριστικοί για την μελλοντική κατεύθυνση του Ευρωπαϊκού σχεδίου. Το 2024 είναι ένα έντονα πολιτικό έτος με σημαντικές προκλήσεις, όπως η ανάδειξη της νέας Ευρωπαϊκής Επιτροπής και οι εκλογές στο Ευρωπαϊκό Κοινοβούλιο.

Οι πολίτες είναι στην καρδιά όλων αυτών ερωτημάτων και αποφάσεων. Οι πολίτες θα πρέπει να ορίζουν τον δρόμο που θα ακολουθήσουν οι αντιπρόσωποι τους. Οι καιροί που η πολιτική γινόταν με σιωπηρή συγκατάθεση τελείωσαν και οι πολίτες εμπλέκονται ενεργά σε ανοικτές πρωτοβουλίες διαβουλεύσεων για τα δικαιώματα τους και το που & πως θα ήθελαν να δουν την Ευρώπη την επόμενη δεκαετία.

Η ενεργή υποστήριξη Ευρωπαϊκών Πρωτοβουλιών Πολιτών από πολίτες, αλλά και από πολιτικούς σχηματισμούς και μη κυβερνητικούς οργανισμούς, μπορεί να γίνει η πεμπτουσία της προώθησης του κοινωνικού διαλόγου και μέσω αυτού η ανάδειξη θεμάτων που απασχολούν την κοινωνία ευρύτερα ή ειδικότερα τμήματα αυτής. Οι ενέργειες αυτές αναμένεται να συμβάλουν στην αναβάθμιση του δημοσίου διαλόγου, στις προϋποθέσεις άσκησης βάσιμης πολιτικής κριτικής, στη διαφάνεια και τελικά στη βελτίωση των πολιτικών που σχεδιάζονται και εφαρμόζονται στην Ευρώπη και κατά προέκταση και στην Ελλάδα.

Εισαγωγή

Η Ευρωπαϊκή Ένωση (ΕΕ) χρειάζεται μεταρρύθμιση. Η Διάσκεψη για το Μέλλον της Ευρώπης και οι Ομάδες Ευρωπαίων Πολιτών κατέδειξαν ότι οι πολίτες μπορούν να αποτελέσουν την κινητήρια δύναμη πίσω από πολύπλοκες αλλαγές που πρέπει να υποστεί η ΕΕ, είτε για την προετοιμασία της ΕΕ για πιθανή διεύρυνση σε 30+ κράτη μέλη είτε για την προώθηση αναγκαίων θεσμικών μεταρρυθμίσεων. Παρά αυτή τη δυναμική, τόσο οι υπεύθυνοι λήψης αποφάσεων της ΕΕ όσο και οι εθνικοί φορείς λήψης αποφάσεων φαίνεται να διστάζουν να αξιοποιήσουν πλήρως τη συμμετοχή των πολιτών. Η συμμετοχική δημοκρατία στην ΕΕ χτυπά ένα αόρατο ανώτατο όριο που μπορεί να

σπάσει μόνο εάν οι πολιτικοί και οι υπεύθυνοι λήψης αποφάσεων σε ευρωπαϊκό και εθνικό επίπεδο αναγνωρίσουν και αντιμετωπίσουν τα βαθύτερα αίτια που εμποδίζουν την ανάπτυξη.

Ωστόσο, ένα εργαλείο που υπάρχει από το 2012 έχει αποδείξει την αξία του, επιτρέποντας σε απλούς πολίτες να διαμορφώσουν την ατζέντα της Ευρωπαϊκής Επιτροπής. Το εργαλείο αυτό είναι οι Ευρωπαϊκές Πρωτοβουλίες Πολιτών (ΕΠΠ).

"Πολίτες της Ένωσης, εφόσον συγκεντρωθεί αριθμός τουλάχιστον ενός εκατομμυρίου, υπήκοοι σημαντικού αριθμού κρατών μελών, μπορούν να λαμβάνουν την πρωτοβουλία να καλούν την Ευρωπαϊκή Επιτροπή, στο πλαίσιο των αρμοδιοτήτων της, να υποβάλλει κατάλληλες προτάσεις επί θεμάτων στα οποία οι εν λόγω πολίτες θεωρούν ότι απαιτείται νομική πράξη της Ένωσης για την εφαρμογή των Συνθηκών." Άρθρο 11.4 της Συνθήκης για την Ευρωπαϊκή Ένωση.

Ιστορικό της Ευρωπαϊκής Πρωτοβουλίας Πολιτών

Η Ευρωπαϊκή Πρωτοβουλία Πολιτών (ΕΠΠ), η οποία εισάχθηκε για πρώτη φορά με την Συνθήκη της Λισσαβώνας το 2012, είναι το πρώτο και μοναδικό εργαλείο που επιτρέπει στους πολίτες από όλες τις χώρες της ΕΕ να ενώνουν τις δυνάμεις τους και να ζητούν νομοθετικές αλλαγές σε ευρωπαϊκό επίπεδο για θέματα που θεωρούν σημαντικά. Η ΕΠΠ παρέχει στους πολίτες της ΕΕ τη δυνατότητα να συμμετέχουν σε διασυνοριακό επίπεδο σε ζητήματα κοινού ενδιαφέροντος.

Το πεδίο εφαρμογής αυτού του εργαλείου καλύπτει τομείς πολιτικής στους οποίους η Ευρωπαϊκή Επιτροπή έχει την εξουσία να προτείνει νομοθεσία. Αυτοί είναι το περιβάλλον, η γεωργία, οι μεταφορές, η προστασία των καταναλωτών, τα κοινωνικά δικαιώματα, αλλά και άλλοι τομείς που επηρεάζουν τη ζωή των ανθρώπων.

Μόλις μια πρωτοβουλία λάβει ένα εκατομμύριο υπογραφές και οι υπογραφές επαληθευτούν από τις εθνικές αρχές, το Σώμα των Επιτρόπων εγκρίνει επίσημη απάντηση στην πρωτοβουλία, με την οποία αποφασίζει ποια δράση πρέπει να αναληφθεί ή όχι και γιατί. Στη συνέχεια, η πρωτοβουλία χαρακτηρίζεται «επιτυχημένη».

Στόχοι της Ευρωπαϊκής Πρωτοβουλίας Πολιτών

Η ΕΠΠ είναι ένας μοναδικός μηχανισμός που έχει ως στόχο να φέρει σε επαφή τους ανθρώπους πέρα από τα σύνορα και να τους δώσει μια συγκεκριμένη πλατφόρμα για να μοιραστούν κοινές ανησυχίες και αξίες. Κάθε πολίτης της ΕΕ έχει το δικαίωμα να υποστηρίξει μια εν εξελίξει πρωτοβουλία ή να ξεκινήσει μια δική του. Αυτό δημιουργεί μια αίσθηση ενότητας, συμμετοχής και εταιρικής σχέσης, προωθώντας παράλληλα τις δημοκρατικές αξίες της ΕΕ.

Από την ίδρυσή της το 2012, περισσότεροι από 1850 διοργανωτές, από τους οποίους 51 ήταν Έλληνες και 12 Κύπριοι, έχουν ξεκινήσει 100+ πρωτοβουλίες ευρωπαίων πολιτών, με την ενεργή παρουσία 26 Ελλήνων και 5 Κυπρίων, συλλέγοντας περισσότερες από 18 εκατομμύρια υπογραφές από όλη την ΕΕ, με περισσότερες από 197 χιλιάδες στην Ελλάδα και 14 χιλιάδες στην Κύπρο, οι οποίες αφορούν διαφορετικούς τομείς πολιτικής: από την καλή μεταχείριση των ζώων και την φορολογία έως τις κοινωνικές υποθέσεις και τα θεμελιώδη δικαιώματα.

Οι διοργανωτές χρησιμοποίησαν την πλατφόρμα για να προωθήσουν και να προκαλέσουν συζήτηση σε σημαντικά ζητήματα κοινού διακρατικού ενδιαφέροντος, ευαισθητοποιώντας την κοινή γνώμη και αλληλοεπιδρώντας με την πολιτική εξουσία. Με άλλα λόγια, οι Ευρωπαϊκές Πρωτοβουλίες Πολιτών επηρεάζουν τη νομοθεσία της ΕΕ και δημιουργούν έναν Ευρωπαϊκό Δήμο.

Μέχρι στιγμής, δώδεκα πρωτοβουλίες έχουν φτάσει στο όριο του ενός εκατομμυρίου έγκυρων υποστηρικτικών υπογραφών. Δέκα από αυτές έχουν ήδη λάβει απάντηση από την Ευρωπαϊκή Επιτροπή. Όλες οι πρωτοβουλίες ήταν επιτυχείς στον στόχο τους να προκαλέσουν συζήτηση γύρω από συγκεκριμένα θέματα, ενώ κάποιες από αυτές κατόρθωσαν να επηρεάσουν την ευρωπαϊκή νομολογία. Από τις επιτυχημένες πρωτοβουλίες, τρεις έφτασαν το κατώφλι του πληθυσμού στην Ελλάδα (14805) "Right2Water", "One of us" and "Stop finning-Stop the trade" και μόλις μία "One of us" στην Κύπρο (4230).

Πώς μπορείτε να εμπλακείτε με την Ευρωπαϊκή Πρωτοβουλία Πολιτών;

Οι ΕΠΠ μπορούν να δρομολογηθούν με τη συγκρότηση μιας "ομάδας διοργανωτών" τα μέλη της οποίας προέρχονται από τουλάχιστον επτά κράτη-μέλη της ΕΕ. Η πρωτοβουλία ελέγχεται από την Ευρωπαϊκή Επιτροπή ως προς την νομιμότητα του αιτήματος της πριν αρχίσει τη συλλογή υπογραφών υποστήριξης.

Αφότου συγκεντρωθούν 1 εκατομμύριο υπογραφές και αφού αυτές επαληθευτούν στη συνέχεια από τις αρμόδιες εθνικές αρχές, η Ευρωπαϊκή Επιτροπή θα εξετάσει την αίτηση και θα στείλει μια επίσημη απάντηση, με την οποία επισημαίνει ποια δράση πρέπει να αναληφθεί ή όχι, και γιατί.

Η σχολική εργαλειοθήκη της δημοκρατίας στην Ευρωπαϊκή Ένωση

Σκοπός της διαδραστικής εργαλειοθήκης «Η δημοκρατία της ΕΕ σε δράση — Πείτε την άποψή σας με την Ευρωπαϊκή Πρωτοβουλία Πολιτών» που οργάνωσε η Ευρωπαϊκή Επιτροπή το 2023 για τα σχολεία είναι να εφοδιάσει τους μαθητές της δευτεροβάθμιας εκπαίδευσης με τις γνώσεις και τις δεξιότητες που θα τους επιτρέψουν να είναι ενεργοί και υπεύθυνοι πολίτες της ΕΕ.

Η εργαλειοθήκη περιλαμβάνει τέσσερις θεματικές ενότητες, καθεμιά από τις οποίες καλύπτει διαφορετικό αντικείμενο, περνώντας από

τις πιο γενικές πληροφορίες σχετικά με την ΕΕ σε πληροφορίες και δραστηριότητες που σχετίζονται ειδικά με την ΕΠΠ.

Η εργαλειοθήκη έχει σχεδιαστεί για να βοηθήσει τους μαθητές της δευτεροβάθμιας εκπαίδευσης να κατανοήσουν τα οφέλη της διασυνοριακής συνεργασίας και ενδεχομένως να δρομολογήσουν τις δικές τους πρωτοβουλίες για τη διαμόρφωση της δημοκρατικής διαδικασίας στην Ευρωπαϊκή Ένωση.

Μάθετε περισσότερα για την Ευρωπαϊκή Πρωτοβουλία Πολιτών

Για να μάθετε περισσότερα σχετικά με την ΕΠΠ και ίσως να βρείτε έμπνευση για να ξεκινήσετε τη δική σας πρωτοβουλία, μπορείτε να δείτε τις πρωτοβουλίες που επί του παρόντος συγκεντρώνουν υπογραφές αλλά και να ακούσετε πραγματικές ιστορίες οργανωτών ΕΠΠ στο podcast «CitizenCentral». Μην ξεχάσετε να υποστηρίξετε τις πρωτοβουλίες που σας «μιλάνε»!

Ανακαλύψτε τα τελευταία στατιστικά στοιχεία για την ΕΠΠ και συνεργαστείτε με τους τοπικούς πρεσβευτές ή τα εθνικά σημεία επαφής σε Ελλάδα και Κύπρο.

Λοιπόν, τι περιμένετε; Διαδώστε το μήνυμα, στηρίξτε τις εν εξελίξει πρωτοβουλίες, και εάν έχετε μια ιδέα, ξεκινήστε μια νέα ΕΠΠ! Με αυτά τα εύκολα βήματα, το μέλλον της δημοκρατικής διαδικασίας της Ευρωπαϊκής Ένωσης βρίσκεται στα χέρια σας!

Βιβλιογραφία

https://www.academia.edu/37789625/Existing_Direct_Democracy_Tools_in_the_EU_The_European_Citizens_Initiative_as_an_Improvable_Effort

https://www.academia.edu/21171872/Strengthening_the_Idea_of_By_Citizens_for_Citizens_in_the_Context_of_the_European_Citizens_Initiative_Brief_Analysis_of_Initiatives

https://www.academia.edu/12161915/Cahiers_de_recherche_politique_de_Bruges_The_European_Citizens_Initiative_A_First_Assessment

https://www.academia.edu/17849630/The_European_Citizens_Initiative_ECI_entrusting_civil_society_participation_versus_enhancing_the_democratic_legitimacy_of_the_EU_institutions

https://www.academia.edu/74657926/The_European_Citizens_initiative_too_much_democracy_for_EU_polity

https://www.academia.edu/42644649/The_European_citizens_initiative_Over_one_million_support_and_what_next

https://www.academia.edu/67699807/Fulfilling_High_Hopes_The_Legitimacy_Potential_of_the_European_Citizens_Initiative

https://www.academia.edu/11719634/The_European_Citizens_Initiative_a_Misnomer

https://www.academia.edu/39500542/The_European_citizens_initiative_Lost_in_admissibility

https://www.academia.edu/35976136/Methodological_aspects_of_measuring_the_effectiveness_of_the_EU_participatory_mechanisms_the_case_of_the_European_citizens_initiative

Ένθετο Α: Κυβερνοασφάλεια: Προκλήσεις και Προοπτικές στην Ψηφιακή Εποχή

Μήνυμα Προσκεκλημένου Εκδότη

Κυβερνοασφάλεια: προκλήσεις και προοπτικές στην ψηφιακή Εποχή

Ελευθέριος Αθουσάκης
Μέντορας ΑΛΛΗΛΟΝ (Τομέα Κυβερνοασφάλειας)
Ειδικός σε θέματα Κυβερνοασφάλειας
Eleftherios A. | Linkedin

Η κυβερνοασφάλεια έχει αναδειχθεί σε κρίσιμο ζήτημα στη σύγχρονη ψηφιακή εποχή, καθώς ο κόσμος μας γίνεται ολοένα και πιο διασυνδεδεμένος. Με την εκθετική αύξηση των ψηφιακών συσκευών, την ευρεία χρήση του διαδικτύου και την αυξανόμενη εξάρτηση από ψηφιακά συστήματα σε όλους τους τομείς της ζωής μας, η ανάγκη για προστασία από κυβερνοαπειλές έχει καταστεί επιτακτική. Οι κυβερνοεπιθέσεις μπορούν να έχουν καταστροφικές συνέπειες, από την κλοπή προσωπικών δεδομένων και οικονομικές απώλειες μέχρι τη διατάραξη κρίσιμων υποδομών και την απειλή της εθνικής ασφάλειας. Συνεπώς, η κυβερνοασφάλεια δεν αποτελεί πλέον μόνο τεχνικό ζήτημα, αλλά έχει εξελιχθεί σε θεμελιώδη πυλώνα για τη διαφύλαξη της ψηφιακής μας ακεραιότητας και ευημερίας. Στο ένθετο αυτού του τεύχους θεωρήσαμε αναγκαίο ν αναφερθούμε στον τομέα της κυβερνοασφάλειας καθότι και ο Οκτώβρης έχει θεσπιστεί ως μήνας Κυβερνοασφάλειας από την ΕΕ.

Κάτω από αυτή την ομπρέλα έχουμε συμπεριλάβει τέσσερα (4) άρθρα με σκοπό την ενημέρωση σας.

1. Του κυρίου Π. Σούλου
2. Του κυρίου Δ. Γεωργίου
3. Του κυρίου Κ. Νασόπουλου

και του υπογράφοντα.

Το άρθρο του κυρίου Π. Σούλου μας εισάγει στην έννοια της «Κυβερνοϋγιεινής» και αναδεικνύει τη σημασία της εφαρμογής της στην καθημερινή μας ζωή. Ο συγγραφέας τονίζει πώς η υιοθέτηση πρακτικών κυβερνοϋγιεινής μπορεί να θωρακίσει τόσο εμάς όσο και τον περίγυρό μας απέναντι στους πολυάριθμους κινδύνους του ψηφιακού κόσμου ώστε να μας καταστήσει πιο ασφαλείς.

Στο άρθρο του ο κύριος Δ. Γεωργίου αναλύει τις κυβερνοεπιθέσεις σε επιχειρήσεις, εστιάζοντας στην πρόληψη, αντιμετώπιση και διερεύνηση. Τονίζει τη σημασία της κυβερνοασφάλειας ως στρατηγικό ζήτημα και παρουσιάζει βασικές πρακτικές πρόληψης, όπως η ανάπτυξη στρατηγικής ασφαλείας, τακτικές αξιολογήσεις κινδύνου, πολιτικές πρόσβασης, προστασία δεδομένων και εκπαίδευση προσωπικού. Αναφέρεται στην αντιμετώπιση περιστατικών μέσω σχεδίων απόκρισης και συνεργασίας με ειδικούς. Τέλος, υπογραμμίζει τη σημασία της ψηφιακής εγκληματολογίας στη διερεύνηση επιθέσεων και την ενίσχυση της συνολικής ασφάλειας των επιχειρήσεων.

Σε επαφή με το προηγούμενο άρθρο ο κύριος Κ. Νασόπουλος αναλύει τη σημασία και τις εφαρμογές της Ψηφιακής Εγκληματολογίας και Αντιμετώπισης Περιστατικών (DFIR) στην καθημερινότητα. Τονίζει τον ρόλο του DFIR στην προστασία προσωπικών δεδομένων, την ασφάλεια στο διαδίκτυο και την εξιχνίαση εγκλημάτων. Επισημαίνει τη σημασία του στον επιχειρηματικό τομέα για την προστασία εταιρικών δεδομένων και τη συμμόρφωση με κανονισμούς. Αναφέρεται στη χρήση του DFIR για την ασφάλεια έξυπνων συσκευών και την ανάκτηση δεδομένων. Τέλος, παρουσιάζει τις προκλήσεις που αντιμετωπίζει ο τομέας, όπως οι εξελισσόμενες απειλές, και τις μελλοντικές τάσεις, συμπεριλαμβανομένης της ενσωμάτωσης τεχνητής νοημοσύνης και μηχανικής μάθησης στις τεχνικές DFIR.

Τέλος στο άρθρο του υπογράφοντα θα βρείτε περιστατικά που συνέβησαν το τελευταίο χρονικό διάστημα σε διαφορετικούς τομείς και ηπείρους. Θα διαπιστώσετε ότι δεν υπάρχουν σύνορα για το κυβερνοέγκλημα και ότι οι τρόποι να προφυλαχτούμε είναι οι ίδιοι και επαναλαμβάνονται σ' όλα τα άρθρα και απ' όλους τους ειδικούς είτε αφορούν την προσωπική σας ζωή είτε την επαγγελματική σας δραστηριότητα.

Ακολουθήστε τις οδηγίες των επαγγελματιών κυβερνοασφάλειας και μείνετε όσο το δυνατόν πιο ασφαλείς.

Προστασία από κυβερνοαπειλές για όλους με απλές πρακτικές κυβερνοϋγιεινής

Παναγιώτης Σούλος
Μέλος ΑΛΛΗΛΟΝ
Information Security GRC Senior Manager
Panagiotis Soulos | Linkedin

Περίληψη

Η χρήση του διαδικτύου και η αλληλεπίδρασή μας με συσκευές τεχνολογίας, όπως υπολογιστές, smartphones, tablets, Internet of Things (IoTs) κ.ά., είναι πλέον μία καθημερινότητα για όλους μας. Τα οφέλη είναι πολλαπλά για κάθε ηλικία και με τα ολοένα κι αυξανόμενα επιτεύγματα στην τεχνολογία γίνεται όλο και πιο εύκολη και άμεση. Ο καθένας μας χρησιμοποιεί το διαδίκτυο και τις συσκευές για ενημέρωση, ψυχαγωγία, διαδικτυακά παιχνίδια, εκπαίδευση, απομακρυσμένη εργασία και πολλά άλλα.

Παρόλα τα οφέλη, το διαδίκτυο ελλοχεύει κινδύνους που ενδέχεται να μας βλάψουν. Μπορούμε να προστατευθούμε ενσωματώνοντας στην καθημερινότητά μας απλές και βέλτιστες πρακτικές κυβερνοασφάλειας, γνωστές ως κυβερνοϋγιεινή.

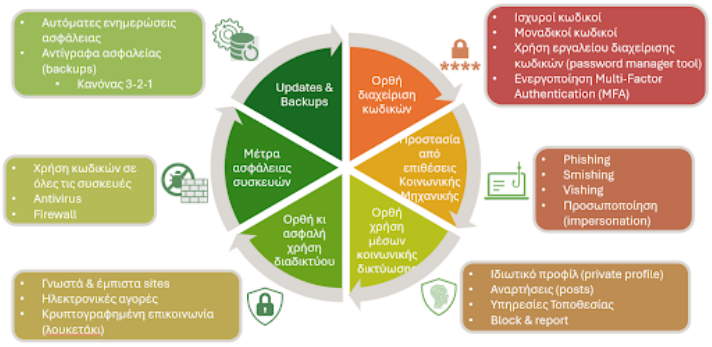
Η προστασία μας από κυβερνοαπειλές είναι πλέον απαραίτητη για όλους, καθώς η καθημερινή μας δραστηριότητα στο διαδίκτυο εκθέτει προσωπικά και επαγγελματικά δεδομένα σε πιθανούς κινδύνους. Μπορούμε να προστατευτούμε αποτελεσματικά εάν ενσωματώσουμε στην καθημερινότητά μας απλές πρακτικές κυβερνοϋγιεινής.

Ως *Κυβερνοϋγιεινή (Cyberhygiene)* αναφερόμαστε στις βέλτιστες πρακτικές ασφάλειας που οι ίδιοι λαμβάνουμε στην καθημερινότητά μας, ως συνήθεις πρακτικές, με σκοπό να προστατεύσουμε τα δεδομένα και τις συσκευές μας.

Τις πρακτικές κυβερνοϋγιεινής μπορούμε να τις εντάξουμε σε έξι χρήσιμα tips/κατηγορίες:

- Ορθή διαχείριση κωδικών (passwords)
- Προστασία από επιθέσεις Κοινωνικής Μηχανικής
- Ορθή χρήση μέσων κοινωνικής δικτύωσης
- Ορθή κι ασφαλή χρήση διαδικτύου
- Μέτρα ασφάλειας συσκευών
- Updates & Backups

Οι πρακτικές κυβερνοϋγιεινής αποτυπώνονται στο παρακάτω σχήμα.



Σχήμα 1, Βέλτιστες Πρακτικές Κυβερνοϋγιεινής

1. Ορθή διαχείριση κωδικών (passwords)

Οι κωδικοί αποτελούν ένα από τα κύρια στοιχεία που χρησιμοποιούμε στην καθημερινότητά μας ώστε να αποκτήσουμε πρόσβαση σε πληροφορίες, συστήματα και υπηρεσίες. Σε περίπτωση που οι κωδικοί μας διαρρεύσουν ή παραβιαστούν, μη εξουσιοδοτημένοι χρήστες θα αποκτήσουν πρόσβαση σε διάφορες υπηρεσίες που χρησιμοποιούμε στο διαδίκτυο. Οι υπηρεσίες αυτές είναι διαφόρων ειδών, από ένα απλό website ενημέρωσης έως το web banking μας.

Για να προστατεύσουμε επαρκώς τους κωδικούς μας προτείνονται οι παρακάτω βέλτιστες πρακτικές:

- Χρήση **ισχυρών κωδικών**. Ένας κωδικός θεωρείται ισχυρός:
  - Έχει μήκος τουλάχιστον 12 χαρακτήρες. Όσο μεγαλύτερος τόσο καλύτερα!
  - Αποτελείται από πεζά, κεφαλαία, αριθμούς και σύμβολα.
  - Δεν περιέχει ευρέως γνωστά στοιχεία για εμάς, όπως το όνομα και επίθετό μας, την ηλικία μας, τη διεύθυνση κατοικίας μας κ.ά.
  - Δεν περιέχει συνεχόμενους χαρακτήρες ή αριθμούς (π.χ. aaaa, 1234)
- Χρήση **μοναδικών κωδικών**. Είναι οι κωδικοί που δεν τους επαναχρησιμοποιούμε. Με τον τρόπο αυτό περιορίζουμε την επίπτωση που μπορεί να έχει η διαρροή ενός κωδικού μας σε έναν μόνο λογαριασμό/υπηρεσία.
- Χρήση **εργαλείου διαχείρισης κωδικών** (password manager tool)[1]. Τα συγκεκριμένα εργαλεία μας επιτρέπουν να:
  - Αποθηκεύουμε τους κωδικούς μας με ασφάλεια, αφού ενσωματώνουν κρυπτογράφηση επιπέδου στρατού.
  - Δημιουργούμε εύκολα και γρήγορα κωδικούς, αφού περιέχουν γεννήτρια κωδικών.
  - Αντιγράφουμε τους κωδικούς μας χωρίς να χρειάζεται να τους θυμόμαστε.
  - Θυμόμαστε μόνο έναν κωδικό, τον κύριο κωδικό (master password), για να αποκτούμε πρόσβαση στους κωδικούς μας.
  - Έχουμε τους κωδικούς μας πάντα μαζί μας και παντού, αφού μπορούν να εγκατασταθούν σε όλες μας τις συσκευές.
- Ενεργοποίηση **αυθεντικοποίηση πολλαπλών παραγόντων** (Multi-Factor Authentication - MFA). Η συγκεκριμένη ρύθμιση βρίσκεται συνήθως στις ρυθμίσεις ασφάλειας του εκάστοτε λογαριασμού μας και πλέον είναι διαθέσιμη σε όλες τις ευρέως γνωστές υπηρεσίες όπως e-mail, social media κ.ά.. Μας προσθέτει ένα επιπλέον παράγοντα αυθεντικοποίησης, όπως έναν κωδικό μίας χρήσης (One-Time Password), ένα push notification από την εφαρμογή στο κινητό μας, τα βιομετρικά μας στοιχεία (π.χ. δακτυλικό αποτύπωμα, αναγνώριση προσώπου κ.λπ.), τη στιγμή που συνδεόμαστε σε κάποια υπηρεσία. Με τον τρόπο αυτό, αποτρέπουμε τους κακόβουλους χρήστες να αποκτήσουν πρόσβαση στον λογαριασμό μας ακόμα κι αν ο κωδικός μας διαρρεύσει, αφού δεν θα έχουν στην κατοχή τους τον επιπλέον παράγοντα.

2. Προστασία από επιθέσεις Κοινωνικής Μηχανικής

Η Κοινωνική Μηχανική (Social Engineering) είναι η εκμετάλλευση ψυχολογικών ιδιοτήτων του ανθρώπινου παράγοντα, με τη χρήση κοινωνικής αλληλεπίδρασης, με σκοπό την εξαπάτησή του και την απόσπαση εμπιστευτικών πληροφοριών. Είναι η προσπάθεια εξαπάτησής μας παρουσιάζοντάς μας μία επείγουσα ανάγκη, όπου κάτι κακό πρόκειται να συμβεί και συνήθως σε πολύ σύντομο χρονικό διάστημα, εάν δεν δράσουμε άμεσα. Σύμφωνα με την πιο πρόσφατη έρευνα 2024 Verizon Data Breach Investigation Report[2], που εξετάζει ετησίως περιστατικά παραβίασης δεδομένων, το 68% των παραβιάσεων δεδομένων το 2023 οφειλόταν στον ανθρώπινο παράγοντα, συμπεριλαμβανομένου της κοινωνικής μηχανικής. Οι τρόποι με τους οποίους μπορεί να εμφανιστεί η κοινωνική μηχανική είναι οι εξής:

- **Phishing**. Απατηλά e-mails που προσπαθούν να μας εξαπατήσουν ώστε να πατήσουμε ένα σύνδεσμο, να κατεβάσουμε και να εκτελέσουμε κάποιο αρχείο, να δώσουμε τα στοιχεία σύνδεσης λογαριασμών μας κ.ά.. Θα πρέπει να είμαστε πάντα υποψιασμένοι και να επιβεβαιώνουμε τον αποστολέα και τους συνδέσμους (links) που περιέχονται, τοποθετώντας από πάνω το mouse μας - χωρίς να κάνουμε click. Εάν το αναγνωρίσουμε ως phishing, δεν απαντάμε, δεν πατάμε τους συνδέσμους, το αγνοούμε και το διαγράφουμε.
- **Smishing**. Είναι όταν μας αποστέλλουν απατηλά μηνύματα στο κινητό μας. Εάν μας αναφέρει ότι κλείνει ο λογαριασμός μας στην τράπεζά μας και πρέπει άμεσα να επιβεβαιώσουμε τα στοιχεία μας πατώντας τον σύνδεσμο στο μήνυμα, δεν πατάμε τον σύνδεσμο και καλούμε τηλεφωνικά την τράπεζά μας να το επιβεβαιώσουμε.
- **Vishing**. Είναι όταν μας καλούν στο τηλέφωνο και προσπαθούν να μας εξαπατήσουν. Δεν δίνουμε κανένα στοιχείο, όπως προσωπικά μας δεδομένα ή δεδομένα καρτών και κλείνουμε άμεσα το τηλέφωνο. Οι νέες συσκευές έχουν τη δυνατότητα αποκλεισμού τηλεφωνικών αριθμών.
- **Προσωποποίηση** (impersonation). Είναι όταν με φυσική παρουσία προσπαθούν να μας εξαπατήσουν, για να αποκτήσουν πρόσβαση σε χώρους, πληροφορίες και χρήματα. Να ρωτάμε πάντα και να μην επιτρέπουμε την πρόσβαση σε αγνώστους, ούτε

να τους δίνουμε πληροφορίες, ακόμα κι αν μας παρουσιάσουν ότι μας γνωρίζουν μέσω κάποιου γνωστού μας. Είναι πολύ πιθανό τα στοιχεία αυτά να τα άντλησαν από το διαδίκτυο!

3. Ορθή χρήση μέσων κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης αποτελούν πλέον το βασικό μας τρόπο επικοινωνίας με την οικογένειά μας, τους φίλους μας αλλά και ενημέρωσης και ψυχαγωγίας. Για το λόγο αυτό, θα πρέπει να προστατεύσουμε τους λογαριασμούς μας σε αυτά, ώστε να αποτρέψουμε πιθανή υποκλοπή τους που θα σήμαινε την υποκλοπή της ψηφιακής μας ταυτότητας. Σε τέτοια περίπτωση, κάποιος κακόβουλος χρήστης θα μπορούσε να κάνει αναρτήσεις σαν εμάς, να δει όλα μας τα προσωπικά μας μηνύματα και να προσπαθήσει να επικοινωνήσει με τους φίλους μας με σκοπό να τους εξαπατήσει. Ένα τέτοιο περιστατικό θα είναι καταστροφικό για την ιδιωτικότητά μας. Για να προστατευτούμε, θα πρέπει να:

- Θέσουμε το προφίλ μας ως **ιδιωτικό** (private), ώστε να ελέγχουμε τα αιτήματα φιλίας και να επιλέγουμε τους φίλους μας.
- Είμαστε προσεκτικοί στις **αναρτήσεις** (posts) που κάνουμε. Οποιαδήποτε πληροφορία αναρτούμε στο διαδίκτυο παραμένει εκεί για **πάντα**. Αποφεύγουμε να αναρτούμε πότε θα πάμε διακοπές ή φωτογραφίες όταν είμαστε σε διακοπές, καθώς είναι σαν να ανακοινώνουμε ότι λείπουμε από το σπίτι μας. Επιπλέον, οι αναρτήσεις που κάνουμε μπορεί να μας επηρεάσουν στο μέλλον είτε σε προσωπικό είτε σε επαγγελματικό επίπεδο.
- Αποφεύγουμε τη χρήση **των υπηρεσιών τοποθεσίας** (location services), ιδιαίτερα όταν αφορούν σε προσωπικούς μας χώρους (π.χ. κατοικία, εξοχικό, εργασία). Μπορεί ένας κακόβουλος χρήστης να έρθει να μας συναντήσει ή να προσπαθήσει να παραβιάσει το σπίτι μας όταν εμείς θα λείπουμε.
- Ενημερωθούμε για τον τρόπο με τον οποίο μπορούμε να κάνουμε αποκλεισμό (**block**) και αναφορά (**report**). Όλα τα μέσα κοινωνικής δικτύωσης έχουν αυτή τη δυνατότητα.

4. Ορθή κι ασφαλή χρήση διαδικτύου

Για να προστατευτούμε στο διαδίκτυο, θα πρέπει να:

- Επισκεπτόμαστε μόνο **γνωστά** κι **έμπιστα websites**. Είναι αυτά που είναι ευρέως γνωστά.
- Προσέχουμε ιδιαίτερα όσον αφορά στις **ηλεκτρονικές πληρωμές**. Δεν κάνουμε αγορές από άγνωστα websites και δεν δίνουμε τα στοιχεία της κάρτας μας σε κανέναν!
- Επιβιώνουμε ότι η **επικοινωνία** είναι **κρυπτογραφημένη** όταν παρέχουμε ευαίσθητα δεδομένα, όπως τα προσωπικά μας δεδομένα, τους κωδικούς μας και τα στοιχεία της κάρτας μας. Κοιτάμε στη μπάρα διεύθυνσης ότι εμφανίζεται το «λουκετάκι» κι ότι δεν εμφανίζεται κάποιο μήνυμα για μη ασφαλή σύνδεση.

5. Μέτρα ασφάλειας συσκευών

Οι συσκευές μας ενδέχεται να χαθούν ή κλαπούν κι ακόμα να μολυνθούν από κακόβουλο λογισμικό. Γι' αυτό θα πρέπει να λάβουμε βασικά μέτρα ασφάλειας, όπως:

- **Χρήση κωδικών** σε όλες τις συσκευές, ώστε να αποτραπεί η πρόσβαση στα δεδομένα των συσκευών μας σε όσους έχουν φυσική πρόσβαση σε αυτές.
- **Antivirus**[3], το οποίο θα προστατεύσει τη συσκευή μας από πιθανή μόλυνση κακόβουλου λογισμικού. Θα πρέπει να το συντηρούμε πάντα ενημερωμένο και με τις τελευταίες ενημερώσεις κακόβουλων λογισμικών.
- **Firewall**, το οποίο θα μας προστατεύσει από πιθανές κυβερνοεπιθέσεις.

6. Updates & Backups

Τα λογισμικά που έχουμε εγκατεστημένα στις συσκευές μας ενδέχεται να έχουν ευπάθειες ασφαλείας και οι συσκευές μας ενδέχεται να χαλάσουν για οποιοδήποτε λόγο. Γι' αυτό θα πρέπει να:

- Ενεργοποιήσουμε τις **αυτόματες ενημερώσεις ασφάλειας** σε οποιοδήποτε λογισμικό έχουμε στις συσκευές μας.
- Λαμβάνουμε περιοδικά **αντίγραφα ασφάλειας** (backup), ώστε να διατηρήσουμε τα δεδομένα μας σε περίπτωση κλοπής ή απώλειας της συσκευής μας. Οι βέλτιστες πρακτικές προτείνουν τον κανόνα 3-2-1, δηλαδή:
  - 3 αντίγραφα ασφάλειας
  - 2 σε διαφορετικά μέσα, π.χ. εξωτερικό σκληρό δίσκο και usb
  - 1 σε διαφορετική τοποθεσία, π.χ. cloud

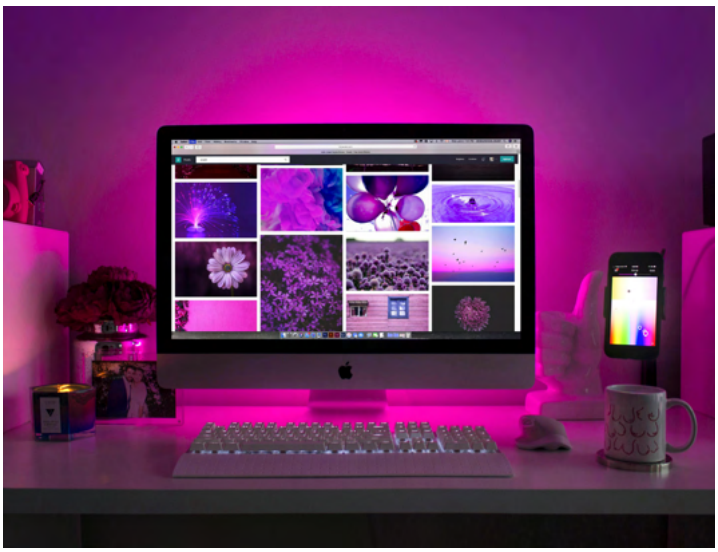
Συνοψίζοντας, οι παραπάνω βέλτιστες πρακτικές κυβερνοϋγιεινής με όλο και πιο συχνή χρήση μπορούν να μας γίνουν καθημερινές συνήθειες για την προστασία των δεδομένων μας στην σύγχρονη εποχή.

Παραπομπές

1 Ενδεικτικά παραδείγματα password manager tools: BitWarden, 1Password

2 Verizon Data Breach Investigation Report

3 Σύγκριση ευρέων γνωστών λύσεων antivirus: https://www.av-test.org/en/



Κυβερνοεπιθέσεις σε επιχειρήσεις

Πρόληψη, αντιμετώπιση και διερεύνηση

Δημήτρης Γεωργίου MSc CPFA CPSP CISSP
Alphabit Cybersecurity, Chief Security Officer, ISC2, Europe Advisory Council, Member, ISC2 Hellenic Chapter, Treasurer
Dimitris Georgiou | Linkedin

Τα τελευταία χρόνια, οι κυβερνοεπιθέσεις έχουν εξελιχθεί σε μια από τις μεγαλύτερες απειλές για τις επιχειρήσεις, ανεξαρτήτως μεγέθους και τομέα. Σύμφωνα με εκτιμήσεις, η αξία του παγκόσμιου κυβερνοεγκλήματος αναμένεται να φτάσει τα 10,5 τρισεκατομμύρια δολάρια μέχρι το 2025. Αυτό αντιπροσωπεύει μια δραματική άνοδο σε σχέση με τα προηγούμενα χρόνια και δείχνει την κλίμακα του προβλήματος.

Μέσα σε αυτό το περιβάλλον, οι διοικήσεις των επιχειρήσεων οφείλουν να αναγνωρίσουν ότι η κυβερνοασφάλεια δεν είναι μόνο τεχνολογικό ζήτημα, αλλά θέμα **στρατηγικής και διαχείρισης κινδύνων**. Η συνεχής **επένδυση σε εργαλεία και τεχνολογίες ασφαλείας**, αλλά και η **δημιουργία κουλτούρας ασφαλείας**, είναι ζωτικής σημασίας για τη θωράκιση των επιχειρήσεων.

Τα πιο διαδεδομένα είδη κυβερνοεπιθέσεων, είναι τα ακόλουθα:

1. Phishing

Το phishing (ηλεκτρονικό ψάρεμα) είναι από τις πιο συνηθισμένες μορφές κυβερνοεπίθεσης, όπου οι επιτιθέμενοι στέλνουν παραπλανητικά μηνύματα μέσω email, SMS ή άλλων μορφών επικοινωνίας, προσπαθώντας να εξαπατήσουν τους εργαζομένους, ώστε να αποκαλύψουν πληροφορίες. Ο αντίκτυπος των επιτυχημένων επιθέσεων phishing μπορεί να είναι καταστροφικός, καθώς οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε συστήματα ή λογαριασμούς, προκαλώντας οικονομικές ζημιές και διαρροή εμπιστευτικών δεδομένων. Παραλλαγή του είναι το **spear phishing**, μια στοχευμένη μορφή phishing, όπου οι επιτιθέμενοι στοχεύουν υψηλόβαθμα στελέχη ή άτομα που έχουν πρόσβαση σε κρίσιμα συστήματα καθιστώντας τον αντίκτυπο μιας επιτυχημένης επίθεσης εξαιρετικά σοβαρό.

2. Malware και Ransomware

Το Malware (κακόβουλο λογισμικό) είναι ένα ευρύ φάσμα προγραμμάτων που στοχεύουν στην υπονόμευση της ασφάλειας μιας επιχείρησης, όπως ιοί, trojans, spyware και worms. Το Ransomware (λυτρισμικό) είναι ένας τύπος malware που κρυπτογραφεί τα δεδομένα και απαιτεί λύτρα για την επαναφορά τους. Μια επιτυχημένη επίθεση ransomware μπορεί να παραλύσει την παραγωγική ικανότητα, προκαλώντας σοβαρές οικονομικές ζημιές, διακοπές λειτουργίας και ανεπανόρθωτη καταστροφή δεδομένων. Το ransomware αποτελεί μια από τις πιο επικερδείς μορφές κυβερνοεγκλήματος, με τεράστιο αντίκτυπο στις επιχειρήσεις, οι οποίες συχνά πληρώνουν τα ζητούμενα λύτρα για να μην υποστούν τις καταστροφικές συνέπειες μιας οριστικής διακοπής στη λειτουργία τους.

3. Distributed Denial of Service (DDoS)

Οι επιθέσεις DDoS (Κατανεμημένης Άρνηση Υπηρεσίας) στοχεύουν στην υπερφόρτωση ενός δικτύου ή ενός διακομιστή με τεράστιες ποσότητες κακόβουλων αιτήσεων, με αποτέλεσμα την αδυναμία εξυπηρέτησης των αιτήσεων των θεμιτών χρηστών. Οι επιτιθέμενοι χρησιμοποιούν συχνά botnets (δίκτυα από μολυσμένους υπολογιστές) για να αυξήσουν τον όγκο των αιτήσεων προς έναν διακομιστή, οδηγώντας σε κατάρρευση της υπηρεσίας. Οι επιπτώσεις για τις επιχειρήσεις μπορεί να είναι η αδυναμία εξυπηρέτησης πελατών, απώλεια εισοδημάτων και σημαντική ζημιά στη φήμη της επιχείρησης, ειδικά εάν η λειτουργία της βασίζεται στην απρόσκοπτη παρουσία στο διαδίκτυο.

4. Man-in-the-Middle Attacks

Στις επιθέσεις Man-in-the-Middle (MITM), ο επιτιθέμενος παρεμβαίνει στις επικοινωνίες μεταξύ δύο μερών (για παράδειγμα, ενός χρήστη και ενός διακομιστή) και μπορεί να υποκλέψει ή να αλλοιώσει τα δεδομένα που ανταλλάσσονται, χωρίς να γίνει αντιληπτός. Οι επιθέσεις MITM μπορούν να εκμεταλλευτούν αδύναμα σημεία σε ασύρματα δίκτυα ή ανεπαρκώς ασφαλισμένες συνδέσεις, ή την έλλειψη εκπαίδευσης των χρηστών σε συνδυασμό με ανεπαρκείς διαδικασίες ασφάλειας, θέτοντας σε κίνδυνο ευαίσθητες πληροφορίες, όπως οικονομικά δεδομένα ή διαπιστευτήρια σύνδεσης. Ο αντίκτυπος αυτών των επιθέσεων μπορεί να περιλαμβάνει την κλοπή δεδομένων, την εγκατάσταση κακόβουλου λογισμικού στα συστήματα της επιχείρησης ή στην περίπτωση μιας υποκατηγορίας που ονομάζεται BEC (παραβίαση επιχειρηματικής αλληλογραφίας) την μεταφορά χρημάτων σε κυβερνοεγκληματίες που υποδύονται προμηθευτές της επιχείρησης.

5. Vulnerability Exploit

Οι επιτιθέμενοι συχνά εκμεταλλεύονται γνωστά κενά ασφαλείας σε εφαρμογές ιστού για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή ευαίσθητα δεδομένα. Αυτά τα κενά ασφάλειας επιτρέπουν την εισαγωγή κακόβουλου κώδικα, την παραβίαση εσωτερικών υπηρεσιών ή την εκτέλεση εντολών στο όνομα του χρήστη χωρίς τη γνώση του. Οι συνέπειες αυτών των επιθέσεων μπορεί να περιλαμβάνουν κλοπή δεδομένων, αλλοίωση πληροφοριών και μη εξουσιοδοτημένη πρόσβαση σε κρίσιμες υπηρεσίες.

6. Zero-Day Exploits

Τα Zero-Day Exploits (Εκμετάλλευση Άγνωστων Κενών Ασφαλείας) είναι επιθέσεις που εκμεταλλεύονται άγνωστες (ή μη δημοσιοποιημένες) ευπάθειες σε λογισμικό ή συστήματα. Δεδομένου ότι οι ευπάθειες αυτές δεν έχουν ακόμη διορθωθεί από τους κατασκευαστές ή τους προγραμματιστές, οι επιτιθέμενοι μπορούν να τις εκμεταλλευτούν για να αποκτήσουν παράνομη πρόσβαση σε συστήματα και να προκαλέσουν ζημιές πριν γίνει διαθέσιμη κάποια επίσημη ενημέρωση ασφαλείας.

7. Social Engineering

Το Social Engineering (Κοινωνική Μηχανική) βασίζεται στον ανθρώπινο παράγοντα και όχι σε τεχνικά μέσα. Οι επιτιθέμενοι χρησιμοποιούν παραπλάνηση για να χειραγωγήσουν εργαζομένους να αποκαλύψουν ευαίσθητες πληροφορίες ή να παραχωρήσουν πρόσβαση σε συστήματα εκμεταλλευόμενοι την εμπιστοσύνη ή την άγνοια κινδύνου του θύματος. Παρόλο που δεν απαιτείται εξειδικευμένη τεχνική για την εκτέλεση αυτών των επιθέσεων, ο αντίκτυπός τους μπορεί να είναι τεράστιος, καθώς μπορούν να παρακάμψουν ακόμα και τα πιο εξελιγμένα μέτρα ασφαλείας.

8. Advanced Persistent Threats (APTs)

Πρόκειται για στοχευμένες επιθέσεις που εστιάζουν σε μια επιχείρηση για παρατεταμένο χρονικό διάστημα. Οι επιτιθέμενοι αυτού του τύπου χρησιμοποιούν εξελιγμένες μεθόδους για να αποκτήσουν πρόσβαση σε δίκτυα και συστήματα, και σύμφωνα με μελέτες περνούν απαρατήρητοι κατά μέσο όρο για 270 ημέρες. Στόχος τους είναι η βιομηχανική κατασκοπεία ή ακόμα και η καταστροφή δεδομένων. Συχνά είναι κρατικά υποστηριζόμενοι χάκερς ή μεγάλες εγκληματικές οργανώσεις. Ο αντίκτυπός τους μπορεί να είναι εξαιρετικά σοβαρός, προκαλώντας κλοπή εταιρικών μυστικών, εκτεταμένες οικονομικές ζημίες και ζημιά στη φήμη της επιχείρησης

9. Credential Stuffing

Στο Credential Stuffing, οι επιτιθέμενοι χρησιμοποιούν κλεμμένα διαπιστευτήρια που πωλούνται το σκοτεινό διαδίκτυο, για να αποκτήσουν πρόσβαση σε άλλους λογαριασμούς που πιθανόν να χρησιμοποιούν τα ίδια διαπιστευτήρια (όπως ονόματα χρήστη και κωδικούς πρόσβασης). Εάν ένα στέλεχος επαναχρησιμοποιεί τον ίδιο κωδικό πρόσβασης σε πολλούς λογαριασμούς, οι επιτιθέμενοι μπορούν να αποκτήσουν πρόσβαση σε διάφορους λογαριασμούς του με αυτόν τον τρόπο. Αυτές οι επιθέσεις μπορούν να προκαλέσουν απώλειες σε προσωπικά δεδομένα, οικονομικές πληροφορίες και πρόσβαση σε κρίσιμα εταιρικά συστήματα.

10. Insider Threat

Ο εσωτερικός κίνδυνος αναφέρεται στις απειλές που προέρχονται από τους ίδιους τους εργαζομένους, συνεργάτες ή άτομα με εξουσιοδοτημένη πρόσβαση στα συστήματα και τα δεδομένα μιας επιχείρησης. Αυτοί οι εσωτερικοί παράγοντες μπορεί να εκμεταλλευτούν την πρόσβασή τους σκόπιμα ή κατά λάθος, προκαλώντας σοβαρά προβλήματα ασφαλείας. Ο εσωτερικός κίνδυνος μπορεί να είναι ιδιαίτερα σοβαρός, καθώς οι εσωτερικοί παράγοντες διαθέτουν νόμιμη πρόσβαση σε κρίσιμες πληροφορίες και συστήματα, καθιστώντας δύσκολο τον έγκαιρο εντοπισμό και την αποτροπή τους. Ο αντίκτυπος μιας επιτυχημένης επίθεσης από κάποιον εσωτερικό παράγοντα μπορεί να περιλαμβάνει κλοπή ευαίσθητων δεδομένων ή πνευματικής ιδιοκτησίας και ιαρροή εμπιστευτικών πληροφοριών πελατών ή επιχειρηματικών στρατηγικών, καταστροφή ή αλλοίωση κρίσιμων αρχείων και πληροφοριών, χρηματικές απώλειες, κυρώσεις λόγω μη συμμόρφωσης με κανονισμούς προστασίας δεδομένων και

ζημιά στη φήμη της εταιρείας.

Πρόληψη: Στρατηγική και Επένδυση

Οι επιχειρήσεις, για να είναι ανθεκτικές στα περιστατικά κυβερνοασφάλειας, πρέπει να υιοθετήσουν ένα σύνολο καλών πρακτικών για την κυβερνοασφάλεια. Ακολουθούν οι πιο κρίσιμες:

- **Ανάπτυξη Στρατηγικής Ασφαλείας**: Είναι ζωτικής σημασίας οι διοικήσεις να ενημερωθούν για τους κινδύνους και να επενδύσουν στην ανάπτυξη μιας στρατηγικής ασφαλείας που περιλαμβάνει την πρόσληψη ειδικών για την εκτίμηση κινδύνων, την ανίχνευση απειλών και κενών ασφαλείας, την υιοθέτηση πολιτικών και διαδικασιών, το σχεδιασμό αντιμετώπισης κυβερνοεπιθέσεων και την οργανωμένη απόκριση σε περιστατικά παραβίασης. Η στρατηγική πρέπει να είναι δυναμική, αναθεωρούμενη τακτικά για να προσαρμόζεται στις νέες απειλές.
- **Τακτικές Αξιολογήσεις Κινδύνου**: Οι διοικήσεις πρέπει να μεριμνούν για τακτικές και ολοκληρωμένες τεχνικές αξιολογήσεις κινδύνου, τόσο σε συστήματα όσο και σε διαδικασίες, για να εντοπίζονται ευπάθειες και να εφαρμόζονται διορθωτικά μέτρα. Οι αξιολογήσεις αυτές πρέπει να περιλαμβάνουν εξωτερικές επιθεωρήσεις και δοκιμές διείσδυσης (penetration testing).
- **Υιοθέτηση Πολιτικών Πρόσβασης**: Οι αρχές της διάκρισης καθηκόντων (separation of duties) και της ελάχιστης πρόσβασης (least privilege) πρέπει να εφαρμόζονται αυστηρά, ώστε οι εργαζόμενοι να έχουν πρόσβαση μόνο στα δεδομένα και τα συστήματα που χρειάζονται για την εργασία τους. Οι πολιτικές αυτές ενισχύονται με χρήση ισχυρών διαπιστευτηρίων, ελέγχων ταυτότητας πολλαπλών παραγόντων (MFA) και συστημάτων παρακολούθησης πρόσβασης.
- **Προστασία δεδομένων και σχεδιασμός επιχειρησιακής συνέχειας**: Ένα ολοκληρωμένο Σχέδιο Ανάκαμψης από Καταστροφή (DRP) και Σχέδιο Επιχειρησιακής Συνέχειας (BCP) είναι απαραίτητα για την προστασία των δεδομένων και τη διασφάλιση της επιχειρησιακής λειτουργίας σε περιπτώσεις κρίσεων, όπως κυβερνοεπιθέσεις ή φυσικές καταστροφές. Αυτά τα σχέδια πρέπει να περιλαμβάνουν δημιουργία πολλαπλών αντιγράφων ασφαλείας, κρυπτογράφηση δεδομένων κατά τη μεταφορά και αποθήκευση, καθώς και δυνατότητα αποκατάστασης σε απομακρυσμένα εφεδρικά συστήματα, με στόχο την ελαχιστοποίηση διακοπών και απωλειών.
- **Εκπαίδευση Προσωπικού**: Το ανθρώπινο λάθος είναι ένας από τους πιο σημαντικούς παράγοντες κινδύνου. Η τακτική εκπαίδευση του προσωπικού στην αναγνώριση των κινδύνων, όπως οι επιθέσεις phishing, οι επιθέσεις κοινωνικής μηχανικής και οι κακόβουλες εφαρμογές, είναι ζωτικής σημασίας. Το προσωπικό πρέπει να εκπαιδεύεται σε θέματα ασφαλούς χρήσης συστημάτων και να ενθαρρύνεται να αναφέρει ύποπτες δραστηριότητες άμεσα.
- **Διαχείριση Ασφαλείας Εξωτερικών Συνεργατών (Third-Party Risk Management)**: Οι επιχειρήσεις πρέπει να διασφαλίσουν ότι οι τρίτοι προμηθευτές ή συνεργάτες συμμορφώνονται με τα πρότυπα ασφαλείας της επιχείρησης. Αυτό περιλαμβάνει την τακτική αξιολόγηση των πολιτικών ασφαλείας τους και την ενσωμάτωση συμβατικών όρων που απαιτούν αυστηρά μέτρα ασφάλειας δεδομένων.

Αντιμετώπιση Περιστατικών (Incident Response)

Τα περιστατικά κυβερνοασφάλειας είναι σχεδόν αναπόφευκτα. Η αντιμετώπιση των περιστατικών πρέπει να είναι άμεση και οργανωμένη. Οι επιχειρήσεις πρέπει να ακολουθήσουν τις εξής καλές πρακτικές για αποτελεσματική απόκριση:

1. **Σχέδιο Αντιμετώπισης Περιστατικών (Incident Response Plan)**: Κάθε επιχείρηση πρέπει να έχει ένα έτοιμο και καταγεγραμμένο σχέδιο για την αντιμετώπιση περιστατικών, το οποίο να περιλαμβάνει σαφείς διαδικασίες για τον εντοπισμό, την αναφορά και την αποκατάσταση από μια επίθεση.
2. **Συνεργασία με Ομάδες Αντιμετώπισης**: Σε πολλές περιπτώσεις, η συνεργασία με εξειδικευμένες ομάδες κυβερνοασφάλειας μπορεί να βοηθήσει στην ταχύτερη και πιο αποτελεσματική διαχείριση των επιθέσεων.
3. **Ενημέρωση των Εμπλεκομένων**: Οι ενδιαφερόμενοι, όπως οι πελάτες και οι ρυθμιστικές αρχές, πρέπει να ενημερώνονται άμεσα σε περίπτωση παραβίασης δεδομένων για να περιοριστούν οι συνέπειες και να εξασφαλιστεί η διαφάνεια.
4. **Εκ των Υστέρων Αξιολόγηση**: Μετά την επίθεση, είναι σημαντικό να γίνει αναλυτική αξιολόγηση του περιστατικού, ώστε να εντοπιστούν τα κενά ασφαλείας και να ληφθούν μέτρα για την αποφυγή μελλοντικών περιστατικών.

Διερεύνηση: Ψηφιακή Εγκληματολογία και Εξέταση Ψηφιακών Πειστηρίων (Digital Forensics)

Η ψηφιακή εγκληματολογία είναι ο τομέας που ασχολείται με τη συλλογή, την ανάλυση και την ερμηνεία ψηφιακών πειστηρίων για τη διερεύνηση που έπεται των κυβερνοεπιθέσεων. Η διαδικασία αυτή περιλαμβάνει τη συλλογή δεδομένων από συσκευές, διακομιστές και δίκτυα, την ανάλυσή τους από ειδικούς σε κατάλληλα εργαστήρια για να εντοπιστούν οι επιτιθέμενοι, και τη δημιουργία αναφορών που μπορεί να χρησιμοποιηθούν σε διαπραγματεύσεις ή νομικές διαδικασίες.

Η ψηφιακή εγκληματολογία παίζει κρίσιμο ρόλο στην προστασία των επιχειρήσεων, καθώς επιτρέπει την αναγνώριση των δραστών, την αποκατάσταση των δεδομένων και την ενίσχυση της συνολικής ασφάλειας. Επιπλέον, σε περίπτωση νομικών διαφορών, η σωστή εξέταση των ψηφιακών πειστηρίων μπορεί να βοηθήσει στην απόδειξη της ευθύνης των επιτιθέμενων και στην αποτροπή μελλοντικών επιθέσεων.

Η αντιμετώπιση των κυβερνοεπιθέσεων απαιτεί ευαισθητοποίηση, ολοκληρωμένη στρατηγική και τεχνολογικά εργαλεία. Οι επιχειρήσεις πρέπει να επενδύσουν σε προηγμένα μέτρα ασφαλείας και εκπαίδευση προσωπικού για να θωρακιστούν ενάντια σε μια διαρκώς εξελισσόμενη και αυξανόμενη απειλή.

Η ψηφιακή εγκληματολογία και αντιμετώπιση περιστατικών στην καθημερινότητα

Κωνσταντίνος Νασόπουλος
Μέλος σε Κέντρο Αντιμετώπισης Περιστατικών ως Αναλυτής κυβερνοεπιθέσεων και Αναλυτής Ψηφιακών πειστηρίων

Περίληψη

Το DFIR (Ψηφιακή Εγκληματολογία και Αντιμετώπιση Περιστατικών) έχει γίνει αναπόσπαστο κομμάτι της καθημερινής ζωής, προστατεύοντας τα προσωπικά δεδομένα και την ασφάλεια στο διαδίκτυο. Χρησιμοποιείται στην εξιχνίαση εγκλημάτων, την προστασία εταιρικών δεδομένων και την ασφάλεια έξυπνων συσκευών. Το DFIR αντιμετωπίζει προκλήσεις όπως εξελισσόμενες απειλές και ενσωματώνει την αναπτυσσόμενη τεχνητή νοημοσύνη. Η εκπαίδευση και ευαισθητοποίηση του κοινού είναι κρίσιμες, καθώς προκύπτουν ηθικά ζητήματα σχετικά με την ισορροπία μεταξύ ασφάλειας και ιδιωτικότητας. Η συνεργασία μεταξύ ατόμων, επιχειρήσεων και κυβερνήσεων είναι απαραίτητη για ένα ασφαλές ψηφιακό περιβάλλον.

Εισαγωγή

Στη σύγχρονη ψηφιακή εποχή, η Ψηφιακή Εγκληματολογία και Αντιμετώπιση Περιστατικών (Digital Forensics and Incident Response - DFIR) έχει γίνει αναπόσπαστο κομμάτι της καθημερινότητάς μας, ακόμη κι αν δεν το συνειδητοποιούμε πάντα. Από την προστασία των προσωπικών μας δεδομένων μέχρι την εξιχνίαση εγκλημάτων, το DFIR διαδραματίζει καθοριστικό ρόλο στη διατήρηση της ασφάλειας και της δικαιοσύνης στον ψηφιακό κόσμο. Αυτό το άρθρο θα εξερευνήσει τις πολλαπλές πτυχές του DFIR και πώς επηρεάζει την καθημερινή μας ζωή.

Η Σημασία του DFIR στην Καθημερινή Ζωή

Προστασία Προσωπικών Δεδομένων

Στην εποχή των μέσων κοινωνικής δικτύωσης και των έξυπνων συσκευών, η προστασία των προσωπικών μας δεδομένων είναι πιο σημαντική από ποτέ. Το DFIR βοηθά στην ανίχνευση και αντιμετώπιση παραβιάσεων δεδομένων, διασφαλίζοντας ότι οι ευαίσθητες πληροφορίες μας παραμένουν ασφαλείς.
Για παράδειγμα, όταν χρησιμοποιούμε εφαρμογές κοινωνικής δικτύωσης, το DFIR μπορεί να βοηθήσει στην ανίχνευση ύποπτης

δραστηριότητας στους λογαριασμούς μας. Αν κάποιος προσπαθήσει να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον λογαριασμό μας, οι τεχνικές DFIR μπορούν να εντοπίσουν αυτή την προσπάθεια και να ειδοποιήσουν τόσο εμάς όσο και την πλατφόρμα, επιτρέποντας την άμεση λήψη μέτρων προστασίας.

Ασφάλεια στο Διαδίκτυο

Καθώς περνάμε όλο και περισσότερο χρόνο στο διαδίκτυο, το DFIR παίζει κρίσιμο ρόλο στην προστασία μας από κυβερνοεπιθέσεις, phishing και άλλες απειλές. Οι τεχνικές DFIR χρησιμοποιούνται για την ανάλυση ύποπτων e-mail, ιστοσελίδων και εφαρμογών, βοηθώντας στην πρόληψη απάτης και κλοπής ταυτότητας.
Ένα καθημερινό παράδειγμα είναι η προστασία από επιθέσεις phishing. Το DFIR βοηθά στην ανάλυση των χαρακτηριστικών των ύποπτων e-mail, όπως η διεύθυνση αποστολέα, οι σύνδεσμοι και τα συνημμένα αρχεία. Αυτό επιτρέπει στα φίλτρα spam και τα συστήματα ασφαλείας να εντοπίζουν και να μπλοκάρουν τέτοια μηνύματα πριν φτάσουν στα εισερχόμενά μας.

Εξιχνίαση Εγκλημάτων

Το DFIR έχει φέρει επανάσταση στον τρόπο με τον οποίο οι αρχές επιβολής του νόμου διερευνούν εγκλήματα. Από την ανάκτηση διαγραμμένων μηνυμάτων μέχρι την ανάλυση ψηφιακών αποτυπωμάτων, οι τεχνικές DFIR παρέχουν κρίσιμα στοιχεία για την επίλυση υποθέσεων.
Για παράδειγμα, σε περιπτώσεις οικονομικών εγκλημάτων, το DFIR μπορεί να χρησιμοποιηθεί για την ανάλυση ηλεκτρονικών συναλλαγών και την ανίχνευση ύποπτων μοτίβων. Αυτό μπορεί να βοηθήσει στον εντοπισμό περιπτώσεων απάτης ή ξεπλύματος χρήματος, συμβάλλοντας στην προστασία των καταναλωτών και στη διατήρηση της ακεραιότητας του χρηματοπιστωτικού συστήματος.

DFIR στην Επιχειρηματική Σφαίρα

Προστασία Εταιρικών Δεδομένων

Οι επιχειρήσεις βασίζονται στο DFIR για την προστασία των ευαίσθητων εταιρικών δεδομένων και της πνευματικής ιδιοκτησίας. Σε περίπτωση παραβίασης, οι ειδικοί DFIR μπορούν να αναλύσουν γρήγορα την έκταση της ζημιάς και να αναπτύξουν στρατηγικές αποκατάστασης.
Ένα πρακτικό παράδειγμα είναι η αντιμετώπιση επιθέσεων ransomware. Όταν μια επιχείρηση πέσει θύμα τέτοιας επίθεσης, οι ειδικοί DFIR μπορούν να αναλύσουν το κακόβουλο λογισμικό, να εντοπίσουν τον τρόπο εισόδου του στο σύστημα και να βοηθήσουν στην ανάκτηση των κρυπτογραφημένων δεδομένων χωρίς την πληρωμή λύτρων.

Συμμόρφωση με Κανονισμούς

Το DFIR βοηθά τις επιχειρήσεις να συμμορφώνονται με τους κανονισμούς προστασίας δεδομένων, όπως ο GDPR. Οι τεχνικές DFIR χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο της πρόσβασης σε δεδομένα, διασφαλίζοντας ότι οι εταιρείες παραμένουν εντός των νομικών πλαισίων.
Για παράδειγμα, σε περίπτωση παραβίασης δεδομένων, το DFIR μπορεί να βοηθήσει στον ακριβή προσδιορισμό των δεδομένων που επηρεάστηκαν και των ατόμων που επηρεάστηκαν. Αυτό επιτρέπει στις επιχειρήσεις να ενημερώσουν έγκαιρα τους πελάτες τους και τις αρμόδιες αρχές, όπως απαιτείται από τον GDPR.

DFIR στην Καθημερινότητα μας

Ασφάλεια Έξυπνων Συσκευών

Με την αυξανόμενη χρήση έξυπνων οικιακών συσκευών, το DFIR γίνεται όλο και πιο σημαντικό για την προστασία της ιδιωτικής μας ζωής. Οι τεχνικές DFIR χρησιμοποιούνται για την ανίχνευση και αντιμετώπιση παραβιάσεων σε συσκευές όπως έξυπνες τηλεοράσεις, θερμοστάτες και συστήματα ασφαλείας.
Για παράδειγμα, αν ένας χάκερ προσπαθήσει να αποκτήσει πρόσβαση στο έξυπνο σύστημα ασφαλείας του σπιτιού μας, οι τεχνικές DFIR μπορούν να εντοπίσουν αυτή την ύποπτη δραστηριότητα και να ενεργοποιήσουν μηχανισμούς προστασίας, όπως το άμεσο μπλοκάρισμα της πρόσβασης και η ειδοποίηση του ιδιοκτήτη.

Ανάκτηση Δεδομένων

Το DFIR δεν αφορά μόνο την ασφάλεια. Οι τεχνικές του χρησιμοποιούνται επίσης για την ανάκτηση χαμένων ή διαγραμμένων δεδομένων από υπολογιστές, smartphones και άλλες συσκευές, σώζοντας πολύτιμες αναμνήσεις και σημαντικές πληροφορίες.
Ένα καθημερινό παράδειγμα είναι η ανάκτηση διαγραμμένων φωτογραφιών από ένα smartphone. Οι τεχνικές DFIR μπορούν να χρησιμοποιηθούν για την ανάλυση της μνήμης της συσκευής και την ανάκτηση αρχείων που φαινομενικά έχουν χαθεί, επιτρέποντας στους χρήστες να ανακτήσουν πολύτιμες αναμνήσεις.

Προκλήσεις και Μελλοντικές Τάσεις

Εξελισσόμενες Απειλές

Καθώς οι κυβερνοεπιθέσεις γίνονται όλο και πιο εξελιγμένες, το DFIR πρέπει να προσαρμόζεται συνεχώς. Οι ειδικοί DFIR εργάζονται ακατάπαυστα για την ανάπτυξη νέων τεχνικών και εργαλείων για την αντιμετώπιση αναδυόμενων απειλών.
Για παράδειγμα, η άνοδος των επιθέσεων “deepfake” απαιτεί νέες τεχνικές DFIR για την ανίχνευση και την αντιμετώπιση αυτής της μορφής παραπληροφόρησης. Οι ειδικοί αναπτύσσουν εργαλεία που μπορούν να αναλύσουν τα μεταδεδομένα (metadata) και τα χαρακτηριστικά των βίντεο για να εντοπίσουν πιθανές παραποιήσεις.

Τεχνητή Νοημοσύνη και Μηχανική Μάθηση

Η ενσωμάτωση της τεχνητής νοημοσύνης και της μηχανικής μάθησης στο DFIR υπόσχεται να επιταχύνει τις διαδικασίες ανάλυσης και να βελτιώσει την ακρίβεια των ερευνών. Αυτές οι τεχνολογίες μπορούν

να βοηθήσουν στην ταχύτερη ανίχνευση ανωμαλιών και στην αυτοματοποίηση ορισμένων πτυχών της διαδικασίας DFIR.
Για παράδειγμα, αλγόριθμοι μηχανικής μάθησης μπορούν να εκπαιδευτούν για να αναγνωρίζουν μοτίβα κακόβουλης δραστηριότητας σε δίκτυα υπολογιστών. Αυτό επιτρέπει την ταχύτερη ανίχνευση και αντιμετώπιση επιθέσεων, μειώνοντας τον χρόνο που οι επιτιθέμενοι έχουν πρόσβαση σε ευαίσθητα συστήματα.

Η Σημασία της Εκπαίδευσης και της Ευαισθητοποίησης

Καθώς το DFIR γίνεται όλο και πιο σημαντικό στην καθημερινή μας ζωή, η εκπαίδευση και η ευαισθητοποίηση του κοινού αποκτούν ολοένα και μεγαλύτερη σημασία. Είναι κρίσιμο οι άνθρωποι να κατανοήσουν τις βασικές αρχές της ψηφιακής ασφάλειας και πώς μπορούν να προστατεύσουν τον εαυτό τους στον ψηφιακό κόσμο.

Εκπαίδευση στην Ψηφιακή Ασφάλεια

Η εκπαίδευση στην ψηφιακή ασφάλεια θα πρέπει να ξεκινά από νεαρή ηλικία και να συνεχίζεται καθ' όλη τη διάρκεια της ζωής. Τα σχολεία, οι επιχειρήσεις και οι κυβερνητικοί οργανισμοί μπορούν να παίξουν σημαντικό ρόλο στην παροχή αυτής της εκπαίδευσης.
Για παράδειγμα, τα σχολεία θα μπορούσαν να εισάγουν μαθήματα ψηφιακής ασφάλειας στο πρόγραμμα σπουδών τους, διδάσκοντας στους μαθητές πώς να αναγνωρίζουν και να αποφεύγουν ψηφιακές απειλές. Οι επιχειρήσεις θα μπορούσαν να προσφέρουν τακτική εκπαίδευση στους υπαλλήλους τους σχετικά με τις βέλτιστες πρακτικές ασφαλείας.

Ευαισθητοποίηση του Κοινού

Η ευαισθητοποίηση του κοινού σχετικά με τη σημασία του DFIR και της ψηφιακής ασφάλειας είναι εξίσου σημαντική. Αυτό μπορεί να επιτευχθεί μέσω δημόσιων εκστρατειών, μέσων κοινωνικής δικτύωσης και άλλων καναλιών επικοινωνίας.
Για παράδειγμα, οι κυβερνήσεις θα μπορούσαν να διοργανώσουν "Μήνες Κυβερνοασφάλειας" με εκδηλώσεις και δραστηριότητες που στοχεύουν στην ενημέρωση του κοινού για τις ψηφιακές απειλές και τις μεθόδους προστασίας. Οι εταιρείες τεχνολογίας θα μπορούσαν να παρέχουν εύκολα κατανοητές οδηγίες ασφαλείας μαζί με τα προϊόντα τους.

Ηθικά Ζητήματα στο DFIR

Καθώς το DFIR γίνεται όλο και πιο διαδεδομένο, προκύπτουν σημαντικά ηθικά ζητήματα που πρέπει να αντιμετωπιστούν.

Ιδιωτικότητα vs Ασφάλεια

Ένα από τα βασικά διλήμματα είναι η ισορροπία μεταξύ ιδιωτικότητας και ασφάλειας. Ενώ οι τεχνικές DFIR μπορούν να βοηθήσουν στην προστασία μας από απειλές, μπορούν επίσης να χρησιμοποιηθούν για την παρακολούθηση και τον έλεγχο των ψηφιακών μας δραστηριοτήτων.

Για παράδειγμα, η χρήση τεχνικών DFIR για την παρακολούθηση της δραστηριότητας των εργαζομένων στο διαδίκτυο μπορεί να βελτιώσει την ασφάλεια της εταιρείας, αλλά ταυτόχρονα μπορεί να παραβιάσει την ιδιωτικότητα των εργαζομένων. Είναι σημαντικό να βρεθεί μια ισορροπία που προστατεύει τόσο την ασφάλεια όσο και την ιδιωτικότητα.

Χρήση DFIR από Κυβερνήσεις

Η χρήση τεχνικών DFIR από κυβερνήσεις για σκοπούς εθνικής ασφάλειας εγείρει επίσης ηθικά ζητήματα. Ενώ αυτές οι τεχνικές μπορούν να βοηθήσουν στην πρόληψη εγκλημάτων και τρομοκρατικών επιθέσεων, υπάρχει ο κίνδυνος κατάχρησης και παραβίασης των ανθρωπίνων δικαιωμάτων.
Είναι σημαντικό να υπάρχουν ισχυροί νόμοι και μηχανισμοί ελέγχου για να διασφαλιστεί ότι οι τεχνικές DFIR χρησιμοποιούνται με υπεύθυνο τρόπο και με σεβασμό στα ανθρώπινα δικαιώματα.

Συμπέρασμα

Το DFIR έχει γίνει αναπόσπαστο κομμάτι της καθημερινής μας ζωής, προστατεύοντας τα προσωπικά μας δεδομένα, διασφαλίζοντας την ασφάλειά μας στο διαδίκτυο και βοηθώντας στην απονομή δικαιοσύνης. Καθώς ο ψηφιακός κόσμος συνεχίζει να εξελίσσεται, η σημασία του DFIR θα συνεχίσει να αυξάνεται, διαδραματίζοντας καθοριστικό ρόλο στη διατήρηση της ασφάλειας και της ακεραιότητας του ψηφιακού μας περιβάλλοντος.

Η κατανόηση των βασικών αρχών του DFIR και η εφαρμογή βέλτιστων πρακτικών ασφαλείας στην καθημερινή μας ζωή μπορεί να μας βοηθήσει να προστατευτούμε καλύτερα από τις ψηφιακές απειλές. Είτε πρόκειται για την προστασία των προσωπικών μας δεδομένων, την ασφάλεια των επιχειρήσεών μας ή την εξασφάλιση της δικαιοσύνης, το DFIR παραμένει ένα ισχυρό εργαλείο στον αγώνα για έναν ασφαλέστερο ψηφιακό κόσμο.

Ωστόσο, καθώς η χρήση του DFIR γίνεται όλο και πιο συχνή, είναι σημαντικό να συνεχίσουμε να εξετάζουμε και να συζητάμε τις ηθικές επιπτώσεις της χρήσης του. Η εξισορρόπηση της ασφάλειας με την ιδιωτικότητα και τα ανθρώπινα δικαιώματα θα παραμείνει μια κρίσιμη πρόκληση καθώς προχωρούμε στο μέλλον.

Τελικά, η αποτελεσματική χρήση του DFIR απαιτεί τη συνεργασία μεταξύ ατόμων, επιχειρήσεων, κυβερνήσεων και της τεχνολογικής κοινότητας. Μόνο μέσω αυτής της συλλογικής προσπάθειας μπορούμε να δημιουργήσουμε ένα ασφαλές και δίκαιο ψηφιακό περιβάλλον για όλους.

Πλοήγηση στο πεδίο του κυβερνοχώρου με ασφάλεια και ενίσχυση των ψηφιακών «οχυρών»

Ελευθέριος Αθουσάκης
Μέντορας ΑΛΛΗΛΟΝ (Τομέα Κυβερνοασφάλειας)
Ειδικός σε θέματα Κυβερνοασφάλειας
Eleftherios A. | Linkedin

Περίληψη

Στον διαρκώς εξελισσόμενο κόσμο της κυβερνοασφάλειας, το 2023 σηματοδότησε ένα κομβικό σημείο. Καθώς τα ψηφιακά σύνορα διευρύνονταν με την αυξανόμενη χρήση Τεχνητής Νοημοσύνης, προέκυπταν νέες προκλήσεις για τους χρήστες της τεχνολογίας, τόσο για τους ιδιώτες όσο και για τις επιχειρήσεις. Σε αυτό το άρθρο εξετάζουμε τις εξελιγμένες επιθέσεις στον κυβερνοχώρο, καθώς και τις τεχνολογικές ανακαλύψεις στον τομέα της ασφάλειας. Δεν είναι απλώς μια αναδρομή στα γεγονότα, είναι ένας καθοδηγητικός φάρος μέσα από την ομίχλη της κυβερνοαβεβαιότητας, προσφέροντας προληπτικά μέτρα και στρατηγική πρόβλεψη. Με την κατανόηση του κυβερνοτοπίου του 2023, οι αναγνώστες γίνονται συμμέτοχοι στη διαμόρφωση ενός πιο ασφαλούς ψηφιακού μέλλοντος.

Ο σιωπηλός πόλεμος στον κυβερνοχώρο

Στην αχανή έκταση του ενός και του μηδέν, μαίνεται ένας σιωπηλός πόλεμος, μια μάχη που δεν διεξάγεται με σπαθιά και ασπίδες, αλλά με γραμμές κώδικα και κρυπτογραφημένους αλγορίθμους. Η κυβερνοασφάλεια, η τέχνη της προστασίας της ψηφιακής μας ύπαρξης, αποτελεί το τελευταίο μας προπύργιο ενάντια σε έναν αόρατο αντίπαλο. Πρόσφατα περιστατικά κατέδειξαν το διακύβευμα: κλεμμένα κρυπτονομίσματα στα οποία κάποιοι ίσως είχαν επενδύσει τους κόπους μιας ζωής, παραβιασμένες εταιρικές "πύλες", με λεία που υπολογίζεται ότι για το 2022 έφτασε τα 8,44 τρισεκατομμύρια Δολάρια Αμερικής **(1)**, και διαρκείς προσπάθειες διείσδυσης σε κρίσιμες υποδομές, όπως συστήματα υγείας, κυβερνητικές υπηρεσίες και εκπαιδευτικά ιδρύματα. Καθώς εμβαθύνουμε στις επιπλοκές αυτού του πολέμου, ας αποκρυπτογραφήσουμε πρώτα το λεξικό της άμυνας στον κυβερνοχώρο μέσα από κάποιες από τις τελευταίες επιθέσεις.

Πρόσφατες επιθέσεις στον κυβερνοχώρο: Μια ματιά στην άβυσσο

1. Κυβέρνηση της Κόστα Ρίκα. Το μέγεθος του "Κάστρου" δεν μετράει

Η κυβέρνηση της Κόστα Ρίκα **(2)** κήρυξε στα τέλη Απριλίου του 2022, κατάσταση έκτακτης ανάγκης μετά από εβδομάδες επιθέσεων Ransomware σε κρίσιμα συστήματά της. Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που κρυπτογραφεί τα δεδομένα ή τη συσκευή του θύματος, καθιστώντας τα μη προσβάσιμα μέχρι να καταβληθούν τα λύτρα τα οποία ο επιτιθέμενος ζητά από το θύμα, απειλώντας ότι θα κρατήσει τα δεδομένα ή τη συσκευή κλειδωμένα. Ως αποτέλεσμα, η κυβέρνηση δεν μπορούσε να πληρώσει εγκαίρως τους εργαζομένους της και τους ζήτησε να υποβάλουν αίτηση πληρωμής μέσω ηλεκτρονικού ταχυδρομείου ή με έντυπες μεθόδους. Η επίθεση διέκοψε επίσης τα φορολογικά και τελωνειακά συστήματα, προκαλώντας την κατάρρευση της εφοδιαστικής αλυσίδας εισαγωγών/εξαγωγών της χώρας. Η συμμορία Conti απαίτησε την καταβολή λύτρων ύψους 20 εκατομμυρίων δολαρίων Αμερικής, ισχυριζόμενη ότι οι επιθέσεις έγιναν για να ανατρέψουν την κυβέρνηση. Η εγκληματική συμμορία δημοσίευσε περίπου το 50% των δεδομένων που εκλάπησαν κατά τη διάρκεια της επίθεσης που διήρκεσε εβδομάδες. Η κυβέρνηση της Κόστα Ρίκα δεν κατέβαλε τα λύτρα. Όπως καταλαβαίνετε κανένα κάστρο, εικονικό ή φυσικό, δεν είναι αδιαπέραστο.

2. Η ληστεία κρυπτονομισμάτων της Crypto.com: Αποκρυπτογράφηση της παραβίασης

Επίσης στις αρχές του 2022, το Crypto.com, ένα από τα μεγαλύτερα κέντρα συναλλαγών κρυπτονομισμάτων, έπεσε θύμα μιας σχολαστικά ενορχηστρωμένης παραβίασης **(3)**. Σχεδόν 500 ψηφιακά πορτοφόλια χρηστών παραβιάστηκαν, με αποτέλεσμα την κλοπή 18 εκατομμυρίων δολαρίων Αμερικής σε Bitcoin και 15 εκατομμυρίων δολαρίων Αμερικής σε Ethereum, δύο από τα πιο γνωστά κρυπτονομίσματα παγκοσμίως. Οι επιτιθέμενοι κατάφεραν και παρέκαμψαν τον έλεγχο ταυτότητας δύο παραγόντων, εκθέτοντας την τρωτότητα ακόμη και των φαινομενικά απόρθητων συστημάτων. Το περιστατικό αυτό χρησιμεύει ως μια υπενθύμιση ότι η επαγρύπνηση είναι η πανοπλία μας και ο εφησυχασμός η αχίλλειος πτέρνα μας.

3. Εθνική Υπηρεσία Υγείας του Ηνωμένου Βασιλείου (NHS)

Το NHS παρέχει υποδομές για δεκάδες χιλιάδες οργανισμούς υγείας. Από τον Απρίλιο του 2022 και σε διάστημα έξι μηνών, μια επίθεση παραβίασε πάνω από 100 λογαριασμούς υπαλλήλων του NHS και τους χρησιμοποίησε για την αποστολή μηνυμάτων ηλεκτρονικού "ψαρέματος" **(4)**. Ορισμένες από τις εκστρατείες phishing, όπως είναι γνωστές, επιχείρησαν να υποκλέψουν διαπιστευτήρια της Microsoft. Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου ήταν κατά κύριο λόγο ψεύτικες ειδοποιήσεις λήψης εγγράφων, συνοδευόμενες από μια δήλωση αποποίησης ευθυνών του NHS στο τέλος κάθε μηνύματος. Ο πόλεμος κατά των απειλών στον κυβερνοχώρο μαίνεται αδιάκοπα, απαιτώντας διαρκή επαγρύπνηση.

4. Η διαρκής πολιορκία της News Corp: Η παραβίαση που αντηχεί στο χρόνο

Η News Corp, ο παγκόσμιος κολοσσός των μέσων ενημέρωσης, αντιμετώπισε παραβιάσεις των διακομιστών του που χρονολογείται ότι ξεκίνησαν από τον Φεβρουάριο του 2020 **(5)**. Η κλίμακα της επίθεσης υπογραμμίζει την επιμονή των κυβερνοεγκληματιών, οι οποίοι συνεχίζουν να εκμεταλλεύονται τα τρωτά σημεία πολύ καιρό μετά την αρχική παραβίαση. Γι' αυτό και οι τακτικοί έλεγχοι ασφαλείας, η διαχείριση ενημερώσεων και η ισχυρή κρυπτογράφηση αποτελούν τα προπύργιά μας απέναντι στους αδυσώπητους αυτούς αντιπάλους.

Επίγνωση της ασφάλειας στον κυβερνοχώρο: Η ασπίδα μας ενάντια στην καταιγίδα

1. Εκπαίδευση και κατάρτιση: Ο φάρος της ανθεκτικότητας

1.1. Μείνετε ενημερωμένοι

Η γνώση είναι η πρώτη γραμμή άμυνάς μας. Μείνετε ενήμεροι για τις αναδυόμενες απειλές μέσω ενημερωτικών δελτίων ασφαλείας, ιστολογίων και διαδικτυακών σεμιναρίων. Κατανοήστε τις τακτικές των εγκληματιών του κυβερνοχώρου, τις τεχνικές ηλεκτρονικού ψαρέματος, τα τεχνάσματα κοινωνικής μηχανικής και τις εκμεταλλεύσεις ευπαθειών άγνωστων μέχρι την ημέρα εύρεσής τους; γνωστές και ως zero-day. **Θυμηθείτε**: η άγνοια είναι σύμμαχός τους - η ευαισθητοποίηση είναι δική μας.

1.2. Προγράμματα κατάρτισης: Η σφυρηλάτηση των Φρουρών

Ενδυναμώστε το προσωπικό σας με εκπαίδευση για την ασφάλεια στον κυβερνοχώρο. Από τη γραμματεία μέχρι τη διοίκηση, ο καθένας παίζει το ρόλο του. Διδάξτε τους να διακρίνουν τα ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, να αναγνωρίζουν τις επικίνδυνες ενδείξεις και να υπερασπίζονται την τήρηση των κανόνων ασφαλείας. Θυμηθείτε, μια καλά εκπαιδευμένη ομάδα είναι το ισχυρότερο αμυντικό προπύργιο ενός οργανισμού.

2. Ισχυροί μηχανισμοί πιστοποίησης: Οχυρώνοντας τις "Πύλες"

2.1. Αυθεντικοποίηση δύο παραγόντων (2FA)

Εφαρμόστε αυθεντικοποίηση δύο παραγόντων όπου είναι εφικτό. Προσθέτει ένα επιπλέον επίπεδο ασφάλειας, απαιτώντας μια δεύτερη μορφή επαλήθευσης πέρα από τους κωδικούς πρόσβασης. Είτε πρόκειται για κωδικό μηνύματος κειμένου είτε για βιομετρική σάρωση, η εφαρμογή της τεχνολογίας 2FA αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση.

2.3. Βιομετρικά στοιχεία: Η υπογραφή του Φύλακα

Αξιοποιήστε τον βιομετρικό έλεγχο ταυτότητας για κρίσιμα συστήματα. Οι σαρώσεις δακτυλικών αποτυπωμάτων, η αναγνώριση προσώπου και τα μοτίβα ίριδας παρέχουν μοναδικά αναγνωριστικά. Δεν ενισχύουν μόνο την ασφάλεια, αλλά και βελτιώνουν την εμπειρία των χρηστών, ένα πλεονέκτημα για τις ψηφιακές μας "εστίες".

3. Τακτικοί έλεγχοι ασφαλείας: Η επαγρύπνηση του Φύλακα

3.1. Δοκιμές διείσδυσης: Αποκάλυψη τρωτών σημείων

Οι ηθικοί χάκερ προσομοιώνουν επιθέσεις που θα εκτελούσαν κακόβουλοι στην υποδομή σας, εξετάζοντας τις άμυνες των συστημάτων σας. Τα ευρήματά τους αποκαλύπτουν πιθανές ρωγμές στη θωράκιση σας. Αντιμετωπίστε τα αμέσως, ο εφησυχασμός προκαλεί συμφορές.

3.2. Διαχείριση διορθώσεων: Σφράγιση σημείων παραβίασης

Οι ενημερώσεις λογισμικού δεν είναι απλώς ενοχλήσεις, είναι ζωτικής σημασίας. Οι διορθώσεις αυτές συχνά αποκαθιστούν ευπάθειες που εκμεταλλεύονται οι επιτιθέμενοι στον κυβερνοχώρο. Η παραμέληση των ενημερώσεων είναι σαν να αφήνετε τις πύλες του "κάστρου" σας μισάνοιχτες.

4. Κρυπτογράφηση δεδομένων και δημιουργία αντιγράφων ασφαλείας

4.1. Κρυπτογράφηση: Η διασφάλιση των "περγαμηνών" μας

Θα πρέπει να γίνεται κρυπτογράφηση ευαίσθητων δεδομένων τόσο κατά τη μετάδοση όσο και κατά την αποθήκευση. Εμπιστευτικά μηνύματα ηλεκτρονικού ταχυδρομείου, οικονομικά αρχεία, πνευματική ιδιοκτησία - όλα αξίζει να επενδυθούν με τον μανδύα της κρυπτογράφησης. Έτσι ακόμα και αν υποκλαπούν, θα παραμείνουν ακατανόητα και άχρηστα για τους κακόβουλους.

4.2. Τακτικά αντίγραφα ασφαλείας: Οι "περγαμηνές" της ανθεκτικότητας

Το Ransomware μπορεί να σας χτυπήσει, αλλά τα αντίγραφα ασφαλείας μπορούν να αποκαταστήσουν τα κρυπτογραφημένα δεδομένα σας χωρίς να χρειαστεί να υποκύψετε σε εκβιασμούς. Δημιουργείστε τακτικά αντίγραφα ασφαλείας των κρίσιμων πληροφοριών. Ο πλεονασμός είναι η ασπίδα μας ενάντια στο χάος.

Η Αποφασιστικότητα του Φύλακα

Καθώς πλοηγούμαστε στα ύπουλα νερά του κυβερνοχώρου, ας λάβουμε υπόψη μας τα λόγια του μεγάλου κρυπτογράφου Bruce Schneier:

"Ο μόνος ασφαλής υπολογιστής είναι αυτός που είναι αποσυνδεδεμένος από την πρίζα, κλειδωμένος σε ένα χρηματοκιβώτιο, και θαμμένος 20 πόδια κάτω από το έδαφος σε μια μυστική τοποθεσία... και δεν είμαι καν πολύ σίγουρος γι' αυτό".

Η επαγρύπνησή μας και η δέσμευσή μας για ευαισθητοποίηση στον τομέα της κυβερνοασφάλειας μπορούν να μεταμορφώσουν αυτό το ζοφερό σενάριο. Ας οχυρωθούμε κατάλληλα.

Πηγές – Βιβλιογραφία

1. https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety
2. Costa Rica State of Emergency Declared After Ransomware Attacks (securityintelligence.com)
3. Crypto.com Admits $35 Million Hack (forbes.com)
4. https://www.netsec.news/113-email-accounts-compromised-in-nhs-phishing-attack/
5. Hack of News Corp Emails Is Believed to Be Linked to China - The New York Times (nytimes.com)

Βιογραφικό

Ο Ελευθέριος Αθουσάκης έχει πάνω από 20 χρόνια συνολικής εμπειρίας στο χώρο των Επικοινωνιών-Πληροφορικής και της ασφάλειας πληροφορίων με πολυετή εμπειρία σε διεθνής οργανισμούς (NATO, ΕΕ).
Είναι κάτοχος MSc στην Ασφάλεια Πληροφοριών και Ηλεκτρονική Εγκληματολογία και μέλος του ISC2 Hellenic Chapter.
Εργάζεται στο Γενικό Επιτελείο Εθνικής Άμυνας.

Ένθετο Β: Ασφάλεια και Ανθεκτικότητα

Μήνυμα Προσκεκλημένου Εκδότη

Η στρατιωτική, αεροπορική, διαστημική, βιομηχανική, οικονομική και τεχνολογική διάσταση της ασφάλειας

Αντισυνταγματάρχης ε.α. Κουκάκης Γεώργιος
Μέλος ΑΛΛΗΛΟΝ
Διεθνολόγος, Συγγραφέας, Κύριος Ερευνητής του ΚΕΔΙΣΑ, Research Associate of HERMES, Μέλος του ΕΛ.Ι.Σ.ΜΕ., της ΑΛΛΗΛΟΝ και της Mercury Negotiation Academy, Ακαδημαϊκός Υπεύθυνος του Προγράμματος «Σπουδές Ασφάλειας στη Μεσόγειο (BASIC)» του ΚΕΔΙΒΙΜ Πανεπιστημίου Αιγαίου
Georgios Koukakis | Linkedin

Στο προηγούμενο μήνυμά μου το οποίο είχε δημοσιευτεί στο 14ο τεύχος του περιοδικού eΆλληλον, είχα αναφερθεί στον προσωπικό στόχο που είχα θέσει ως Προσκεκλημένος Εκδότης να συμβάλλω στην απομυθοποίηση των πολυδιάστατων εννοιών της **ασφάλειας** (security) και της **ανθεκτικότητας** (resilience). Το εν λόγω ένθετο, το οποίο αποτελεί συνέχεια του αντίστοιχου του 14ου τεύχους, περιέχει επτά (7) άρθρα τα οποία αναδεικνύουν τις ποικίλες συνιστώσες της ασφάλειας και της ανθεκτικότητας, δίνοντας έμφαση στην **αμυντική της διάσταση**.

Κατόπιν των παραπάνω, είμαι στην ευχάριστη θέση να σας παρουσιάσω τους **αρθρογράφους** του ένθετου του 15ου τεύχους –τους οποίους ευχαριστώ θερμά για την συμβολή τους– καθώς και να αναφέρω με συντομία τις **θεματικές** των άρθρων τους, τα οποία παρουσιάζονται με τη γεωγραφική-χωροταξική σειρά των πεδίων (domains) του πολυχωρικού πεδίου μάχης (Multi-Domain Battlefield, MDB), δηλαδή το **χερσαίο πεδίο** (land domain), το **εναέριο πεδίο** (air domain) και το **διαστημικό πεδίο** (space domain), ακολουθούμενα από ένα άρθρο για το ρόλο της **οικονομίας** και ένα για το ρόλο της **αμυντικής βιομηχανίας**, παράγοντες οι οποίοι συμβάλλουν στη ενίσχυση της ασφάλειας και της ανθεκτικότητας.

Ο **κ. Θεοχαράκος Σπυρίδων** συμμετέχει στο παρόν τεύχος με ένα άρθρο το οποίο –με αφορμή την ένοπλη σύγκρουση μεταξύ Ισραήλ και Χαμάς– αναδεικνύει την επίδραση των περιφερειακών συγκρούσεων στην εθνική ασφάλεια της Ελλάδας. Μεταξύ άλλων αναφέρεται στις επιδιώξεις του Ισραήλ, την εργαλειοποίηση της πίστης, τις αθρόες μεταναστευτικές ροές, τις οικονομικές συνέπειες, τα κυρίαρχα συμφέροντα των κρατών και τους κίνδυνους που ελλοχεύουν από την τηρητέα στάση αυτών, καταλήγοντας στην ανάγκη θέσπισης μίας εθνικής στρατηγικής.

Η **κ. Λυριστής Μηνάς** αναφέρεται σε μία άλλη διάσταση της ένοπλης σύγκρουσης στη Λωρίδα της Γάζας, την ενδεχόμενη επέκτασή της στο Βορρά και τη δημιουργία ενός νέου μετώπου μεταξύ Ισραήλ - Λιβάνου και πως μία τέτοια εξέλιξη θα επηρεάσει την εθνική ασφάλεια της Ελλάδας και την περιφερειακή ασφάλεια γενικότερα. Αναλύσει τα στρατιωτικά μέσα και τις τακτικές της Χεζμπολάχ τονίζοντας το ρόλο των UAVs, του ηλεκτρονικού πολέμου και των επιχειρήσεων στον κυβερνοχώρο, και την επίδραση των νέων συνθηκών στα υφιστάμενα δόγματα που διέπουν τις επιχειρήσεις αέρος-εδάφους.

Ο **κ. Καρατζάς Ελευθέριος** πραγματοποιεί μία ανάλυση των διδαγμάτων που προκύπτουν από τη χρήση μικρών Μη Επανδρωμένων Συστημάτων (Unmanned Systems) στις σύγχρονες ένοπλες συγκρούσεις με έμφαση στον τρόπο που αυτά επιδρούν στη στρατιωτική ανθεκτικότητα διάφορων δρώντων. Αναφέρεται στους τρόπους δράσης τους, τις κύριες αποστολές, το σημαντικό ρόλο που διαδραματίζει ο χειριστής, καθώς και τις μελλοντικές τάσεις που αναμένεται να επικρατήσουν στο τομέα της χρήσης των εν λόγω συστημάτων.

Ο **κ. Γιακουμής Άγγελος** αναφέρεται στη διαστημική ασφάλεια,

αναλύοντας τα είδη και τις επιπλοκές των διαστημικών όπλων, το ισχύον ρυθμιστικό πλαίσιο που διέπει την εκμετάλλευση του διαστήματος, το φαινόμενο της οπλοποίησης του διαστήματος (weaponization of space) και πως αυτό επηρεάζει την ανθεκτικότητα των διαστημικών υποδομών και τέλος εγείρει την προσοχή όλων μας, καθώς –όπως επισημαίνει– αν δεν ληφθούν κατάλληλα μέτρα στο προσεχές μέλλον, η υφιστάμενη αρχιτεκτονική ασφάλειας του διαστήματος ενδέχεται να ανατραπεί.

Ο **κ. Χωριανόπουλος Άγγελος**, μέσα από το άρθρο του για το μέλλον της αεροδιαστημικής βιομηχανίας υπό το πρίσμα της τεχνητής νοημοσύνης (Artificial Intelligence, AI) επισημαίνει το ρόλο τόσο της διαστημικής όσο και της βιομηχανικής ασφάλειας, αναλύοντας τις τάσεις που επικρατούν όσον αφορά τις στρατηγικές συμφωνίες και τις επενδύσεις στην AI, της ηγέτιδες χώρες στον εν λόγω τομέα, τις μελλοντικές επιπτώσεις, και την ανάγκη ενσωμάτωσης των εν λόγω τεχνολογιών από τις Ένοπλες Δυνάμεις.

Ο **κ. Μπλάνος Παναγιώτης** συμμετέχει στο παρόν τεύχος με ένα άρθρο το οποίο αναδεικνύει το ρόλο του Ευρωπαϊκού Μηχανισμού για την Ειρήνη (European Peace Facility, EPF) όσον αφορά την ασφάλεια και την ανθεκτικότητα σε εθνικό (κράτη-μέλη) και υπερεθνικό (ΕΕ) επίπεδο, εντός του πλαισίου της Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας (ΚΕΠΠΑ) της ΕΕ. Με τον τρόπο αυτό μας δίνει να καταλάβουμε τη σχέση μεταξύ της οικονομικής ασφάλειας/ανθεκτικότητας και της στρατιωτικής ασφάλειας/ανθεκτικότητας, των δύο βασικών πυλώνων της σκληρής ισχύος (hard power).

Η συνεισφορά τέλος του **υποφαινόμενου προσκεκλημένου εκδότη** έγκειται σε ένα άρθρο σχετικά με την Ευρωπαϊκή Αμυντική Βιομηχανική Στρατηγική (European Defence Industrial Strategy) που δημοσιεύτηκε για πρώτη φορά στις 5 Μαρτίου 2024 και τη συμβολή της όχι μόνο στην Ευρωπαϊκή και εθνική ασφάλεια και την ανθεκτικότητα, αλλά και την επιχειρηματικότητα και τη μείωση της ανεργίας.

Θα ήθελα επίσης να ευχαριστήσω και πάλι μέσα από το δημόσιο αυτό βήμα που μου δίδεται τον Ιδρυτή και Πρόεδρο της ΑΛΛΗΛΟΝ κ. **Άγγελο Παγκράτη**, τη **συντακτική ομάδα** του eΆλληλον, καθώς και **όλες/όλους όσοι συνέβαλαν με οποιονδήποτε τρόπο** στην εκπόνηση και δημοσίευση του παρόντος τεύχους.

Ολοκληρώνοντας τέλος το παρόν μήνυμα και έχοντας ήσυχη τη συνείδησή μου όσον αφορά τη μικρή συμβολή μου στην αποκατάσταση της «υπόληψης» της παρεξηγημένης ασφάλειας και της αφανούς ανθεκτικότητας, θα ήθελα να επισημάνω το ζωτικό ρόλο που διαδραματίζει η ασφάλεια και η ανθεκτικότητα σε κάθε έκφανση της καθημερινής ζωής των πολιτών και να ευχηθώ να μην χρειαστεί ποτέ να καταλάβουμε τη σημασία αυτών μέσα από την απουσία τους. Εν κατακλείδι, πρέπει να γίνει αντιληπτό αυτό που ο **Thomas Hobbes** επεσήμανε ήδη από τις αρχές του 17ου αιώνα, ότι δηλαδή:

«[…] χωρίς ασφάλεια δεν υπάρχει δεν υπάρχει χώρος για τη βιομηχανία .. δεν υπάρχουν τέχνες, δεν υπάρχουν γράμματα, δεν υπάρχει κοινωνία και το χειρότερο είναι απ' όλα, συνεχής φόβος και κίνδυνος βίαιου θανάτου- και η ζωή του ανθρώπου, μοναχική, φτωχή, άσχημη, κτηνώδης και σύντομη».[1]

1 Coupland, R. (2001). Humanity: What is it and how does it influence international law?. ICRC.83(844), 980. https://international-review.icrc.org/sites/default/files/S156077550018349Xa.pdf

Πώς επηρεάζουν οι περιφερειακές συγκρούσεις την εθνική μας ασφάλεια;

Η περίπτωση του πολέμου Ισραήλ – Χαμάς και οι κίνδυνοι κλιμάκωσης της σύγκρουσης

Θεοχαράκος Σπυρίδων
Μέντορας ΑΛΛΗΛΟΝ
Αξιωματικός Στρατού Ξηράς, φοιτητής Τμήματος Βαλκανικών, Σλαβικών και Ανατολικών Σπουδών του Πανεπιστημίου Μακεδονίας
Spiros Theocharakos | LinkedIn

Περίληψη

Σε ένα αλληλοεξαρτούμενο, παγκοσμιοποιημένο κόσμο, γεγονότα σε ένα κράτος είναι ικανά να προκαλέσουν αλυσιδωτές αντιδράσεις σε άλλα μέρη του κόσμου, με απρόβλεπτα αποτελέσματα. Το άρθρο θα επιχειρήσει να αναδείξει τους κινδύνους που αναδύονται από την κλιμάκωση του πολέμου στη Μέση Ανατολή για τη χώρα μας και την εθνική μας ασφάλεια. Ενδεικτικά θα γίνει αναφορά σε τομείς όπως η μετανάστευση, η ενεργειακή αστάθεια, ο οικονομικός αντίκτυπος, η στρατιωτική ασφάλεια και αβεβαιότητα, η πολιτική αστάθεια και τα διπλωματικά διλήμματα που ανακύπτουν.

Με την τεταμένη κατάσταση της σύρραξης στη Μέση Ανατολή ανάμεσα στο Ισραήλ και τη Χαμάς, έχουμε γίνει μάρτυρες ενός επικίνδυνου "γεωπολιτικού παιγνίου" με διαστάσεις ανθρωπιστικής κρίσης. Η απόφαση της κυβέρνησης Νετανιάχου για άνευ προηγουμένου κλιμάκωση της σύγκρουσης, με στρατιωτικές επιχειρήσεις μεγάλης κλίμακας στο έδαφος της Γάζας, έχει πυροδοτήσει την αντίδραση της διεθνούς κοινότητας, που σπεύδει να καταδικάσει ή να υπερασπιστεί τη μια ή την άλλη πλευρά. Παραδοσιακά προπύργιο της Δύσης στη Μέση Ανατολή, το Ισραήλ διατηρεί αμφιλεγόμενα την υποστήριξη της κυβέρνησης των Η.Π.Α., παρόλο που η τελευταία ασκεί πιέσεις για αποκλιμάκωση. Στον αντίποδα, ανοιχτά κατά των ενεργειών του Τελ Αβίβ τάσσεται η πλειονότητα των Μουσουλμανικών κρατών της περιοχής, με εξέχον το Ιράν και τις υποστηριζόμενες από αυτό παραστρατιωτικές οργανώσεις του σε άλλα κράτη.

Καθώς η κατάσταση ολοένα και κλιμακώνεται, το Ισραήλ περιχαρακώνεται σθεναρά σε μια στρατηγική εξόντωσης του αντιπάλου, χωρίς υπολογισμό των συνεπειών της "επόμενης ημέρας" του πολέμου. Με φρούδες ελπίδες εξεύρεσης μιας κοινά αποδεκτής

λύσης, είναι εύλογο, πλέον, να αναρωτιόμαστε για τις συνέπειες αυτής της νέας τάξης πραγμάτων στη Μέση Ανατολή για τον υπόλοιπο κόσμο. Η μελέτη, επομένως, των χαρακτηριστικών που διαθέτει ένας περιφερειακός πόλεμος, όπως αυτός στη Μέση Ανατολή, είναι ικανή να μας προσφέρει μια ρεαλιστική πρόγνωση των γεγονότων τα οποία θα κληθούμε να αντιμετωπίσουμε ως ελληνισμός.

Το παράδειγμα της Μέσης Ανατολής είναι διαβόητο στο θέμα της συνύπαρξης πληθυσμών με διαφορετικές θρησκευτικές πεποιθήσεις. Η μισαλλοδοξία και η εργαλειοποίηση της πίστης έχουν εδραιώσει εχθρικό κλίμα στις διακρατικές σχέσεις και στις σχέσεις των τοπικών κοινοτήτων. Σε παρόμοιο πλαίσιο, οι εθνοτικοί διαχωρισμοί έχουν αποτελέσει γόνιμο έδαφος για ριζοσπαστικές ιδεολογίες και εξτρεμιστικές ομάδες. Αυτές οι ομάδες μπορεί να επιδιώξουν να επεκτείνουν την επιρροή τους πέρα από τα σύνορα, συνιστώντας άμεση απειλή για την ασφάλεια των γειτονικών χωρών μέσω της τρομοκρατίας. Ο πόλεμος έρχεται να διαιωνίσει αυτή την κατάσταση, με τον κίνδυνο εξάπλωσης των φαινομένων αυτών στα γειτονικά κράτη. Ως επακόλουθο, τα κράτη μπορεί να οδηγηθούν σε αναταραχές στο εσωτερικό τους, διακοινοτική βία και προκλήσεις για τη συνοχή και τη διακυβέρνησή τους.

Δεν αποτελεί έκπληξη ότι η μετανάστευση πληθυσμών συνιστά τον κυριότερο άμεσο αντίκτυπο κάθε εμπόλεμης σύγκρουσης. Καθώς η επιτυχία εν πολλοίς καθορίζεται από τον έλεγχο εδάφους και κατοικημένων περιοχών, οι αντιμαχόμενοι θέτουν ως προτεραιότητα τον έλεγχο αυτών με δραματικές, συνήθως, επιπτώσεις στην ασφάλεια του τοπικού πληθυσμού. Αυτό με τη σειρά του οδηγεί σε μετατόπιση πληθυσμών, προσφυγικές ροές και εξάπλωση φαινομένων βίας. Το γενικότερο κλίμα αστάθειας έχει την τάση να διαχέεται στις γύρω περιοχές, απειλώντας την ασφάλεια και τη σταθερότητά τους.

Σε οικονομικό επίπεδο, οι ένοπλες συγκρούσεις προκαλούν άμεσες και έμμεσες συνέπειες τόσο στα εμπόλεμα μέρη, όσο και στη διεθνή κοινότητα. Η παγκοσμιοποίηση του εμπορίου καθίσταται εφικτή αν και εφόσον οι εμπορικές οδοί διατηρούνται ανοιχτές, ασφαλείς και με επαρκείς υποδομές. Δυστυχώς, η αστάθεια που έπεται ενός πολέμου προκαλεί αλλαγές στην παγκόσμια εμπορική δραστηριότητα, ενώ οι επενδύσεις στα ίδια τα εμπόλεμα μέρη κρίνονται ως υψηλού ρίσκου. Η οικονομία των περιοχών αυτών πλήττεται, με τις επιπτώσεις να κυμαίνονται από απώλεια εσόδων έως αυξημένα έξοδα που απαιτούνται για τη διαχείριση των συνεπειών της σύγκρουσης. Η διεθνής κοινότητα επιβαρύνεται επίσης, με αυξημένο κόστος που οφείλεται στις αλλαγές των εμπορικών δρομολογίων, την αδυναμία εισαγωγών και εξαγωγών προς και από τα εμπόλεμα κράτη και τη μείωση του διεθνούς ανταγωνισμού, που προκύπτει από το μοντέλο της οικονομίας της αγοράς που επικρατεί.

Στον ενεργειακό τομέα, οι τιμές του πετρελαίου και του φυσικού αερίου επηρεάζονται, ως γνωστόν, από τις εκάστοτε διεθνείς προκλήσεις. Στην περίπτωση της Μέσης Ανατολής, τυχαίνει να συγκεντρώνονται τεράστια ποσοστά της παγκόσμιας παραγωγής, με άμεσο αντίκτυπο στις παγκόσμιες τιμές της ενέργειας και κατ' επέκταση των καταναλωτικών αγαθών και υπηρεσιών. Οι διαδρομές δε των αγωγών μεταφοράς είναι κρίσιμης σημασίας για το τελικό κόστος της ενέργειας. Η αστάθεια μιας σύρραξης εκτοξεύει το κόστος της ενέργειας, καθώς περιορίζεται η προσφορά της, ενώ αναζητούνται νέες, ασφαλέστερες οδοί για να καλύψουν την ολοένα και αυξανόμενη ζήτηση.

Η πολιτική δεν θα μπορούσε, σαφώς, να λείπει από το κάδρο, καθώς στη σύγχρονη εποχή, περισσότερο ίσως από ποτέ, οι διεθνείς σχέσεις κυριαρχούνται από πολιτικές συμμαχίες και "παιχνίδια συμφερόντων". Υπό αυτό το πρίσμα, οι πολεμικές συγκρούσεις προκαλούν ρωγμές στα θεμέλια των διμερών σχέσεων, με τα κράτη να αναγκάζονται, πολλές φορές, να πάρουν θέση ή να ακολουθήσουν περίπλοκες πολιτικές, που μπορεί να επηρεάσουν τα συμφέροντα και τις συμμαχίες τους, με αρνητικό αντίκτυπο στην εθνική τους ασφάλεια.

Απόρροια των όσων αναφέρθηκαν είναι η ενδεχόμενη στρατιωτική εμπλοκή τρίτων μερών. Λόγοι εθνικής ασφάλειας ή ενδυνάμωσης του εκάστοτε κυβερνώντος καθεστώτος οδηγούν τα τρίτα κράτη σε στρατιωτική στήριξη μιας εμπόλεμης παράταξης. Αυτό συμβαίνει με απώτερο σκοπό την προστασία των συμφερόντων τους και την πρόσβαση σε ζωτικούς πόρους, όπως το έδαφος, η πρόσβαση στη θάλασσα, η ενέργεια και οι φυσικοί πόροι. Η στήριξη μπορεί να είναι έμμεση, με τη μορφή, για παράδειγμα, στρατιωτικού εξοπλισμού, ιατροφαρμακευτικής περίθαλψης, ιματισμού και χρηματικού κεφαλαίου, ή και άμεση, με πλήρους κλίμακας στρατιωτική εμπλοκή στο πλευρό του υποστηριζόμενου μέρους.

Η Ελλάδα και η Κύπρος τοποθετούνται γεωγραφικά στην "ευρύτερη γειτονιά" της Μέσης Ανατολής. Ως εκ τούτου επηρεάζονται ποικιλοτρόπως από τα τεκταινόμενα της περιοχής. Ας μην ξεχνάμε ότι αμφότερες διαθέτουν εκτενείς ακτογραμμές και θαλάσσια σύνορα σε σχετικά μικρή απόσταση από τις ακτές της Συρίας, του Λιβάνου, του Ισραήλ και της Λωρίδας της Γάζας. Ως οι εγγύτερες σε απόσταση από τη Μέση Ανατολή ευρωπαϊκές χώρες, είναι εύλογο να πρωτοστατούν στη χάραξη της πολιτικής της Ευρωπαϊκής Ένωσης γύρω από την περιοχή. Η αστάθεια που επικρατεί στη Μέση Ανατολή, είναι ικανή να οδηγήσει στην εξάπλωση εξτρεμιστικών και παραστρατιωτικών ομάδων, οι οποίες θα στραφούν όχι μόνο κατά του Ισραήλ, αλλά και κατά των κρατών που δείχνουν ανοχή και στήριξη στην πολιτική του, όπως η πλειονότητα των χωρών της Δύσης.

Η συνύπαρξη των λαών της Μέσης Ανατολής δεν ήταν ποτέ ειρηνική. Όμως κανένας λαός δεν επιθυμεί εγγενώς τη σύγκρουση. Η ειρήνη στην περιοχή υποδαυλίζεται συνεχώς από πολιτικές που επιτάσσουν οι ελίτ πολιτικού, θρησκευτικού και στρατιωτικού φάσματος. Η πρόσφατη σύγκρουση μεταξύ Ισραήλ και Χαμάς και η εξέλιξή της, έχει εκτροχιάσει την ελπίδα για μια μακροπρόθεσμη, βιώσιμη συνύπαρξη των λαών. Και παρόλο που η περιοχή βρίσκεται στο επίκεντρο της προσοχής των ισχυρών διεθνών δρώντων, δεν παρατηρούμε δυναμικές παρεμβάσεις για αποκλιμάκωση της σύγκρουσης. Καθίσταται, επομένως, επιτακτική η υιοθέτηση εθνικής στρατηγικής, με γνώμονα το διεθνές δίκαιο, για την υπεράσπιση των εθνικών μας συμφερόντων

σε αυτό το νέο, δυναμικό, διεθνές πλαίσιο που σχηματίζεται.

Ενδεικτικές Πηγές

- Indyk, M. (2021). *Master of the game: Henry Kissinger and the Art of Middle East Diplomacy.* Knopf.
- El-Baghdadi, I., & Gatnash, A. (2021). *The Middle East Crisis Factory: Tyranny, Resilience and Resistance.* Oxford University Press.
- Von Clausewitz, C. (2008). *On war*. Princeton University Press.
- Walzer, M. (2015). *Just and unjust wars: A Moral Argument with Historical Illustrations*. Hachette UK.
- Iklé, F. C. (2005). *Every war must end*. Columbia University Press.

Η πιθανή σύγκρουση Ισραήλ-Λιβάνου και οι νέες τακτικές μάχης ως παράγοντας επιρροής της εθνικής ασφάλειας της Ελλάδας και της περιφερειακής ασφάλειας

Μηνάς Λυριστής
Μέλος ΑΛΛΗΛΟΝ
Υπ. Διδάκτωρ Διεθνούς Πολιτικής στη Μέση Ανατολή, Δόκιμος Έφεδρος Αξιωματικός (ΠΖ)
Minas Lyristis | LinkedIn

Περίληψη

Η πιθανότητα πολέμου μεταξύ Ισραήλ και Χεζμπολάχ αυξάνεται, με τα μη επανδρωμένα αεροσκάφη (UAVs) να παίζουν κρίσιμο ρόλο. Το Ισραήλ έχει ενισχύσει τις δυνάμεις του στα βόρεια σύνορα, ενώ η Χεζμπολάχ έχει βελτιώσει σημαντικά τις δυνατότητες της στα UAVs, επιτρέποντας της να επιτηρεί και να στοχεύει βαθιά εντός της ισραηλινής επικράτειας. Αν και οι δυνατότητες της παραμένουν περιορισμένες σε σύγκριση με το Ισραήλ, η Χεζμπολάχ δείχνει ότι τα UAVs θα είναι κεντρικά σε μια πιθανή σύγκρουση, υπογραμμίζοντας την ανάγκη για προσαρμογή στις νέες τεχνολογικές συνθήκες.

Έπειτα από το πρόσφατο κύμα επιβεβαιωμένων και μη δολοφονιών και χτυπημάτων στη Βηρυτό, την Τεχεράνη και το Χαν Γιουνίς, η πιθανότητα ενός τρίτου πολέμου μεταξύ Ισραήλ και Χεζμπολάχ έχει αυξηθεί αισθητά. Σε μία τέτοια περίπτωση οι δύο αντίπαλοι αναμένεται να αναπτύξουν εκτενώς μη επανδρωμένα αεροσκάφη, διαφόρων τύπων με σκοπό την υπεροχή σε αναγνώριση, επιθετικές ενέργειες ή αντεπιθέσεις. Το σενάριο «ειρήνης μέσω της τρομοκρατίας», όπου η συμβατική αποτροπή θα απέτρεπε ή θα ανέβαλε το ξέσπασμα ενός πολέμου πλήρους κλίμακας ήταν το προηγούμενο διάστημα το κυρίαρχο αφήγημα. Τότε, η στάση του Ισραήλ κατά μήκος των λιβανικών συνόρων ήταν κυρίως αμυντική. Ωστόσο, η στάση του Τελ Αβίβ μετατράπηκε γρήγορα σε επιθετική.

Εικόνα 1: Χάρτης της ευρύτερης περιοχής του πολέμου στη Γάζα
Πηγή: https://map.proxi.co/r/wt-kxaUyqy7x9v_jObc9

Αυτή η επιθετική στάση ενισχύθηκε από την αναδιάταξη μονάδων από τη Γάζα, συμπεριλαμβανομένων ταξιαρχιών από την 36η τακτική μεραρχία της Βόρειας Διοίκησης. Πρόκειται για την ίδια μεραρχία που προηγουμένως διχοτόμησε τη Γάζα σε βόρειο και νότιο τμήμα, πολεμώντας προς τη Μεσόγειο για τη δημιουργία του διαδρόμου Netzarim. Επιπλέον, ταξιαρχίες από την επίλεκτη 98η Μεραρχία Αλεξιπτωτιστών και την 146η Εφεδρική Μεραρχία έχουν μεταφερθεί ή τοποθετηθεί εκ νέου στο βορρά. Η σημερινή μάχιμη δύναμη των τριών μεραρχιών –12 ταξιαρχίες– είναι περίπου διπλάσια από το μέγεθος της δύναμης εισβολής του Ισραήλ τον Ιούλιο του 2006. Τον Αύγουστο του 2024, μόνο μερικές από τις ταξιαρχίες εφόδου αυτών των μεραρχιών αναφέρονταν ότι βρίσκονταν στις θέσεις τους. Παρ' όλα αυτά, για να αποφευχθούν οι πανωλεθρίες του πολέμου του 2006 [1] και για να εκδιωχθούν με επιτυχία οι επίμονες μονάδες της Χεζμπολάχ πάνω από τον ποταμό Λιτάνι προς τα βόρεια, ο ισραηλινός στρατός θα χρειαστεί σημαντικό πρόσθετο ανθρώπινο δυναμικό.

Προκειμένου να υπονομεύσει αποτελεσματικά τους επιχειρησιακούς στόχους του ισραηλινού στρατού, η Χεζμπολάχ είναι πιθανό να εντείνει τον πόλεμο με μη επανδρωμένα αεροσκάφη και να χρησιμοποιήσει διάφορους τύπους UAVs –συμπεριλαμβανομένων των σταθερών πτερύγων, των multi-rotor UAVs, των περιπλανώμενων πυρομαχικών και των first-person-view αναγνωρίσεως UAVs– ως πολλαπλασιαστές ισχύος εναντίον των ανώτερων ισραηλινών δυνάμεων.

Τον Ιούλιο του 2006, η Χεζμπολάχ κατόρθωσε να υποκλέψει και να αποκρυπτογραφήσει τις βιντεοσκοπήσεις και τις επικοινωνίες των ισραηλινών μη επανδρωμένων αεροσκαφών χρησιμοποιώντας έναν συνδυασμό τεχνικών ηλεκτρονικού πολέμου, κατασκοπείας σημάτων και επίγειων υποκλοπών. Η διείσδυση αυτή τους επέτρεψε να αποκτήσουν πληροφορίες σε πραγματικό χρόνο για τα επιχειρησιακά σχέδια και τις κινήσεις των μονάδων του ισραηλινού στρατού στο νότιο Λίβανο. Η Χεζμπολάχ δεν διέκοψε τις μεταδόσεις πληροφοριών των ισραηλινών κατασκοπευτικών αεροσκαφών. Αντ' αυτού, οι μονάδες της κατασκόπευαν τους «ιπτάμενους κατασκόπους» - τα μη επανδρωμένα αεροσκάφη επιτήρησης του ισραηλινού στρατού. Εντοπίζοντας τις στοχευμένες τοποθεσίες, οι μονάδες μάχης της Χεζμπολάχ προετοίμαζαν ενέδρες για τις μονάδες εφόδου του ισραηλινού στρατού.

Οι μαχητές της Χεζμπολάχ ναρκοθέτησαν και παγίδευσαν ορισμένες από τις στοχευμένες τοποθεσίες, ενώ οι ομάδες αντιαρματιστών της οργάνωσης ήταν έτοιμες τόσο με αντιαρματικούς κατευθυνόμενους πυραύλους όσο και με μη κατευθυνόμενους πυραύλους. Όλες αυτές οι προετοιμασίες βασίστηκαν σε κινήσεις σε πραγματικό χρόνο που φαίνονταν στις μεταδόσεις των μη επανδρωμένων αεροσκαφών. Επιπλέον, η Χεζμπολάχ επανατοποθέτησε τις δυνάμεις της με σκοπό την μεγαλύτερη αντοχή στις ισραηλινές επιθέσεις, με αποτέλεσμα την αύξηση της ανθεκτικότητας της. Επιπλέον, αναδιοργάνωσε τα έμμεσα πυρά της, όπως το πυραυλικό πυροβολικό και τους όλμους, για μεγαλύτερη ακρίβεια γνωρίζοντας τις θέσεις και τις κινήσεις των μονάδων του ισραηλινού στρατού. Συνολικά, το 2006, η Χεζμπολάχ εκτέλεσε μια επιχείρηση άξια ακαδημαϊκής μελέτης που αφαίμαξε τον ισραηλινό στρατό κυρίως εξαιτίας των θανατηφόρων ενεδρών που υλοποίησε.

Εικόνα 2: Κυριότερα μη επανδρωμένα αεροσκάφη της Χεζμπολάχ
Πηγή: https://jinsa.org/wp-content/uploads/2024/07/Hezbollahs-New-Drone-Threats-to-Israel-7-2-24-5.pdf

Η σημερινή Χεζμπολάχ δεν είναι η ίδια δύναμη του 2006. Οι σύγχρονες στρατιωτικές δυνατότητες της οργάνωσης είναι ανώτερες από τη συντριπτική πλειοψηφία των μη κρατικών δυνάμεων και από τις χερσαίες δυνάμεις αρκετών μικρών κρατών. Οι χερσαίες δυνάμεις εξακολουθούν να διαδραματίζουν κυρίαρχο ρόλο στις στρατιωτικές δυνατότητες της Χεζμπολάχ. Περιλαμβάνουν διάφορους τύπους πεζικού, ειδικές δυνάμεις, τεθωρακισμένα, πυροβολικό και επίγεια αεράμυνα. Η επιχειρησιακή ετοιμότητα της Χεζμπολάχ αναδείχθηκε ακόμη περισσότερο από τις ομάδες πεζικού κατά τεθωρακισμένων το 2006. Αυτές οι ομάδες προκάλεσαν το μεγαλύτερο ποσοστό των ισραηλινών θανάτων στο Λίβανο σε σύγκριση με άλλες μονάδες και κλάδους, συμπεριλαμβανομένων των πυραύλων και όλμων, των αυτοσχέδιων εκρηκτικών μηχανισμών, των ελεύθερων σκοπευτών, ακόμη και σε σύγκριση με τα ισραηλινά φίλια πυρά, τα οποία είχαν ως αποτέλεσμα περίπου το 12% των θανάτων του ισραηλινού στρατού.

Η οργάνωση είναι επίσης ικανή στον ηλεκτρονικό πόλεμο, τον κυβερνοχώρο και τους τομείς των πληροφοριών, αλλά είναι αδύναμη ως ναυτική δύναμη. Οι ικανότητες της στις εναέριες επιχειρήσεις εξελίσσονται σταθερά, αλλά με συμβατικό τρόπο. Το 2006, τα έμμεσα πυρά από ρουκέτες και πυραύλους οδήγησαν σε περισσότερες απώλειες αμάχων στο Ισραήλ από ό,τι στρατιωτικές απώλειες στο Λίβανο, κυρίως λόγω έλλειψης ακρίβειας όσον αφορά την προσβολή των στόχων. Το 2024 το επίπεδο ακρίβειας (καθώς και οι εμβέλειες και τα ωφέλιμα φορτία) έχει αλλάξει σημαντικά. Αυτό οφείλεται εν μέρει στην μη επανδρωμένη αεροπορία της Χεζμπολάχ. Αν και η Χεζμπολάχ είχε ιστορικό βασικής χρήσης UAV ακόμη και πριν από τον πόλεμο του 2006, η οργάνωση έχει επιδείξει μια σχετικά νέα ικανότητα το 2024: μπορεί να «βλέπει» βαθιά μέσα στο Ισραήλ. Το «βλέπει» στη στρατιωτική ορολογία μεταφράζεται σε «πληροφορίες , επιτήρηση και αναγνώριση» (Intelligence, Surveillance, Reconnaissance, ISR).

Η Χεζμπολάχ εκτέλεσε με επιτυχία πολλαπλές παραβιάσεις του εναέριου χώρου, όπου στρατιωτικού επιπέδου UAV διείσδυσαν

βαθιά στον ισραηλινό εναέριο χώρο για να συλλέξουν πληροφορίες και να εκτελέσουν επιχειρήσεις επιτήρησης και αναγνώρισης [2]. Οι στοχοποιημένες τοποθεσίες περιελάμβαναν την καλά αμυνόμενη αεροπορική βάση Ramat David [3] και μια ισραηλινή ναυτική βάση στη Χάιφα, καθώς και αρκετά πολεμικά πλοία και υποδομές της μονάδας υποβρυχίων του ισραηλινού πολεμικού ναυτικού, Shayetet 7 [4]. Οι επιχειρήσεις αυτές κατέδειξαν την ικανότητα της Χεζμπολάχ να διεξάγει εξ αποστάσεως επιτήρηση πάνω από ισραηλινές αεροπορικές και ναυτικές βάσεις, καθώς και αστικά κέντρα, ή –όταν ξεσπάσει πόλεμος– αυτά τα UAVs να είναι σε θέση να διαβιβάσουν πιθανότατα τις συντεταγμένες της θέσης των στόχων τους σε συστοιχίες πυραύλων, μονάδες πυραύλων, UAV μάχης και/ή πυρομαχικά διασποράς (drones μονής κατεύθυνσης ή «αυτοκτονίας») για πλήγματα ακριβείας.

Κατά κάποιον τρόπο, αυτό μιμείται τις ενέργειες των ρωσικών UAV ISR Orlan-10 και των πυρομαχικών διασποράς Lancet στην Ουκρανία. Ο συντονισμός μεταξύ των ρωσικών UAV ISR και των UAV μάχης και των πυραυλικών μονάδων της Ρωσίας μάλλον είχε ως αποτέλεσμα την καταστροφή δύο συστοιχιών εκτοξευτών Patriot της Ουκρανίας –ένα από τα πιο ικανά και ακριβότερα συστήματα αεράμυνας στον κόσμο– από τις ρωσικές δυνάμεις κατοχής στην Ουκρανία [5].

Κατά έναν ειρωνικό τρόπο, η Χεζμπολάχ μπορεί να ακολουθεί ένα παλιό αγγλοαμερικανικό στρατιωτικό ρητό: «Αν μπορεί να φανεί, μπορεί να χτυπηθεί. Αν μπορεί να χτυπηθεί, μπορεί να σκοτωθεί». Το πρόβλημα της Χεζμπολάχ με το τυφλό πυραυλικό πυροβολικό και τα ανακριβή έμμεσα πυρά εξαλείφεται εν μέρει λόγω των UAV. Η οργάνωση πραγματοποίησε απομακρυσμένα πλήγματα βαθιά μέσα στο Ισραήλ, πιο πρόσφατα τον Αύγουστο του 2024 [6] . Πολλαπλά μη επανδρωμένα αεροσκάφη κατάφεραν να διεισδύσουν στο βόρειο Ισραήλ, με αποτέλεσμα τον τραυματισμό ισραηλινών στρατιωτών και αμάχων. Οι επιθέσεις υπογράμμισαν τη διττή χρήση του στόλου μη επανδρωμένων αεροσκαφών της Χεζμπολάχ τόσο για επιχειρήσεις επιτήρησης όσο και για επιχειρήσεις κρούσης.

Εικόνα 3: Κυριότερα μη επαδρωμένα αεροοσκάφη του Ισραήλ.
Πηγή: https://drones.rusi.org/countries/israel/

Σε γενικές γραμμές, οι επιπτώσεις των UAV στον πόλεμο εξακολουθούν να συζητούνται έντονα μεταξύ των στρατιωτικών εμπειρογνωμόνων και των ειδικών σε θέματα ασφάλειας. Παρόλα αυτά, τόσο για τη Χεζμπολάχ όσο και για τον ισραηλινό στρατό, τα μη επανδρωμένα αεροσκάφη θα ασκήσουν σημαντικό ρόλο και πιθανώς επιχειρησιακές επιπτώσεις στην πιθανή σύγκρουση. Πάντως, παρότι τα μη επανδρωμένα αεροσκάφη –ανεξάρτητα από τους τύπους τους– δεν αποτελούν στρατηγική κατηγορία οπλικών συστημάτων και έτσι είναι απίθανο να κρίνουν την έκβαση του πολέμου. Ακόμη και στο επιχειρησιακό επίπεδο του πολέμου, η Χεζμπολάχ αντιμετωπίζει προκλήσεις στην ανάπτυξη, διάρθρωση και χρήση της μη επανδρωμένης αεροπορικής της δύναμης.

Επί του παρόντος, η οργάνωση δεν μπορεί να παρατάξει και να διατηρήσει τα μεγάλα σμήνη UAV που είναι απαραίτητα για την επίτευξη αεροπορικής υπεροχής κάτω από τα 3.000 πόδια και επομένως να πραγματοποιήσει σημαντικές αεροπορικές επιθέσεις. Με τα σμήνη UAV, η Χεζμπολάχ θα μπορούσε να αντιμετωπίσει τις παρεμβολές συχνότητας, τον ηλεκτρονικό πόλεμο και τις προηγμένες ηλεκτρονικές επιθέσεις του Ισραήλ. Χωρίς τα σμήνη UAV και τα πλεονεκτήματα τους, η αποτελεσματικότητα της Χεζμπολάχ στον εναέριο τομέα μπορεί να παραμείνει περιορισμένη, ιδίως σε σύγκριση με τις αντιαρματικές ομάδες πεζικού της ή ακόμη και με το μη κατευθυνόμενο πυραυλικό πυροβολικό της. Αυτό ισχύει ακόμη και με την ανάπτυξη στρατιωτικών πυρομαχικών διασποράς όταν η οργάνωση επιχειρεί σε μικρούς αριθμούς.

Παρ' όλα αυτά, οι δυνατότητες της Χεζμπολάχ στα UAV εξελίσσονται. Επί του παρόντος, τα UAV έχουν ήδη παράσχει στη Χεζμπολάχ πρωτοφανείς δυνατότητες αθόρυβης αναγνώρισης, ανώτερες από αυτές του Ισραήλ και ενισχυμένη αδιάλειπτη στόχευση ακριβείας. Αυτό αντιπροσωπεύει μια αξιοσημείωτη πρόοδο, η οποία θεωρούνταν αδύνατη μόλις πριν από μερικές δεκαετίες. Η εξέλιξη του πολέμου με μη επανδρωμένα αεροσκάφη είναι συνεχής και απέχει πολύ από το να τελειώσει. Καθώς η Χεζμπολάχ συνεχίζει να βελτιώνει και να επεκτείνει το οπλοστάσιό της με UAV, αυτά τα μη επανδρωμένα αεροσκάφη θα μπορούσαν να γίνουν μια υπολογίσιμη δύναμη στον εναέριο χώρο.

Ως εκ τούτου, δεδομένων των παραπάνω, είναι πιθανό να βρισκόμαστε προ των πυλών μιας αλλαγής δόγματος όσον αφορά τις μάχες αέρος-εδάφους στον σύγχρονο πόλεμο, μία εξέλιξη που η χώρα μας οφείλει να λάβει πολύ σοβαρά υπόψη προκειμένου να μην την προλάβουν οι εξελίξεις. Η χρήση UAVs κατά τη διεξαγωγή στρατιωτικών επιχειρήσεων αυξάνει κατακόρυφα όχι μόνο τα ποσοστά επιτυχίας προσβολής εχθρικών στόχων, αλλά και –μέσω της παροχής πληροφοριών– την επιβιωσιμότητα των φίλιων μέσων αυξάνοντας την ανθεκτικότητα αυτών. Μέσω επομένως της ενίσχυσης της στρατιωτικής ασφάλειας, ενισχύεται και η εθνική ασφάλεια. Σε περιφερειακό δε επίπεδο η εν λόγω αλλαγή ενδέχεται να συμβάλλει στην ευκολότερη εμπλοκή λοιπών δρώντων, καθώς μειώνει κατά πολύ τόσο το οικονομικό όσο και το πολιτικό (μηδενικές απώλειες προσωπικού) κόστος, με αποτέλεσμα η περιφερειακή ασφάλεια να απειλείται πολύ περισσότερο σε σχέση με το παρελθόν.

Βιβλιογραφία

[1] Cordesman, Anthony H., George Sullivan, and William D. Sullivan. "Lessons of the 2006 Israeli-Hezbollah War." CSIS. https://www.csis.org/analysis/lessons-2006-israeli-hezbollah-war.
[2] HOROVITZ, DAVID. "Waiting for the Drones and the Missiles, at the Opening of a Regional Conflict | The Times of Israel." The Times of Israel, 14 Απριλίου 2024. https://www.timesofisrael.com/waiting-for-the-rockets-at-the-opening-of-a-regional-conflict/.
[3] FABIAN, EMANUEL. "Hezbollah Publishes Drone Footage of Ramat David Airbase in North | The Times of Israel." The Times of Israel, 24 Ιουλίου 2024. https://www.timesofisrael.com/hezbollah-publishes-drone-footage-of-ramat-david-airbase-in-north/.
[4] FABIAN, EMANUEL. "In Open Threat, Hezbollah Publishes Drone Footage of Sites in Northern Israel | The Times of Israel." The Times of Israel, 18 Ιουνίου 2024. https://www.timesofisrael.com/in-open-threat-hezbollah-publishes-drone-footage-of-sites-in-northern-israel/.
[5] "Russia Claims Strikes on Two Ukrainian Patriot Systems That Kyiv Says Were Decoys | Reuters." Reuters, 7 Ιουλίου 2024. https://www.reuters.com/world/europe/russian-iskanders-destroy-two-patriot-launchers-ukraine-russian-agencies-report-2024-07-07/.
[6] FABIAN, EMANUEL. "Two IDF Soldiers Moderately Wounded in Hezbollah Drone Attack on North | The Times of Israel." The Times of Israel, 5 Αυγούστου 2024. https://www.timesofisrael.com/two-idf-soldiers-moderately-wounded-in-hezbollah-drone-attack-on-north/.

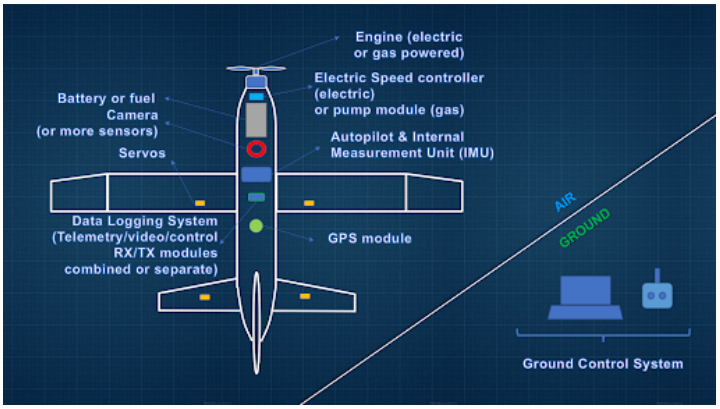
Διδάγματα της χρήσης χαμηλού κόστους και διαστάσεων μη επανδρωμένων συστημάτων (ΣμηΕΑ) υπό το πρίσμα της ανθεκτικότητας στο σύγχρονο πεδίο επιχειρήσεων

Ελευθέριος Καρατζάς
Αξιωματικός Ε.Σ. (OF-1), Ερευνητής του Διακλαδικού Κέντρου Έρευνας/Τεχνολογικής Ανάπτυξης και Καινοτομίας (ΚΕΤΑΚ)
Eleftherios Karatzas | LinkedIn

Περίληψη

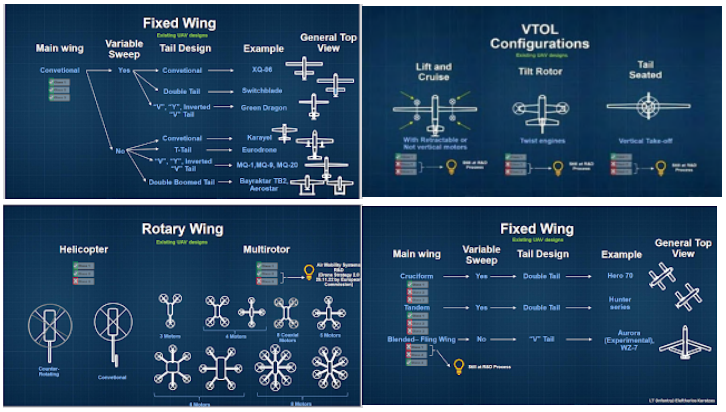
Το άρθρο πραγματεύεται τον τρόπο που τα ΣμηΕΑ αυτής της κατηγορίας έχουν κυριαρχήσει στο σύγχρονο πολυχωρικό πεδίο επιχειρήσεων, καθώς και τους λόγους που οδήγησαν στην εκτεταμένη χρήση τους. Ο αναγνώστης διαβάζοντας το παρακάτω άρθρο θα είναι σε θέση, εάν το επιθυμεί, να συνεχίσει την έρευνά του σε άλλα πεδία ενδιαφέροντος (policy, technical).

Σε μία περίοδο τεχνολογικής άνθισης των ρομποτικών εφαρμογών και δη των μη επανδρωμένων συστημάτων (Unmanned Systems), αυτά δεν γίνεται να μην επηρεάσουν τον τρόπο διεξαγωγής και σχεδίασης επιχειρήσεων στο νέο, σύγχρονο πολυχωρικό επιχειρησιακό περιβάλλον. Τα διδάγματα από την χρήση τους στον 20ο αιώνα, σε συνδυασμό με την εν παραλλήλω εξέλιξή τους με τα αντίστοιχα επανδρωμένα, μπορούν να θεωρηθούν ως προπομπός της σημερινής εκτεταμένης, άνευ ελέγχου εξάπλωσης αυτών, σε σημείο όπου απόψεις περί μερικής ή ολικής αντικατάστασης του ανθρώπινου παράγοντα στο εγγύς μέλλον, έχουν αρχίσει να παρουσιάζονται μεταξύ των αμυντικών, βιομηχανικών και ακαδημαϊκών κύκλων. Η μελέτη των παρουσών όμως εξελίξεων αποδίδουν μία διαφορετική εικόνα από την εκτιμητέα, η οποία τονίζει ότι **το επίπεδο τεχνολογικής ωριμότητας, ιδιαίτερα στα μικρά (σε διαστάσεις και βάρη) συστήματα, δεν μπορεί να απορρίψει την άμεση εξάρτηση του συστήματος από τον χειριστή (operator) και το λοιπό προσωπικό που απαιτείται**. Το παρακάτω άρθρο, θα παρουσιάσει στον αναγνώστη μία προσέγγιση για τα αυτόνομα συστήματα χαμηλού κόστους προκειμένου να κατανοήσει τις δυνατότητες αυτών και το πώς αυτές διαμορφώνουν τον υφιστάμενο σχεδιασμό σε εθνικό και συμμαχικό επίπεδο.



Βασική αρχιτεκτονική ΣμηΕΑ
(Καρατζάς Ελευθέριος)

Η παρουσία διαφόρων σχεδιασμών και κατασκευών μικρών έναντι μεγάλων μη επανδρωμένων συστημάτων είναι πραγματικότητα και το κόστος δεν αποτελεί μοναδικό παράγοντα αλλά απαιτούμενο. Η σχέση αυτή λοιπόν, σε συνδυασμό με την ανάγκη χρήσης υλικοτεχνικού (hardware) και λογισμικού (software) με ή χωρίς εν δυνάμει περιορισμούς σε μεγάλες ποσότητες στην διάρκεια του χρόνου, δίνει στον ενδιαφερόμενο **δύο πιθανούς τρόπους ενεργείας**. Ο πρώτος, κυρίως αναγκαίος σε αμυντικές εφαρμογές, είναι η χρήση υποσυστημάτων στρατιωτικών προδιαγραφών (mil-spec), ενώ ο δεύτερος η χρήση εμπορικά διαθέσιμων υλικών (commerce of the self). Η πρώτη περίπτωση, δίνει πρόσβαση στην πλέον καινοτόμο τεχνολογία (disruptive technologies), συνήθως εμπορικά μη διαθέσιμη, με το κόστος της περιορισμένης ή και μηδενικής επέμβασης στον κώδικα και την αρχιτεκτονική αυτού, καθώς και του υψηλού οικονομικού αντιτίμου. Επιπρόσθετα, οι πιθανές κυρώσεις κρατών κάτω από το πλαίσιο εθνικών και συμμαχικών στρατηγικών έχουν ως αποτέλεσμα τον αποκλεισμό (embargo) αυτών των συστημάτων ανεξαρτήτως πιθανώς επιβληθεισών περιορισμών χρήσης υλικοτεχνικού εξοπλισμού από τρίτους, και συνεπώς στην πιθανή ή ολική παύση της παραγωγής και χρήσης ή και τροποποίησης του εν λόγω συστήματος. Συνεπώς, οι παραπάνω παράγοντες οδηγούν στην εναλλακτική οδό των εμπορικά διαθέσιμων τεχνολογιών.



Σχεδιαστικές τάσεις ΣμηΕΑ
(Καρατζάς Ελευθέριος)

Θα λέγαμε πως η μετάπτωση αυτή, εμφανίστηκε κυρίως κατά τη δεύτερη δεκαετία του 21ου αιώνα, καθώς τεχνολογίες όπως η μονάδα αυτομάτου πιλότου (autopilot) και Global Positioning System (GPS) έχουν γίνει διαθέσιμες εμπορικά, σε έναν τομέα, που μέχρι τότε αποτελούσε μία πολύ ιδιαίτερη και εξειδικευμένη ασχολία, τον αερομοντελισμό. Η έλευση αυτών, έκανε ακόμη και τα πιο δύσκολα τηλεκατευθυνόμενα μοντέλα, όπως τα ακροβατικά σταθερής πτέρυγας, να χειρίζονται με μεγαλύτερη άνεση και να εκτελούν αυτόνομες ή ημιαυτόματες αποστολές. Παράλληλα, η χρήση συνθέτων υλικών και 3D εκτυπωτών, σε συνδυασμό με τους χαμηλού κόστους ηλεκτροκινητήρες, δίνουν την δυνατότητα εμφάνισης μίας νέας μορφής ιπτάμενου μέσου, το οποίο σε επανδρωμένη μορφή είχε εμφανιστεί ήδη από την δεκαετία του 1960, τα πολυκόπτερα (multirotors) περιστρεφόμενης πτέρυγας. Τα παραπάνω επέφεραν **δύο κατευθύνσεις ανάπτυξης**. Πρώτον, την εμφάνιση εταιριών κατασκευής drone να επενδύουν σε αυτά τα μοντέλα, παρέχοντας ένα ιπτάμενο μέσο, το οποίο είναι φιλικό στον χρήστη, με λιγότερους περιορισμούς σε σχέση με αντίστοιχα σταθερής πτέρυγας. Έπειτα, η φιλοσοφία των αυτοσχέδιων (custom), μετατρέπει τον χειριστή σε κατασκευαστή αυτόνομων αεροχημάτων σταθερών ή και περιστρεφόμενων πτερύγων. Σε κάθε περίπτωση βλέπουμε τη δημιουργία του, γνωστού σήμερα, Συστήματος μη Επανδρωμένου Αεροχήματος (ΣμηΕΑ) καθώς το ίδιο το ιπτάμενο μη επανδρωμένο μέσο (unmanned vehicle) παύει να ακολουθεί τη φιλοσοφία του τηλεκατευθυνόμενου (remote piloted).

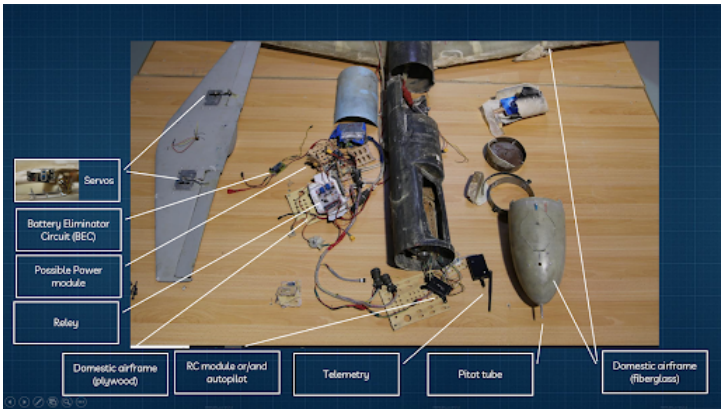
Αυτό θα οδηγήσει και στην άμετρη ανάπτυξη αυτών από κρατικούς και μη δρώντες. Το πολύ χαμηλό κόστος και η προμήθεια υποσυστημάτων από την παγκόσμια αγορά, κυρίως ασιατική, επιτρέπει την έρευνα, ανάπτυξη και παραγωγή αυτοσχέδιων ΣμηΕΑ που δεν εμπίπτουν στους περιορισμούς των έτοιμων προς πτήση (RTF-Ready To Flight), όπως η απαγόρευση πτήσης σε συγκεκριμένες περιοχές (γεωπεριφράξεις – Geofrences). Ένα χαρακτηριστικό παράδειγμα, δεν είναι άλλο από τα αυτοσχέδια FPV (first person view) τετρακόπτερα, που χρησιμοποιούνται κατά κόρον στην Ρωσο-Ουκρανική σύγκρουση λόγω της μεγάλης ταχύτητας που μπορούν να αναπτύξουν, αλλά και τη δυνατότητα πτήσης χωρίς GPS. Ωστόσο αντίστοιχες τεχνικές έχουν ήδη εφαρμοστεί στη Συρία και σε άλλες ένοπλες συγκρούσεις στη Μέση Ανατολή. Οι **κύριες αποστολές** κατά τις οποίες τα ΣμηΕΑ εντάχθηκαν σε επιχειρήσεις, δεν είναι άλλες από την αναγνώριση, τη συλλογή πληροφοριών, την παρατήρηση και την προσβολή στόχων. Στην πραγματικότητα, το κενό της εγγύς αεροπορικής υποστήριξης καλύπτεται από πλατφόρμες με κόστος μερικών εκατοντάδων ευρώ.

Κατηγοροιοποίηση ΣμηΕΑ βάσει NATO

Class & Weight (kg)	Category	Normal Employment	Normal Operating Altitude, h(ft)	Normal Mission Radius	Primary Supported Commander	Example Platform
Class I, w<150 kg	Small, 150>w>20 kg	Tactical Unit (employs launch system)	h =< 5000 AGL	50 (LOS)	Battalion, Regiment	Luna, Hermes 90
	Mini, 2=<w=<20 kg	Tactical Unit (manual launch)	h =< 3000 AGL	25 (LOS)	Company, Platoon, Squad	Scan Eagle, Skylark, Raven, DH3, Aladin, Strix
	Micro < 2 kg	Tactical Patrol/Section, individual (single operator)	h =< 200 AGL	5 (LOS)	Platoon, Squad	Black Widow
Class II, 150=<w=<600	Tactical	Tactical Formation	h =< 10000 AGL	200 (LOS)	Division, Brigade	Sperwer, Iview 250, Hermes 450, Aerostar, Range
Class III, w>600	Strike/Combat	Strategic/National	h =< 65000 MSL	Unlimited (BVLOS)	Theater	Loyal Wingman
	HALE	Strategic/National	h =< 65000 MSL	Unlimited (BVLOS)	Theater	Global Hawk
	MALE	Operational/Theater	h =< 45000 MSL	Unlimited (BVLOS)	Joint Task Force	Predator A, Predator B, Heron, Heron TP, Hermes 900

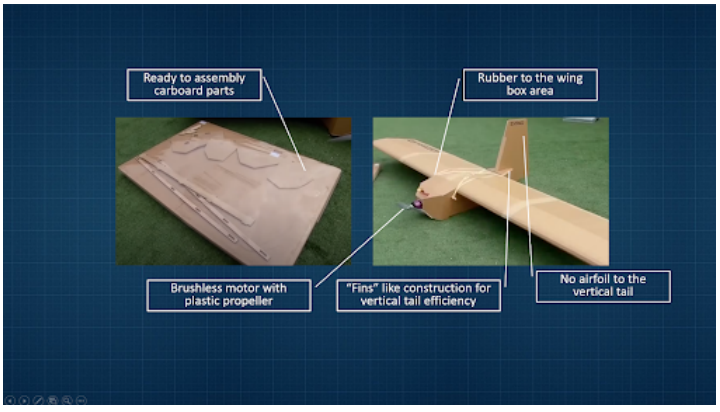
Ως επακόλουθο, η σταδιακή ένταξή τους στο πεδίο επιχειρήσεων, ανέδειξε την αδυναμία αναχαίτισης αυτών από τα υφιστάμενα αντιαεροπορικά συστήματα. Ιδιαίτερα, **οι πολύ μικρές πλατφόρμες αποτελούν την μεγαλύτερη απειλή**. Σε αυτή την κατηγορία, παρατηρούμε τις παρακάτω σχεδιαστικές τάσεις: ηλεκτροκινητήρες

με χρήση έλικας, μπαταρίες λιθίου υψηλής ενεργειακής πυκνότητας και ρυθμού αποφόρτισης, χρήση χαμηλού κόστους αυτομάτων πιλότων και χρήση διαφορετικών συχνοτήτων για μεταφορά εικόνας, χειρισμού και στοιχείων πτήσης (MHz – Ghz). Μεγάλο ρόλο ακόμη διαδραματίζει η χρήση των μέσων κοινωνικής δικτύωσης, για την ανταλλαγή πληροφοριών και τεχνικών επιχειρησιακής αξιοποίησης και συναρμολόγησης – κατασκευής αυτών.



Ανακτημένο ΣμηΕΑ των Χούθι από τα HAE (https://storymaps.arcgis.com/stories/46283842630243379f0504ece90a821f/print)

Πράγματι, οι χειρότεροι φόβοι έγιναν πραγματικότητα, όπως αποδεικνύεται από την **εκτεταμένη χρήση σε Ουκρανία, Υεμένη και Λωρίδα της Γάζας**. Δεν πρέπει ωστόσο να μας εκπλήσσει αυτή η πραγματικότητα, αν αναλογιστούμε τις ένοπλες συγκρούσεις των προηγούμενων ετών σε Συρία, Ναγκόρνο – Καραμπάχ και Λιβύη. Η άνθιση των μικρών δε ΣμηΕΑ ανέδειξε χώρες όπως το Ιράν και Κίνα ως κύριους μέτοχους σε αυτή την κούρσα κυριαρχίας στον τομέα των αυτόνομων συστημάτων. Τα παραπάνω λοιπόν συντελούν στην ανακατανομή δυνάμεων στο νέο σύγχρονο πολυχωρικό, όπως τονίστηκε στην εισαγωγή, επιχειρησιακό περιβάλλον. Επιπρόσθετα, τα όρια μεταξύ πολιτικών και στρατιωτικών συστημάτων πλέον είναι αμφιλεγόμενα, δεδομένου του τρόπου χρησιμοποιήσεώς τους. Αυτό που πρέπει να τονιστεί ωστόσο, είναι ότι **ο χειριστής δεν αντικαθίσταται ακόμη και αν το ΣμηΕΑ μπορεί να εκτελέσει αυτόνομη αποστολή**, σε σημείο που ο ίδιος μπορεί να αποτελέσει στόχος. Παράδειγμα αυτού δεν είναι άλλο από το C-UAS Aeroscope της DJI, που χρησιμοποιήθηκε επανειλημμένα στην Ουκρανία.



ΣμηΕΑ αυτοκτονίας που χρησιμοποιείται στον Ρωσο-Ουκρανικό πόλεμο κατασκευασμένο από σκληρό χαρτόνι (https://www.atlanticcouncil.org/blogs/new-atlanticist/ukraines-drone-strikes-are-a-window-into-the-future-of-warfare/)

Τα παραπάνω, αναμφίβολα έκρουσαν τον κώδωνα του κινδύνου σε Εθνικό, Νατοϊκό και Ευρωπαϊκό επίπεδο. **Εντός των καινοτόμων τεχνολογιών που παρουσιάζει η Ευρωπαϊκή Υπηρεσία Άμυνας (European Defence Agency – EDA) τονίζεται τόσο η σημασία ανάπτυξης αυτόνομων συστημάτων όσο και δυνατοτήτων αντιμετώπισης (Counter UAS – CUAS) αυτών, ιδιαιτέρως των μικρών σε διαστάσεις**. Επιπρόσθετα, το ΝΑΤΟ εξέδωσε προσφάτως οδηγίες και προτάσεις περί τεχνολογιών και τακτικών C-UAS. Η παραπάνω κατεύθυνση επιβεβαιώνεται και από τα προϊόντα που παρουσιάζονται σε εγχώριες διεθνείς εκθέσεις όπως η DEFEA που διεξήχθησαν το 2021 και 2023.

Η αναφορά της EDA ως προς τα προγράμματα UAS (https://eda.europa.eu/uas)

Η επικράτηση των μικρών ΣμηΕΑ είναι πλέον δεδομένη, καθώς ένα σύστημα ανοιχτού βρόγχου δέχεται συνεχώς ανατροφοδότηση, υπό τη μορφή νέων τεχνολογιών, τακτικών και γραμμών υποστήριξης. Ως επακόλουθο, η αλλαγή της ισορροπίας δυνάμεων είναι αναπόφευκτη. Συνεπώς είναι η κατάλληλη στιγμή να αναληφθεί δράση σε αυτό το πεδίο, όχι μόνο σε ερευνητικό επίπεδο, υπό την μορφή δοκιμαστικού πρωτοτύπου, αλλά και σε βιομηχανική παραγωγή. **Αυτό προϋποθέτει φυσικά την εκτενή μελέτη των διδαγμάτων του σήμερα, αλλά και των τακτικών του παρελθόντος** που τείνουν να επαναληφθούν με την χρήση νέων συστημάτων, κάτι που το συναντάμε στο βιβλίο του Κλαούζεβιτς, «Περί πολέμου» ως φύση και χαρακτηριστικά αυτού.

Πως όμως τα νέα συστήματα θα συμβάλλουν στην επαύξηση της ανθεκτικότητας όχι μόνο του μέσου, αλλά και του ίδιου του δρώντα που το επιχειρεί; **Η απάντηση κρύβεται πίσω από την αρχιτεκτονική του ίδιου του συστήματος**. Ο εντοπισμός ενός τόσων μικρών διαστάσεων ΣμηΕΑ, καθίσταται δυνατός από τις εκπομπές και όχι από την ραδιοτομή (radio cross section) αυτού. Ιδιαίτερα, το στίγμα GPS είναι αυτό που συνήθως προδίδει όχι μόνο το ιπτάμενο μέσο αλλά και τον χειριστή. Για αυτό και βλέπουμε στα υφιστάμενα πεδία μαχών, ιδιαίτερα της Ουκρανίας, να **χρησιμοποιούνται έτοιμα προς πτήση (ready to fly), εμπορικά διαθέσιμα ΣμηΕΑ μαζί με αυτοσχέδια (custom) χωρίς GPS σαν ζεύγος**. Η μέθοδος αυτή, πέραν της ακρίβειας που προσφέρει στην προσβολή στόχων, αυξάνει και την επιβιωσιμότητα του προσωπικού. Στην πραγματικότητα, με κατάλληλη αναγνώριση εδάφους από το πρώτο, το δεύτερο μπορεί να ίπταται από τον χειριστή του στην επιθυμητή περιοχή, χωρίς την χρήση βοηθημάτων, παρά μόνο με χαρακτηριστικά σημεία του εδάφους. Θα μπορούσαμε να το παρομοιάσουμε με τον εξ όψεως κανόνων πτήσης (Visual Flight Rules) που χρησιμοποιείται στη γενική αεροπορία.

Ακόμη, νέα συστήματα έχουν αναπτυχθεί ήδη, για την **πλοήγηση με οπτική αναγνώριση** (terrain-pattern recognition) ή και ακόμη με **εσωτερικά συστήματα πλοήγησης** (internal navigation systems – INS). Αυτές οι μέθοδοι, μαζί με την **κατάλληλη χρήση του ΣμηΕΑ**

από τον χειριστή, όπως η ταχεία ανάπτυξη και ο εξειδικευμένος τρόπος πτήσης, επαυξάνουν την επιβιωσιμότητα του προσωπικού στο πεδίο. Επιπρόσθετα, η **εύρεση νέων αδιάλειπτων χαμηλού κόστους υλικών** θα επαυξήσει την εμπιστοσύνη που οι τελικοί δρώντες έχουν ως προς το σύστημα. Έτσι θα προάγεται και η συνεχής ανατροφοδότηση με νέα στοιχεία και διδάγματα που θα πρέπει να προσαρμοστούν, ώστε να αποτελούν έναν ακόμη πολλαπλασιαστή ισχύος ως προς την ανθεκτικότητα στο νέο σύγχρονο πολυχωρικό επιχειρησιακό περιβάλλον.

ΕΝΔΕΙΚΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Karatzas, E., Kostopoulos, V, & Lappas, V. (2023). Preliminary weight estimation of canister based light foldable wing electric propulsion UAV, as a platform for swarm applications. Journal of Physics: Conference Series, 2526 (2023) 012082, 1–8. https://www.doi.org/10.1088/1742-6596/2526/1/012082

Karatzas, E. (2019). ΑΝΑΠΤΥΞΗ ΜΗ ΕΠΑΝΔΡΩΜΕΝΟΥ ΑΕΡΟΧΗΜΑΤΟΣ ΜΑΧΗΣ - ΠΑΡΑΜΕΤΡΙΚΗ ΜΕΛΕΤΗ (Development of UCAV - Conceptual Study). ΔΔΜΠΣ Πολυτεχνείου Κρήτης-Στρατιωτικής Σχολής Ευελπίδων [Master Thesis]. https://www.doi.org/10.26233/heallink.tuc.83782

Karatzas, E. (2022). Η άνοδος των τουρκικής προέλευσης μη επανδρωμένων αεροσκαφών (The rise of Turkish made Unmanned Aircraft Vehicles). Η Ελλάδα, η Ευρώπη & ο Κόσμος. Τεύχος 17. https://www.researchgate.net/publication/365473051_The_rise_of_Turkish_made_Unmanned_Aircraft_Vehicles_E_anodos_ton_tourkikes_proeleuses_me_epandromenon_aeroskaphon

Development Concepts and Doctrine Centre Crown (UK), 0-30.2 (JDP 0-30.2) Unmanned Aircraft Systems. Royal Ministry of Defence (UK). 2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_dat a/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf

Mark Voskuij, Performance analysis and design of loitering munitions: A comprehensive technical survey of recent developments. Faculty of Military Sciences, Netherlands Defence Academy, Den Helder, The Netherlands. 2021.

Daniel P. Raymer, Aircraft Design: A Conceptual Approach, Sixth Edition, AIAA Education Series, 2018.

Roskam, Jan. Preliminary Sizing of Airplanes, Part I, Aviation and Engineering Corporation, 1985.

European Union External Actions, 2022. A Strategic Compass for Security And Defence. Brussels: s.n.

Ασφάλεια στο διάστημα: τα διαστημικά όπλα, το διεθνές δίκαιο και η αποτροπή πολεμικών συγκρούσεων στο διάστημα

Άγγελος Γιακουμής
Αξιωματικός ΠΑ
Μέλος ΑΛΛΗΛΟΝ
Angelos Giakoumis | LinkedIn

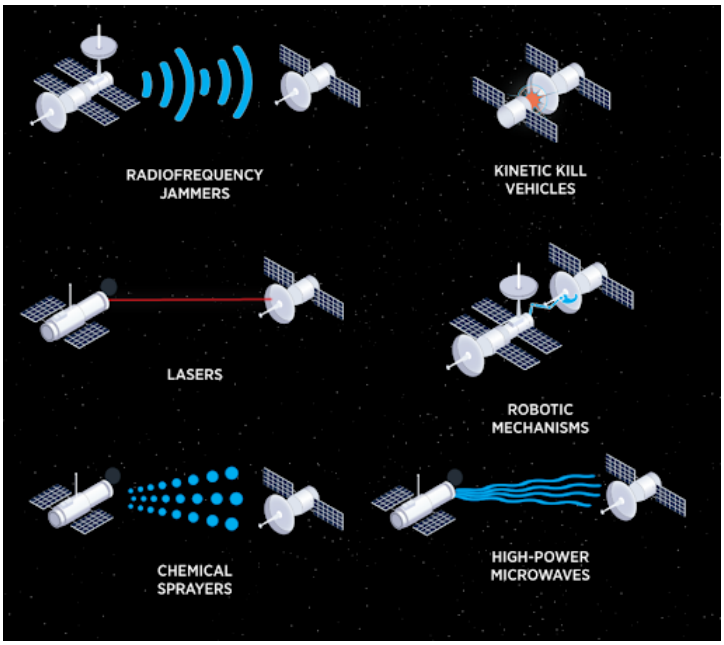
Περίληψη

Το παρόν άρθρο εξετάζει κατά πόσο το λεγόμενο "weaponization of space" και το ισχύον ρυθμιστικό πλαίσιο συμβάλλουν στην αποτροπή πολεμικών συγκρούσεων στο διάστημα και τι επιπλοκές έχουν για την ασφάλεια στο διάστημα και για την ανθεκτικότητα των διαστημικών υποδομών. Διαπιστώνεται ότι ενώ τα διαστημικά όπλα και το ισχύον ρυθμιστικό πλαίσιο έχουν αποτρέψει τις συγκρούσεις μεγάλης κλίμακας στο διάστημα και έχουν επιφέρει ένα είδος ισορροπίας, αποτυγχάνουν να εμποδίσουν τις συγκρούσεις χαμηλής έντασης, οι οποίες τα τελευταία χρόνια αυξάνονται συνεχώς. Οι συνεχιζόμενοι εξοπλισμοί στο διάστημα και οι ελλείψεις του νομικού πλαισίου, μπορούν να λειτουργήσουν αποσταθεροποιητικά και να ανατρέψουν στο μέλλον την υφιστάμενη αρχιτεκτονική ασφάλειας του διαστήματος, αν δεν ληφθούν κατάλληλα μέτρα.

Τα τελευταία χρόνια πληθαίνουν οι φωνές, ιδιαίτερα στην Δύση, υπέρ της σκοπιμότητας των εξοπλισμών στο διάστημα, του λεγόμενου "weaponization of space". Μεγάλη μερίδα αναλυτών υποστηρίζει ότι οι ΗΠΑ και οι σύμμαχοι τους θα πρέπει να εξοπλιστούν και να αναπτύξουν στρατιωτικές δυνατότητες, που θα λειτουργούν αποτρεπτικά εναντίον ενός επίδοξου αντιπάλου, λόγω του φόβου των αντιποίνων (**1**). Το ερώτημα που τίθεται είναι τι επιπλοκές μπορεί να έχει η τάση αυτή για την ασφάλεια στο διάστημα, για την ανθεκτικότητα των διαστημικών υποδομών και για την αποτροπή μιας ενδεχόμενης πολεμικής σύγκρουσης στο διάστημα. Το ζήτημα θα εξεταστεί εντός του ισχύοντος ρυθμιστικού πλαισίου και με θεωρητική αφετηρία το γεγονός ότι η σύγχρονη αρχιτεκτονική ασφάλειας του διαστήματος βασίζεται στην θεωρία της αποτροπής και στον ανταγωνισμό των δύο υπερδυνάμεων της εποχής του Ψυχρού Πολέμου, δηλαδή τις ΗΠΑ και την Σοβιετική Ένωση. Η τότε προσέγγιση για την ασφάλεια στο διάστημα, ήταν ανάλογη με το σκεπτικό της πυρηνικής αποτροπής, δηλαδή οποιαδήποτε επίθεση εναντίον εθνικών μέσων στο διάστημα, θα επέφερε τα πιο αυστηρά αντίποινα (**2**). Ωστόσο, με το πέρας των ετών η δυτική στρατηγική σκέψη μετασχηματίστηκε και άρχισε να αντιμετωπίζει το διάστημα σαν ένα ξεχωριστό επιχειρησιακό τομέα, με ιδιαίτερα χαρακτηριστικά και διαφορετικές δυναμικές. Τα μαζικά αντίποινα έδωσαν την θέση τους στην πολυστρωματική (multilayered) αποτροπή, η οποία προάγει, μεταξύ άλλων, την ενίσχυση της ανθεκτικότητας της αρχιτεκτονικής της αντιμετώπισης των επιθέσεων και την σύναψη συμμαχιών που προάγουν τις νόρμες και τις υπεύθυνες συμπεριφορές στο διάστημα. Η εν λόγω στρατηγική προσέγγιση διατηρεί σε κάθε περίπτωση, το δικαίωμα ανταπόδοσης σε περίπτωση εχθρικής επιθετικής ενέργειας (**3**).

Διαστημικά όπλα: τα είδη τους και οι επιπλοκές από ενδεχόμενη χρήση τους

Υπάρχουν διάφορα είδη διαστημικών όπλων, ανάλογα με το αν βρίσκονται στην γη ή σε τροχιά, ανάλογα με το είδος της ζημιάς που προκαλούν, με τις τεχνολογίες που ενσωματώνουν και με την ευκολία εντοπισμού τους. Για τους σκοπούς της παρούσας ανάλυσης, τα διαστημικά όπλα κατατάσσονται σε δύο βασικές κατηγορίες: στα κινητικά ή διαστημικά όπλα κινητικής ενέργειας και στα μη κινητικά. Τα πρώτα χρησιμοποιούν εκρηκτικά και τις αρχές της συμβατικής φυσικής για να καταστρέψουν τον στόχο. Οι επιθέσεις με όπλα κινητικής ενέργειας δημιουργούν μη αναστρέψιμες ζημιές, αποτελούν ηχηρό μήνυμα προβολής ισχύος και είναι εύκολο να αποδοθούν στον επιτιθέμενο. Στην κατηγορία αυτή ανήκουν τα όπλα anti-satellite (ASAT), δηλαδή όπλα που βρίσκονται σε τροχιά ή που εκτοξεύονται από επίγειους σταθμούς και έχουν στόχο να καταστρέψουν δορυφόρους που βρίσκονται σε τροχιά. Τα μη κινητικά διαστημικά όπλα προκαλούν ζημιά σε δορυφόρους και σε επίγειους σταθμούς χωρίς εκρήξεις και χωρίς να έρχονται σε επαφή μαζί τους. Σε αυτή την κατηγορία ανήκουν για παράδειγμα τα όπλα ηλεκτρομαγνητικής ακτινοβολίας, τα οποία στοχοποιούν το ηλεκτρομαγνητικό φάσμα που χρησιμοποιούν οι δορυφόροι για εκπομπή και λήψη πληροφοριών. Χρησιμοποιούν συσκευές παρεμβολής σήματος (jammers) που αυξάνουν το θόρυβο στην συχνότητα και κακόβουλες εφαρμογές (spoofers) που προσπαθούν να αποκτήσουν μόνιμη πρόσβαση σε ευαίσθητες πληροφορίες του δορυφόρου και να δώσουν ψευδείς εντολές. Οι κυβερνοεπιθέσεις από την άλλη, στοχεύουν τα συστήματα που ελέγχουν την ροή των δεδομένων (data stream) και προσπαθούν να υποκλέψουν δεδομένα ή να εισάγουν ψευδείς εντολές στο σύστημα. Τα πυρηνικά όπλα από την άλλη έχουν γνωρίσματα και των δύο παραπάνω κατηγοριών, αφού αν ενεργοποιηθούν μπορούν να καταστρέψουν τους εχθρικούς δορυφόρους που βρίσκονται εντός των ορίων της έκρηξης τους και να υποβαθμίσουν λειτουργικά τους υπόλοιπους, λόγω του περιβάλλοντος έντονης ακτινοβολίας που δημιουργούν (**4**).



Εικόνα 1: Απεικόνιση διαστημικών όπλων τύπου "space-based weapons" στην έκδοση της DIA (Defense Intelligence Agency) του 2022, με τίτλο "Challenges to Security in Space. Space Reliance in the Era of Competition".
Πηγή: https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf

Δεδομένης της πληρότητας του ρυθμιστικού πλαισίου για την χρήση πυρηνικών όπλων και της διακοπής των πυρηνικών δοκιμών στα διάστημα από το 1961 και μετά, τα πυρηνικά όπλα εξαιρούνται από την ανάλυση που ακολουθεί. Από τα κινητικά διαστημικά όπλα, τα όπλα ASAT αποτελούν την μεγαλύτερη απειλή για την ασφάλεια του διαστήματος και για την ανθεκτικότητα των διαστημικών υποδομών. Ενδεχόμενη χρήση τους σε μια υποθετική σύγκρουση, θα προκαλέσει μη αναστρέψιμες ζημιές στις διαστημικές υποδομές, θα αυξήσει τις πιθανότητες για αντίποινα και θα δημιουργήσει **διαστημικά συντρίμμια** ("space debris"), τα οποία αποτελούν απειλή για όλους τους δορυφόρους που βρίσκονται σε τροχιά. Τα space debris θα περιορίσουν την ελεύθερη πρόσβαση σε τροχιές των δορυφόρων που θα τεθούν σε τροχιά μελλοντικά και την ανεμπόδιστη κίνηση των υφιστάμενων δορυφόρων. Μπορούν να συγκρουστούν με δορυφόρους και με διαστημικούς σταθμούς σε τροχιά και να προκαλέσουν ζημιές ή ακόμα και να απειλήσουν τις ζωές των πληρωμάτων των επανδρωμένων διαστημικών αποστολών. Το 2007, η **Κίνα** πραγματοποίησε την πρώτη δοκιμή όπλου ASAT και κατέστρεψε τον δορυφόρο Fengyun-1C, προκαλώντας πάνω από 3.000 διαστημικά συντρίμμια. Ανάλογες δοκιμές έχουν πραγματοποιήσει η **Ινδία**, η **Ρωσία** και οι **ΗΠΑ**. Και τα μη κινητικά όπλα μπορεί να απειλήσουν σοβαρά την ανθεκτικότητα των διαστημικών υποδομών και την ασφάλεια. Μια **κυβερνοεπίθεση** μπορεί να προκαλέσει διακοπή των δεδομένων ενός δορυφόρου που παρέχει για παράδειγμα υπηρεσίες GPS ή επικοινωνίες, ή μπορεί να επιτρέψει στον επιτιθέμενο να αποκτήσει τον έλεγχο του δορυφόρου και να διακόψει την λειτουργία του δορυφόρου ή να του προκαλέσει ηθελημένα βλάβες. Οι κυβερνοεπιθέσεις έχουν μόνιμο ή προσωρινό χαρακτήρα και είναι πολύ δύσκολο να αποδοθούν σε κάποιον δρώντα. Τέλος, η χρήση όπλων που εκπέμπουν **ακτινοβολίες λέιζερ** ή **δέσμες μικροκυμάτων υψηλής έντασης** μπορεί να «τυφλώσουν» τους οπτικούς αισθητήρες του δορυφόρου ή να καταστρέψουν τα ηλεκτρονικά τους κυκλώματα (**5**).

Το ρυθμιστικό πλαίσιο για την χρήση του διαστήματος

Το ζήτημα της στρατιωτικοποίησης (militarization) και των εξοπλισμών στο διάστημα απασχόλησε νομικά την διεθνή κοινότητα από τα πρώτα χρόνια του αγώνα για την κατάκτηση του διαστήματος. Ωστόσο, δεδομένου ότι το διάστημα αποτέλεσε την προέκταση του ψυχροπολεμικού ανταγωνισμού μεταξύ ΗΠΑ και Σοβιετικής Ένωσης, ο καθορισμός κανόνων δικαίου για την χρήση του διαστήματος ήταν ένα ιδιαίτερα περίπλοκο ζήτημα, καθώς αποσκοπούσε πρωτίστως στην διασφάλιση των εθνικών συμφερόντων των δύο υπερδυνάμεων και λιγότερο στην παγκόσμια ασφάλεια. Οι πυρηνικές δοκιμές που εκτέλεσαν οι ΗΠΑ και η Σοβιετική Ένωση στο διάστημα στα τέλη της δεκαετίας του 1950, έδειξαν ότι η ακτινοβολία από τις πυρηνικές εκρήξεις είχε διαφορετική συμπεριφορά στο διάστημα, σε σχέση με τις πυρηνικές δοκιμές στη γη και μεγαλύτερη διάρκεια, οπότε πιθανόν να απειλούσε τις επικείμενες επανδρωμένες διαστημικές αποστολές. Αρχικά, οι δύο πλευρές συμφώνησαν αμοιβαία να αναστείλουν προσωρινά τις πυρηνικές δοκιμές. Τελικά υπέγραψαν το **1963** μαζί με το Ηνωμένο Βασίλειο, την "**Limited Nuclear Test Ban Treaty**" για την συνολική απαγόρευση των δοκιμών πυρηνικών όπλων στο διάστημα. Οι συνομιλίες συνεχίστηκαν και κατέληξαν στην υπογραφή της συνθήκης "Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies" στις αρχές του **1967**, ή απλά **"Outer Space Treaty (OST)"** (**6**). Το άρθρο IV της OST ασχολείται με την

αποστρατιωτικοποίηση του διαστήματος και ορίζει την ειρηνική χρήση του. Απαγορεύει να τεθούν σε τροχιά γύρω από την γη πυρηνικά όπλα και όπλα μαζικής καταστροφής (**7**). Το νομικό πλαίσιο συμπληρώνεται από τις υπόλοιπες διατάξεις της συνθήκης του διαστήματος αλλά και εκείνες του ευρύτερου διεθνούς δικαίου (δίκαιο του αφοπλισμού και ελέγχου των εξοπλισμών, διεθνές ανθρωπιστικό δίκαιο) που καθορίζουν την χρήση του διαστήματος για ειρηνικούς σκοπούς, απαγορεύουν την απειλή ή χρήση βίας και τη χρήση μεθόδων πολέμου που μπορούν να προκαλέσουν μακροπρόθεσμη βλάβη στο φυσικό περιβάλλον.

Οι πρακτικές των διαστημικών δρώντων και η OST

Παρά την φαινομενική πληρότητα του ρυθμιστικού πλαισίου, μια πληθώρα χωρών με δυνατότητες πρόσβασης στο διάστημα μεταξύ των οποίων συγκαταλέγεται η Ρωσία και η Κίνα, έχουν παραδεχθεί δημοσίως ότι συνεχίζουν να αναπτύσσουν όπλα για καταστροφή δορυφόρων και μέσα για παρεμβολές του συστήματος GPS των ΗΠΑ. Μέχρι σήμερα δεν έχει υπάρξει κάποια στρατιωτική σύγκρουση μεγάλης κλίμακας στο διάστημα. Ωστόσο οι κυβερνοεπιθέσεις, οι πτήσεις κατασκοπείας των αντίπαλων μέσων, οι υποκλοπές δεδομένων, οι προκλήσεις δολιοφθορών σε δορυφόρους του αντιπάλου, το jamming και το spoofing έχουν αυξηθεί ραγδαία, σε σημείο που έχουν γίνει η νέα κανονικότητα (**8**). Οι δορυφόροι αποτελούν τμήμα των κρίσιμων υποδομών των διαστημικών και όχι μόνο κρατών και σχετίζονται με την διεξαγωγή στρατιωτικών επιχειρήσεων αλλά και με ένα τεράστιο εύρος εμπορικών και οικονομικών δραστηριοτήτων. Επομένως, μια επιθετική ενέργεια εναντίον ενός δορυφόρου σε τροχιά, μπορεί πολύ εύκολα να προκαλέσει κλιμάκωση στο διάστημα ή αντίποινα σε κρίσιμες υποδομές του αντιπάλου στην γη. Φανταστείτε πόσο επικίνδυνο μπορεί να γίνει το spoofing και τι αντίδραση πιθανόν να προκαλέσει, όταν για παράδειγμα σε μια επίγεια στρατιωτική επέμβαση, τα στοιχεία θέσης και επίγνωσης κατάστασης (situational awareness) που παρέχονται δορυφορικά αλλοιωθούν, για να μην παρουσιάζουν την πραγματική εικόνα του πεδίου της μάχης σε αυτούς που πρέπει να σχεδιάσουν και να εκτελέσουν την επιχείρηση.

Εικόνα 2: Εκτόξευση βλήματος ASAT από το αμερικανικό καταδρομικό USS Lake Erie, κλάσης Ticonderoga, εναντίον του μη λειτουργικού αμερικανικού δορυφόρου USA-193, την 21 Φεβρουαρίου 2008 (Επιχείρηση Burnt Frost).
Πηγή: https://www.defense.gov/Multimedia/Photos/igphoto/2002025758/

Από την άλλη, έχουν αρχίσει να γίνονται φανερά τα όρια της OST, μετά από 57 χρόνια από την υπογραφή της. Η Συνθήκη ναι μεν απαγορεύει να τεθούν σε τροχιά πυρηνικά όπλα και όπλα μαζικής καταστροφής και τις δοκιμές όπλων, αλλά δεν ορίζει τι ακριβώς θεωρείται διαστημικό όπλο. Επίσης δεν περιλαμβάνει προβλέψεις για τα υπόλοιπα είδη συμβατικών όπλων και για τις μη κινητικές δυνατότητες που μπορεί να απειλήσουν την ορθή λειτουργία ενός δορυφόρου. Η έλλειψη ενός κοινώς αποδεκτού ορισμού του διαστημικού όπλου και των ιδιοτήτων του, καθιστά ιδιαίτερα πολύπλοκη την εκπόνηση νομοθετικών ρυθμίσεων για τον περιορισμό της εξάπλωσης του. Επίσης, η αποκλειστική αναφορά της OST σε πυρηνικά όπλα και σε όπλα μαζικής καταστροφής επιτρέπει την διασταλτική ερμηνεία του άρθρου IV από τις διαστημικές δυνάμεις, οι οποίες στο πλαίσιο της διαφύλαξης των εθνικών τους συμφερόντων στο διάστημα και της εξασφάλισης της ανθεκτικότητας των διαστημικών τους υποδομών, θεωρούν ότι μια πιθανή τοποθέτηση συμβατικών όπλων σε τροχιά δεν παραβιάζει την OST. Τέλος, το νομικό πλαίσιο συνολικά, αδυνατεί μέχρι στιγμής να ενσωματώσει προβλέψεις για τις σύγχρονες τεχνολογικές εξελίξεις στο διάστημα, αναφορικά με μέσα και δορυφόρους διττού ρόλου (dual use) που έχουν στρατιωτικές και μη στρατιωτικές εφαρμογές (**9**).

Τελικά λειτουργούν αποτρεπτικά τα διαστημικά όπλα και το ρυθμιστικό πλαίσιο;

Αναμφισβήτητα, οι εξοπλισμοί και η ανάπτυξη στρατιωτικών δυνατοτήτων βελτιώνουν την αποτρεπτική ισχύ ενός κράτους, καθώς δημιουργούν δεύτερες σκέψεις σε έναν αντίπαλο που σχεδιάζει μια επιθετική ενέργεια. Αντίστοιχα λειτουργούν και τα διαστημικά όπλα. Οποιοσδήποτε κρατικός ή μη δρώντας που δραστηριοποιείται στο διάστημα, μπορεί να αντιληφθεί τη σοβαρότητα ενός πλήγματος των διαστημικών του υποδομών από ένα όπλο ASAT και τις συνέπειες που αυτό θα έχει στην πρόσβασή του σε διαστημικές υπηρεσίες για να διεξάγει πολεμικές επιχειρήσεις ή να υποστηρίξει τις οικονομικές του δραστηριότητες. Κατά συνέπεια, αποτελούν ένα σαφές μήνυμα αποτροπής, καθώς συνιστούν ξεκάθαρη δήλωση των δυνατοτήτων και των προθέσεων για αντίποινα. Το μήνυμα δείχνει να λειτουργεί και το επιχειρησιακό πεδίο φαίνεται να βρίσκεται σε μια κατάσταση ισορροπίας, διότι παρά την ύπαρξη διαστημικών όπλων και τον έντονο ανταγωνισμό των διαστημικών κρατών, δεν έχει προκληθεί μέχρι και σήμερα κάποια στρατιωτική σύγκρουση μεγάλης κλίμακας στο διάστημα. Παρόλα αυτά, ούτε το νομοθετικό πλαίσιο, ούτε τα διαστημικά όπλα έχουν καταφέρει να εξαλείψουν πλήρως τις προκλητικές ενέργειες μικρότερης κλίμακας, τις «μη φιλικές συμπεριφορές» και τις επιθέσεις με μη κινητικά μέσα. Προκύπτει έτσι το εξής παράδοξο: ενώ τα διαστημικά όπλα και το ρυθμιστικό πλαίσιο έχουν αποτρέψει τις συγκρούσεις μεγάλης κλίμακας εδώ και 60 περίπου χρόνια, αποτυγχάνουν να αποτρέψουν τις συγκρούσεις χαμηλής έντασης, οι οποίες αυξάνονται συνεχώς τα τελευταία χρόνια. Οι συνεχιζόμενοι εξοπλισμοί και οι ελλείψεις του νομικού πλαισίου που προαναφέρθηκαν, ενδέχεται να ανατρέψουν κάποια στιγμή την υπάρχουσα ισορροπία και να απειλήσουν την ασφάλεια στο διάστημα. Κατά συνέπεια, επιβάλλεται ο εκσυγχρονισμός των υφιστάμενων

νομοθετικών διατάξεων και η θέσπιση κοινά αποδεκτών κανόνων για τον περιορισμό της εξάπλωσης και της χρήσης των διαστημικών όπλων.

Ενδεικτική Βιβλιογραφία

(1) Για την σχετική συζήτηση βλέπε ενδεικτικά Everett C. Dolman, Astropolitik: Classical Geopolitics in the Space Age, London: Frank Cass, 2002; David W. Ziegler, "Safe Heavens: Military Strategy and Space Sanctuary," in Bruce M. DeBlois, ed., Beyond the Paths of Heaven: The Emergence of Space Power Thought. The School of Advanced Airpower Studies, Maxwell AFB, Alabama.: Air University Press, September 1999.

(2) Michael Krepon. "Space Nuclear and Deterrence". In Michael Krepon and Julia Thomas eds. Anti-Satellite Weapons, Deterrence and Sino-American Space Relations. Washington DC; Stimson Center, 2013, p. 5, 26.

(3) U.S. Department of Defense. Office of the Director of National Intelligence. US National Security Space Strategy. Unclassified Summary. Washington DC. January 2011, p. 10-14; United States Space Force (USSF). Space Capstone Publication. Spacepower. Doctrine for Space Forces. June 2020, p. 19-22.

(4) Todd Harrison, Kaitlyn Johnson & Makena Young. Foreword by Doug Loverro. Defense against the dark arts in space: Protecting space systems from counterspace weapons. Washington DC: Center for Strategic and International Studies (CSIS). February 25, 2021, p. 7-9.

(5) Defense Intelligence Agency (DIA). Challenges to Security in Space. Space Reliance in the Era of Competition. Washington DC: DIA, March 2022, p. 37-39; Kari A. Bingen, Kaitlyn Johnson & Makena Young, foreword by John W. Jay Raymond. Space Threat Assessment 2023: A Report of the CSIS Aerospace Security Project. Washington DC: Center for Strategic and International Studies (CSIS). April 2023, p. 3-7; Brian Weeden. 2007 Chinese Anti-Satellite Test Fact Sheet. Secure World Foundation (SWF), updated November 23, 2010. https://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf (πρόσβαση 01 Αυγούστου 2024).

(6) Bruce McClintock, Katie Feistel, Douglas C Ligor & Kathryn O`Connor. Responsible Space Behavior for the New Space Era Preserving the Province of Humanity. Santa Monica, CA: RAND Corporation. 2021, p. 5; James Clay Moltz. The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests. Stanford, CA: Stanford University Press, 2011, p. 47.

(7) Το άρθρο IV της OST του 1967 ορίζει ότι "States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner. The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden". Βλέπε United Nations (UN) Office for Outer Space Affairs. International Space Law: United Nations Instruments. UN Office at Vienna. 2017, p. 5.

(8) Clayton Swope, Kari A. Bingen, Makena Young, Madeleine Chang, Stephanie Songer, Jeremy Tammelleo, foreword by Eric Fanning. Space Threat Assessment 2024: A Report of the CSIS Aerospace Security Project. Washington DC: Center for Strategic and International Studies (CSIS). April 2024, p. 16-19.

(9) Πρόκειται για τις λεγόμενες "dual-use" space technologies. Βλέπε ενδεικτικά Emily Taft. "Outer Space: The Final Frontier or the Final Battlefield." Duke Law and Technology Review. Vol 15, No 1. 2018. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1313&context=dltr (πρόσβαση 02 Αυγούστου 2024).

Το μέλλον της αεροδιαστημικής βιομηχανίας υπό το πρίσμα της εισαγωγής τεχνητής νοημοσύνης στην ανάπτυξη συστημάτων

Άγγελος Χωριανόπουλος
Ιδρυτής του Δικτύου Ανάλυσης Αμυντικού & Γεωπολιτικού Ρίσκου Future Warfare,
Αναλυτής Γεωπολιτικού Ρίσκου
Aggelos Chorianopoulos | LinkedIn

Περίληψη

Εν έτει 2024 η εισαγωγή τεχνητής νοημοσύνης στην πολεμική διαδικασία έχει αλλάξει τον τρόπο με τον οποίο αναλύουμε τις συγκρούσεις παγκοσμίως. Επίσης έχει αλλάξει σε βιομηχανικό και τεχνολογικό επίπεδο την συντριπτική πλειοψηφία κατασκευής σύγχρονων οπλικών συστημάτων τόσο στον τομέα της άμυνας όσο και στον τομέα της πολιτικής προστασίας. Οι μεταφορές κεφαλαίων που γίνονται από την ανάπτυξη συμβατικών οπλικών συστημάτων προς την εισαγωγή τεχνητής νοημοσύνης στην αμυντική βιομηχανία δεν έχουνε παρατηρηθεί σε κάποια άλλη περίοδο της στρατιωτικής ιστορίας. Οι αλλαγές ειδικότερα στον τομέα της αεροδιαστημικής μας αφορούν και θα μας αφορούν για τις επόμενες δεκαετίες δεδομένης της αυξανόμενης σημαντικότητας των μη επανδρωμένων εναέριων μέσων σε επιχειρήσεις πολιτικής προστασίας και στρατιωτικών εφαρμογών.

Εισαγωγή

Η τεχνητή νοημοσύνη (AI) μεταμορφώνει θεμελιωδώς τη βιομηχανία της αεροδιαστημικής,καθώς επίσης και την έννοια της άμυνας και της ασφάλειας. Αυτή η τεχνολογική επανάσταση αναδιαμορφώνει τις λειτουργίες των οπλικών συστημάτων ενισχύοντας την αποτελεσματικότητά τους στο πεδίο της μάχης. Καθώς οι αμυντικές εταιρείες αξιοποιούν την τεχνητή νοημοσύνη και τη μηχανική μάθηση για ανάπτυξη προϊόντων βλέπουμε μία ραγδαία εισαγωγή νέων εξοπλιστικών προγραμμάτων στην πολεμική διαδικασία, μεταβάλλοντας τον τρόπο με τον οποίο αναλύουμε τις συγκρούσεις διεθνώς.

Η τεχνητή νοημοσύνη ενσωματώνεται σε διάφορες πτυχές των αεροδιαστημικών και αμυντικών επιχειρήσεων, προσφέροντας καινοτόμες λύσεις που ενισχύουν τόσο την αποτελεσματικότητα των όπλων όσο και την έννοια της αποτροπής στα κράτη που τις χρησιμοποιούν. Για παράδειγμα, η Porsche Automobil Holding SE έχει αναπτύξει ένα πατενταρισμένο σύστημα που χρησιμοποιεί drones για τη φόρτιση αεροσκαφών κατά την πτήση, ενώ η BETA AIR, LLC έχει εισαγάγει μια μέθοδο μέτρησης των επιπέδων καυσίμων σε αεροσκάφη. Το δίπλωμα ευρεσιτεχνίας της Samsung Group επικεντρώνεται στη διαχείριση ενός στόλου μη επανδρωμένων εναέριων οχημάτων (UAV), βελτιώνοντας την επικοινωνία και τον ζωντανό συντονισμό (live coordination) μεταξύ των μέσων. Το δίπλωμα ευρεσιτεχνίας της Nokia Corp περιλαμβάνει τον συντονισμό των πτήσεων UAV εντός ενός εταιρικού ομίλου προσφέροντας κρυπτογραφημένα δίκτυα επικοινωνίας μεταξύ των συμμετεχόντων.

Αυτές οι εξελίξεις δεν περιορίζονται σε συγκεκριμένες εταιρείες, αλλά αντιπροσωπεύουν μια ευρύτερη τάση στον κλάδο της άμυνας. Ο ρόλος της τεχνητής νοημοσύνης στη βελτίωση των διαδικασιών λήψης αποφάσεων, στον εξορθολογισμό των λειτουργιών και στη βελτίωση των επιδόσεων καθίσταται ολοένα και πιο κρίσιμος.

Τάσεις στρατηγικών συμφωνιών και επενδύσεις στην τεχνητή νοημοσύνη

Οι βιομηχανίες αεροδιαστημικής, άμυνας και ασφάλειας δεν επικεντρώνονται μόνο στην καινοτομία αλλά και στις στρατηγικές επενδύσεις στην τεχνητή νοημοσύνη, την μηχανική νέφους και τους ημιαγωγούς. Αυτές οι επενδύσεις στοχεύουν στην εξασφάλιση προσοδοφόρων συνεργασιών και τοποθετούν τις εταιρείες στην πρώτη γραμμή των εξελίξεων της αεροδιαστημικής βιομηχανίας παγκοσμίως. Ο αριθμός των συμφωνιών που σχετίζονται με την τεχνητή νοημοσύνη στους τομείς της αεροδιαστημικής, της άμυνας και της ασφάλειας αυξήθηκε κατά 40% το 4ο τρίμηνο του 2023 σε σύγκριση με το 4ο τρίμηνο του 2022. Η ανάπτυξη αυτή υπογραμμίζει τη σημασία της τεχνητής νοημοσύνης για την προώθηση στρατηγικών πρωτοβουλιών και την ενίσχυση των επιχειρησιακών δυνατοτήτων των ενόπλων δυνάμεων της Δύσης, με τις ΗΠΑ να κατέχουν το μεγαλύτερο ποσοστό σε επενδύσεις.

Η ενσωμάτωση της τεχνητής νοημοσύνης στον κλάδο της αεροδιαστημικής επηρεάζει επίσης τις τάσεις στον τομέα των προσλήψεων στον χώρο της άμυνας. Το 4ο τρίμηνο του 2023, ο κλάδος παρουσίασε αύξηση 2% στις νέες θέσεις εργασίας σε σύγκριση με το προηγούμενο τρίμηνο. Ωστόσο, σημειώθηκε ετήσια μείωση 21% στις αγγελίες εργασίας, υποδεικνύοντας μια στροφή προς πιο εξειδικευμένους ρόλους ανάπτυξης AI.

Τα επαγγέλματα πληροφορικής και μαθηματικών αναδείχθηκαν ως οι κορυφαίοι ρόλοι εργασίας που σχετίζονται με την τεχνητή νοημοσύνη, αντιπροσωπεύοντας το 30% των νέων αγγελιών εργασίας το 4ο τρίμηνο του 2023. Ακολούθησαν οι ρόλοι της αρχιτεκτονικής και της μηχανικής, με αύξηση 8% στις αγγελίες εργασίας από το προηγούμενο τρίμηνο. Τα επαγγέλματα διαχείρισης ψηφιακών δεδομένων και οι επιχειρηματικές και οικονομικές δραστηριότητες κατέλαβαν επίσης σημαντικό μερίδιο των νέων αγγελιών εργασίας που σχετίζονται με την τεχνητή νοημοσύνη. Οι κορυφαίες εταιρείες στις προσλήψεις AI στους κλάδους της αεροδιαστημικής, της άμυνας και της ασφάλειας περιλαμβάνουν τις Huntington Ingalls Industries, CAE, Leidos, Boeing και RTX.

Χώρες που ηγούνται της υιοθέτησης της τεχνητής νοημοσύνης

Οι Ηνωμένες Πολιτείες βρίσκονται στην πρώτη γραμμή της υιοθέτησης της τεχνητής νοημοσύνης στους κλάδους της αεροδιαστημικής, της άμυνας και της ασφάλειας, με τον μεγαλύτερο αριθμό διπλωμάτων ευρεσιτεχνίας, θέσεων εργασίας και συμφωνιών που σχετίζονται με την τεχνητή νοημοσύνη. Η **Κίνα**, το **Ηνωμένο Βασίλειο**, η **Γαλλία** και η **Εσθονία** διατηρούν επίσης σημαντικές θέσεις στην υιοθέτηση της τεχνητής νοημοσύνης στον συγκεκριμένο τομέα.

Η ηγετική θέση των ΗΠΑ στην υιοθέτηση της τεχνητής νοημοσύνης καθοδηγείται από σημαντικές επενδύσεις στην **έρευνα και την ανάπτυξη**, την ισχυρή εστίαση στην **καινοτομία** και ένα ισχυρό οικοσύστημα που υποστηρίζει την πρόοδο της τεχνητής νοημοσύνης στον τομέα της άμυνας.

Μελλοντικές τάσεις και επιπτώσεις

Το μέλλον της αμυντικής βιομηχανίας θα επηρεαστεί σε μεγάλο βαθμό από τις τεχνολογίες τεχνητής νοημοσύνης και μηχανικής νέφους. Καθώς οι εταιρείες συνεχίζουν να επενδύουν σε καινοτομίες που βασίζονται σε AI, αρκετές βασικές τάσεις αναμένεται να διαμορφώσουν το τοπίο του κλάδου, μερικές από τις οποίες είναι οι παρακάτω:

1. **Βελτιωμένη λειτουργική αποδοτικότητα**: Οι τεχνολογίες AI θα συνεχίσουν να βελτιώνουν τη λειτουργική αποδοτικότητα αυτοματοποιώντας εργασίες ρουτίνας, βελτιστοποιώντας την κατανομή πόρων και ενισχύοντας τις διαδικασίες λήψης αποφάσεων. Αυτό θα οδηγήσει σε πιο εξορθολογιστικές λειτουργίες και αυξημένη παραγωγικότητα στον τομέα ανάπτυξης όπλων.

2. **Βελτιωμένη ασφάλεια και προστασία**: Τα συστήματα που βασίζονται στην τεχνητή νοημοσύνη θα ενισχύσουν την ασφάλεια και την προστασία στις αεροδιαστημικές και αμυντικές επιχειρήσεις. Οι προηγμένοι αλγόριθμοι τεχνητής νοημοσύνης μπορούν να εντοπίζουν και να ανταποκρίνονται σε απειλές ταχύτερα και ακριβέστερα, μειώνοντας τον κίνδυνο περιστατικών και βελτιώνοντας τη συνολική ασφάλεια.

3. **Καινοτομία και νέες δυνατότητες**: Η τεχνητή νοημοσύνη θα προωθήσει την καινοτομία, επιτρέποντας στις εταιρείες να αναπτύξουν νέες δυνατότητες και να βελτιώσουν τις υφιστάμενες. Αυτό περιλαμβάνει εξελίξεις στις τεχνολογίες UAV, τα αυτόνομα συστήματα και τα προηγμένα όπλα, τα οποία θα παρέχουν στρατηγικά πλεονεκτήματα σε στρατιωτικές επιχειρήσεις.

4. **Στρατηγικές συμπράξεις και συνεργασίες**: Η σημασία των στρατηγικών εταιρικών σχέσεων και συνεργασιών θα αυξηθεί καθώς οι εταιρείες επιδιώκουν να αξιοποιήσουν τις τεχνολογίες τεχνητής νοημοσύνης και να τις εντάξουν στην κατασκευή οπλικών συστημάτων. Οι προσπάθειες συνεργασίας μεταξύ αμυντικών εταιρειών, εταιρειών τεχνολογίας και ερευνητικών ιδρυμάτων θα προωθήσουν την καινοτομία και θα επιταχύνουν την ανάπτυξη λύσεων τεχνητής νοημοσύνης, με την Κίνα και τις ΗΠΑ να ηγούνται σε αυτόν τον τομέα.

5. **Μετασχηματισμός εργατικού δυναμικού**: Η ενσωμάτωση της τεχνητής νοημοσύνης θα μεταμορφώσει τον ρόλο δράσης του εργατικού δυναμικού, με αυξανόμενη ζήτηση για ταλέντα τεχνητής νοημοσύνης και εξειδικευμένους ρόλους. Οι εταιρείες θα πρέπει να επενδύσουν στην κατάρτιση και την ανάπτυξη για να εξοπλίσουν το εργατικό δυναμικό τους με τις απαραίτητες δεξιότητες για να εργαστεί με τεχνολογίες τεχνητής νοημοσύνης.

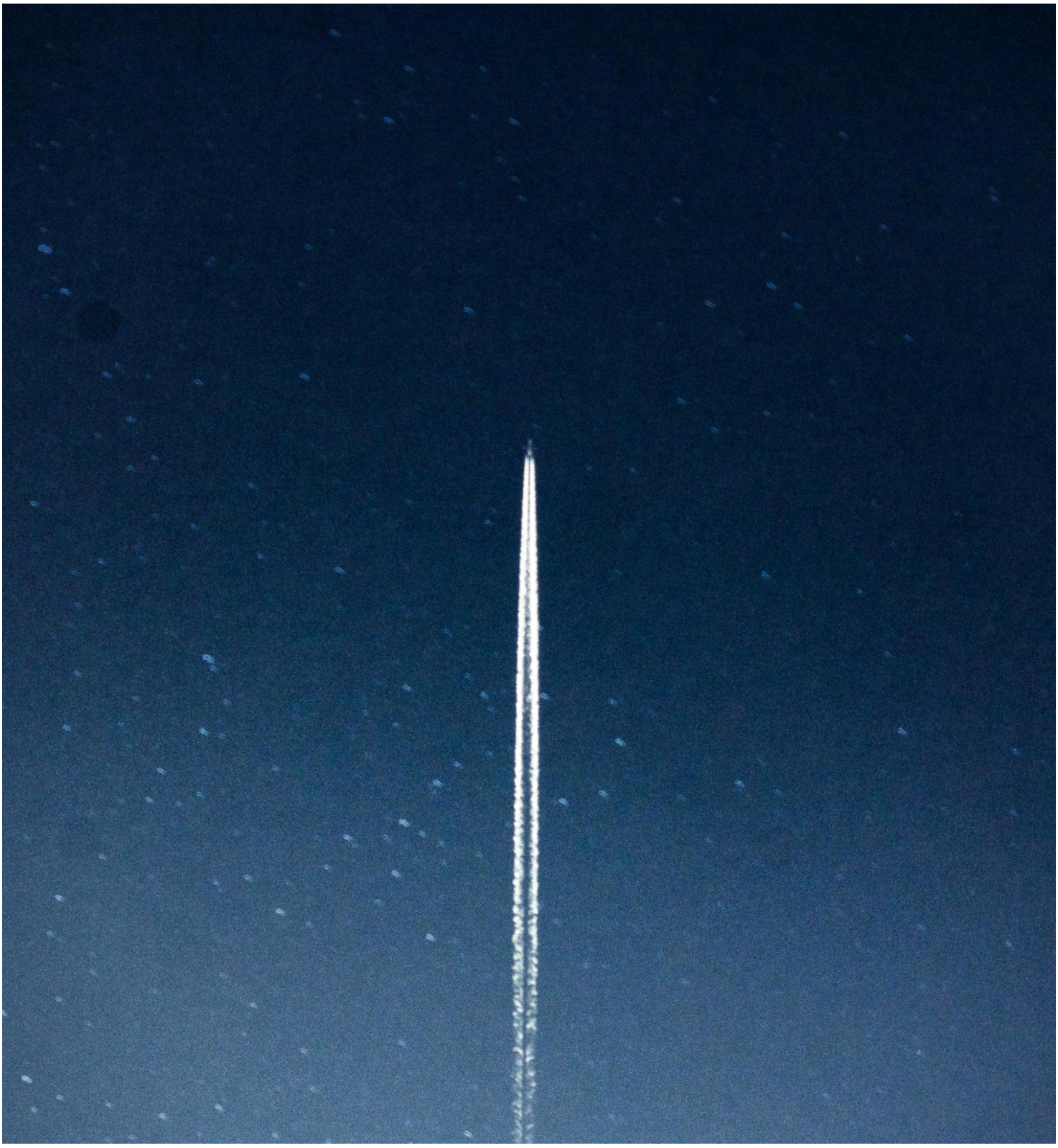
6. **Παγκόσμια ανταγωνιστικότητα**: Οι χώρες που επενδύουν στην τεχνητή νοημοσύνη και προωθούν την καινοτομία θα ενισχύσουν την παγκόσμια ανταγωνιστικότητά τους στην αεροδιαστημική και αμυντική βιομηχανία. Αυτό θα δώσει ώθηση στην οικονομική ανάπτυξη και θα ενισχύσει την εθνική ασφάλεια αλλά και την φονικότητα των παραγόμενων προϊόντων.

Συμπέρασμα

Η τεχνητή νοημοσύνη έχει μεταβάλει ήδη τον τρόπο λειτουργίας της αεροδιαστημικής βιομηχανίας τόσο σε επίπεδο ανάπτυξης προϊόντων όσο και σε επίπεδο βελτίωσης της διαχείρισης των

υλικών και ανθρωπίνων πόρων αλλά και στον εκσυγχρονισμό και την αποτελεσματικότητα ήδη υπαρχόντων οπλικών συστημάτων. Η συζήτηση πλέον έχει μεταβληθεί και δεν εξετάζουμε το τι θα γίνει σε περίπτωση ενσωμάτωσης της τεχνητής νοημοσύνης στη βιομηχανία άμυνας, αλλά πόσο αποτελεσματική θα είναι και σε ποιους τομείς θα χρησιμοποιηθεί η τεχνητή νοημοσύνη για την βελτίωση του στρατεύματος.

Η δημιουργία και η συντήρηση ενός αξιόμαχου στρατεύματος μετατρέπεται σε μία πολύ πιο προσιτή και απλή διαδικασία καθώς πλέον τα προβλήματα ανάπτυξης μεταφέρονται από τον υλικό κόσμο προς τον ψηφιακό. Δεν πρέπει να ξεχνάμε πως για την ανάπτυξη λογισμικών τεχνητής νοημοσύνης χρειάζονται αρκετά εξελιγμένοι υπολογιστές με τοποθετημένους ημιαγωγούς στο εσωτερικό τους. Οι ημιαγωγοί αυτοί για να λειτουργήσουν με λογισμικό τεχνητής νοημοσύνης χρειάζεται να περιλαμβάνουν σπάνιες γαίες από την Κίνα και να έρχονται από τα εργοστάσια της TSMC στην Ταϊβάν προς τα δυτικά κράτη. Η δυναμική αυτή συνθέτει ένα πάρα πολύ επικίνδυνο και ανταγωνιστικό τοπίο στην Ανατολική Ασία το οποίο μπορεί ανά πάσα στιγμή να παγώσει κυριολεκτικά σε ψηφιακό και οικονομικό επίπεδο ολόκληρο τον πλανήτη.



The contribution of the European Peace Facility to the security and resilience of the EU and its Member States

Panagiotis (Panos) Blanos
Μέλος ΑΛΛΗΛΟΝ
Commander (Hellenic Navy), EU Military Finance Expert, ESDC trainer
MSc 'Law of the Economy and of the Enterprises'
Panagiotis (Panos) Blanos | LinkedIn

Περίληψη

The European Peace Facility, an off-EU budget CFSP instrument, proves to be an important element of the EU's effort to increase the security and resilience of itself and of its Member States. The recognition of this role of the EPF is proven through taking into consideration the different elements of the CFSP, as described in the EU's Strategic Compass, whose costs are partly or fully eligible for common funding under the EPF, namely the EU military operations, the assistance measures to partners, the Rapid Deployment Capacity, the Military Planning and Conduct Capability and the EU military exercises.

Introduction

After the deterioration of the security environment in February 2022, resilience has become a priority for the EU's Common Foreign and Security Policy (CFSP). The present article is an effort to approach the contribution of the European Peace Facility (EPF), an off-EU budget financial instrument of the CFSP, to the security and resilience of the European Union and its Member States.

Picture 1: Facts regarding the EPF
Source: Security Compass (europa.eu)

The European Peace Facility

The EPF was established in 2021, repealing pre-existing CFSP instruments, for the financing of the common costs of the EU military operations and of assistance measures to third countries, including Ukraine. It is an intergovernmental instrument of the CFSP, managed by a *Facility Committee* of Member States' representatives, chaired by the rotating Presidency of the Council of the EU. As an integral element of the CFSP, it is explicitly referred to in the EU's Strategic Compass (established 2022) under the 'ACT' work strand, and in its first implementation report (2023) it is referred to by the High Representative as a '*game changer*'.

The EPF is currently used for the financing of:

1. Nine (9) on-going military operations of the Union, including:

   a. The unprecedented in magnitude and mandate '*EUMAM Ukraine*', launched in November 2022 for the training of tenths of thousands of Ukrainian soldiers on European soil, and
   b. The naval operation '*ASPIDES*', launched in February 2024 for the protection of navigation in the Red Sea against Houthi attacks to merchant vessels.

2. Numerous assistance measures to third countries in the Eastern and Southern Neighbourhood, including:

   a. In support of the *Ukrainian Armed Forces* with lethal and non-lethal military equipment of a value over 4,5 billion euros.
   b. In support of *African countries* (such as Somalia and Mozambique), inter alia with training equipment complimenting the mandate of EU military training missions in those countries, in implementation of the so-called 'train and equip' model.

Resilience in the EU's Common Foreign and Security Policy

Resilience is a significant element and target of the EU's CFSP and it is understood as a capability against factors that could jeopardise the integrity and the interests of the Union and its Member States. Those factors are conventional threats, including territorial sovereignty and infrastructure security, but also hybrid threats, including cyber-attacks, foreign information manipulation, and instrumentalization of immigration. Resilience is also tightly linked to the idea of strategic autonomy, in the vein of security and defence, but also economically and world-trade wise, namely in the sense of critical raw materials.

The EU's Strategic Compass is clear regarding resilience:

"The more hostile security environment requires us to make a quantum leap forward and increase our capacity and willingness to act, strengthen our resilience and ensure solidarity and mutual assistance. [...] We aim to become a more assertive security and defence actor by enabling more robust, rapid and decisive action, including for the resilience of the Union and our mutual assistance and solidarity [..] Our strategic competitors are targeting us with a broad set of tools and testing our resilience with the aim to diminish our security and actively undermine our secure access to the maritime, air, cyber and space domains".

EPF as a security & resilience tool

One could ask: How specifically has the EPF contributed to the security and resilience of the EU and its Member States in these last 3.5 years of its existence?

Picture 2: The 4 pillars of the EU Strategic Compass
Source: Security Compass (europa.eu)

This contribution is mainly provided through the following dimensions:

1. EU military operations and missions: The EPF is the CFSP instrument for the financing of the common costs of the EU military operations and missions. As highlighted in the first pillar (ACT) of the Strategic Compass:

"More robust, flexible and modular CSDP civilian and military missions and operations should allow us to adapt swiftly to new threats and challenges and increase their effectiveness, also in view of the new security context and the growing presence of our strategic competitors in operational theatres".

Therefore, the EPF proves to be an integral supportive element of a swifter adaptation of the EU to new threats. This remains extremely important, in light of the presence of the EU's strategic competitors (Russia, China) in critical areas of the world in the Eastern and Southern Neighborhood.

2. Support to partners: Once again, the Strategic Compass provides that:

"[...] Through an increased use of the European Peace Facility, the EU can rapidly provide important assistance to partners for example providing military equipment often supplementing training by CSDP missions. This can also be done by supporting partners' defence capabilities in moment of crisis, as in the case of the assistance package to support the Ukrainian armed forces to defend their territorial integrity and sovereignty and protect the civilian population from an unprovoked and unjustified aggression".

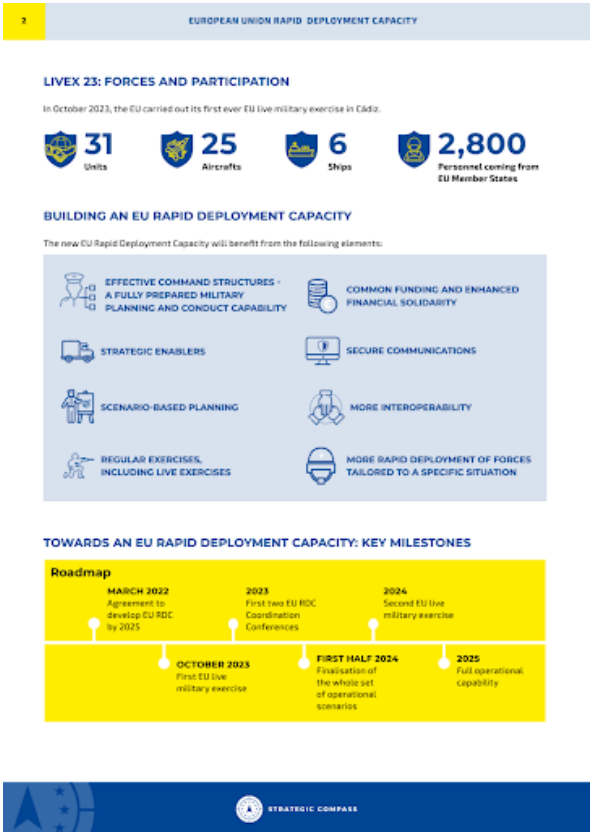
The increased resilience of the EU's partners, through either the military training missions or the assistance measures under the EPF, is therefore supported by the financing of the instrument. In the 2024 progress report of the Strategic Compass, the European External Action Service (EEAS) refers to the reinforcement by the EU "*of its support in the Western Balkans through the EPF as well as on counterterrorism and resilience*".

3. Military Planning and Conduct Capability (MPCC): The Strategic Compass describes a need to:

"[…] gradually further strengthen our civilian and military command and control structures. We will ensure that the MPCC is fully able to plan, control and command non-executive and executive tasks and operations, as well as live exercises. In this context, we will ramp up personnel contributions and ensure that we have the necessary communication and information systems, as well as required facilities. Once the MPCC reaches its full operational capability, it should be seen as the preferred command and control structure".

The EPF funds the incremental costs of the MPCC. In this sense, it could be seen as an instrument to reinforce the EU's Command and Control (C2) structure, therefore strengthening the EU's resilience.

4. Rapid Deployment Capacity (RDC): The Strategic Compass commits to the development of an RDC, a modular force of up to 5,000 troops, including land, air and maritime components, as well as the required strategic enablers, in order for the Union to be able to "[…] *respond to imminent threats or quickly react to a crisis situation outside the Union at all stages of the conflict cycle*". Part of the incremental costs of the RDC are eligible for common funding under the EPF and in this sense the Facility can be deemed as a contributor to the EU resilience stemming from the increased ability to counter crises and threats.



Picture 3: Facts regarding the EU RDC
Source: 2024-03-EU-Rapid-Deployment-Capacity_EN.pdf (europa.eu)

5. Expansion of the EPF common costs: One of the commitments undertaken by the EU leaders that agreed on the text of the Strategic Compass in March 2022 was the expansion of the width and of the scope of common costs under the EPF. Currently, the EPF finances mainly costs other than those that in any case would have been borne by an EU Member State ('incremental costs', stemming from the nature of the EU's effort as a common one). These discussions may be arisen in the vein of the mid-term review of the Council Decision establishing the EPF, a discussion expected in 2024. If these discussions prove to be fruitful and in the direction implied by the Strategic Compass, then it could be claimed that the EPF will be reinforced as a contributor to the EU's resilience, through the stronger financing of EU military operations and missions.

6. Common Security and Defence Policy (CSDP) exercises: The Strategic Compass embraces the approach that:

"[…] Readiness and interoperability are crucial elements of our response to threats and strategic competition. Frequent civilian and military live exercises in all domains, as well as reinforced advance planning, will help us to substantially boost our readiness, foster interoperability and support a common strategic culture. Live exercises in an EU framework, with the progressive involvement of the Military Planning and Conduct Capability will shape the EU Rapid Deployment Capacity in particular, and more generally will reinforce our posture, add to our strategic communication and strengthen interoperability, including with partners".

Having in mind that the EPF can also finance military exercises, especially live ones, it appears that the instrument contributes substantially to activities that establish more robustly the EU as a sovereign and resilient global security provider. Special reference is needed to the *MILEX 2023*, the first ever live military exercise of the EU, in Cadiz (Spain), exceptionally financed by the EPF with common costs broader than the ones provided in principle, in transitional provisions of one of the amendments of the Council Decision establishing the EPF.

Conclusion

Through specific elements of the CFSP that –according to the legal framework of the EPF– are eligible for common funding under this CFSP instrument, the article revealed the role of this tool in enhancing and strengthening the Union's and its Member States' security and resilience. What remains to be seen is the extent of the political will of the Member States to really make the full use of the instrument implied in the Strategic Compass, having in mind the budgetary restrictions and priorities to be set, under the political framework of the new 5-year EU cycle.

References

- Council of the EU, European Peace Facility European Peace Facility - Consilium (europa.eu)
- European External Action Service The European Peace Facility Factsheet | EEAS (europa.eu)
- European Publications Office EUR-Lex - 02021D0509-20240318 - EN - EUR-Lex (europa.eu)
- Strategic Compass A Strategic Compass for Security and Defence | EEAS (europa.eu)

- P. Blanos, G. Papagiannis, I. Foukas, 'The Role of the European Peace Facility in Enhancing EU Security and Defence cooperation', European Journal for Security Research
- P. Blanos, 'The European Peace Facility, a game changer in the CFSP of the EU', NRDC-GR Herald (2024), 49-53. https://nrdc.gr/wp-content/uploads/2024/02/NRDC-GR-Herald-Magazine-Issue-21-LQ.pdf

Η Ευρωπαϊκή Αμυντική Βιομηχανική Στρατηγική (European Defence Industrial Strategy) και η συμβολή όσον αφορά την ασφάλεια, την ανθεκτικότητα, την επιχειρηματικότητα και τη μείωση της ανεργίας

Αντισυνταγματάρχης ε.α. Κουκάκης Γεώργιος
Μέλος ΑΛΛΗΛΟΝ
Διεθνολόγος, Συγγραφέας, Κύριος Ερευνητής του ΚΕΔΙΣΑ, Research Associate of HERMES, Μέλος του ΕΛ.Ι.Σ.ΜΕ., της ΑΛΛΗΛΟΝ και της Mercury Negotiation Academy, Ακαδημαϊκός Υπεύθυνος του Προγράμματος «Σπουδές Ασφάλειας στη Μεσόγειο (BASIC)» του ΚΕΔΙΒΙΜ Πανεπιστημίου Αιγαίου
Georgios Koukakis | LinkedIn

Περίληψη

Το παρόν άρθρο αναφέρεται στην Ευρωπαϊκή Αμυντική Βιομηχανική Στρατηγική που δημοσιεύτηκε για πρώτη φορά από την Ευρωπαϊκή Ένωση στις 5 Μαρτίου 2024. Υποστηρίζει δε ότι το εν λόγω στρατηγικό έγγραφο συμβάλλει σημαντικά –εκτός από την αυτονόητη ανάπτυξη του τομέα της άμυνας και ασφάλειας– στην προώθηση της επιχειρηματικότητας και την καταπολέμηση της ανεργίας.

Αν και οι έννοιες της ασφάλειας και της ανθεκτικότητας είναι άρρηκτα συνδεδεμένες με αυτή της άμυνας –δηλαδή της προάσπισης ενός δρώντα από εξωτερικές στρατιωτικές απειλές– εν τούτοις είναι πολύ πιο ευρείες, περιλαμβάνοντας την προστασία του δρώντα και τη μείωση των τρωτοτήτων του αντίστοιχα έναντι κάθε είδους εσωτερικών ή/και εξωτερικών απειλών (οικονομικές, περιβαλλοντικές, υγειονομικές, κ.λπ.). Παρ' όλα αυτά, η άμυνα αποτελεί τη «ραχοκοκαλιά» της ασφάλειας και της ανθεκτικότητας, καθώς εξασφαλίζει την ειρήνη και τη σταθερότητα, συνθήκες οι οποίες επιτρέπουν στους πολίτες, τις επιχειρήσεις και τους οργανισμούς να αναπτύξουν απερίσπαστοι τις οικονομικές, εμπορικές, κ.λπ. δραστηριότητές τους, διευκολύνοντας με τον τρόπο αυτό την ανάπτυξη σε ατομικό και συλλογικό επίπεδο.

Εικόνα 1: Ενημερωτικό Φυλλάδιο της ΕΕ για την Ευρωπαϊκή Αμυντική Βιομηχανική Στρατηγική
Πηγή: https://defence-industry-space.ec.europa.eu/european-defence-industrial-strategy-factsheet_en

Αναπόσπαστο δε κομμάτι της άμυνας είναι η **αμυντική βιομηχανία**, το σύνολο δηλαδή των δημόσιων και ιδιωτικών επιχειρήσεων οι οποίες παράγουν ή προμηθεύουν τους κρατικούς και μη δρώντες με αγαθά ή παρέχουν υπηρεσίες που σχετίζονται με οποιονδήποτε τρόπο με τον αμυντικό τομέα. Αναγνωρίζοντας την ιδιαίτερα σημαντική αυτή συμβολή –σε συνδυασμό με το γεγονός ότι το σύγχρονο περιβάλλον ασφάλειας αποτελεί ένα περιβάλλον **αεικρίσεων** (permacrises) και **πολυκρίσεων** (polycrises) – η Ευρωπαϊκή Ένωση (ΕΕ) εξέδωσε στις 5 Μαρτίου 2024 την πρώτη **Ευρωπαϊκή Αμυντική Βιομηχανική Στρατηγική** (European Defence Industrial Strategy, EDIS) η οποία αποσκοπεί:

1. Στην αύξηση και βελτίωση των **επενδύσεων** των κρατών-μελών (κ-μ) της ΕΕ,
2. Στη διευκόλυνση της **συνεργασίας** των κ-μ της ΕΕ, και
3. Στο **συντονισμό** των δράσεων των κ-μ της ΕΕ όσον αφορά τον τομέα της ασφάλειας και της άμυνας.

Εικόνα 2: Ενημερωτικό Φυλλάδιο της ΕΕ για την Ευρωπαϊκή Αμυντική Βιομηχανική Στρατηγική
Πηγή: https://defence-industry-space.ec.europa.eu/european-defence-industrial-strategy-factsheet_en

Επιπλέον, το εν λόγω έγγραφο επισημαίνει ότι η Αμυντική Βιομηχανία της ΕΕ συμβάλλει ζωτικά στην **επιχειρησιακή ετοιμότητα** του αμυντικού τομέα, καθώς επιτρέπει στα κ-μ της ΕΕ να προστατεύουν τους πολίτες τους, την ακεραιότητα του εδάφους και των κρίσιμων περιουσιακών στοιχείων και υποδομών, καθώς και τις θεμελιώδεις δημοκρατικές αξίες και διαδικασίες. Επιπλέον παρέχει στην ΕΕ τη δυνατότητα να παρέχει **στρατιωτική βοήθεια** στους εταίρους της (όπως συμβαίνει πρόσφατα με την Ουκρανία), αλλά και να ενεργεί **ταχύτερα** και πιο **αποφασιστικά** σε περιόδους κρίσεων.

Εικόνα 3: Ενημερωτικό Φυλλάδιο της ΕΕ για το Ευρωπαϊκό Πρόγραμμα Αμυντικής Βιομηχανίας
Πηγή: https://defence-industry-space.ec.europa.eu/european-defence-industry-programme-factsheet_en

Η Ευρωπαϊκή Αμυντική Βιομηχανική Στρατηγική τονίζει επίσης μεταξύ άλλων την ανάγκη ενδυνάμωσης της **Ευρωπαϊκής Αμυντικής Τεχνολογικής και Βιομηχανικής Βάσης** (European Defence Technological and Industrial Base, EDTIB) συμπεριλαμβανομένων και των μικρομεσαίων επιχειρήσεων, μέσω:

1. Περισσότερων, καλύτερων, ομαδικών και ευρωπαϊκών **επενδύσεων**,
2. Της ενίσχυσης της **ασφάλειας ανεφοδιασμού**,
3. Της ανάπτυξης εξειδικευμένων **οικονομικών εργαλείων**,
4. Της καλλιέργειας **κουλτούρας αμυντικής ετοιμότητας**, και
5. Της ανάπτυξης **συνεργατικών σχημάτων** με εταίρους όμοιας ιδεολογίας.

Για την υποστήριξη δε της εν λόγω στρατηγικής, η ΕΕ έχει εκπονήσει το Ευρωπαϊκό Πρόγραμμα Αμυντικής Βιομηχανίας (European Defence Industry Programme, EDIP), μέσω του οποίου:

1. Παρέχεται **οικονομική υποστήριξη** ύψους 1.500.000.000€ από τον προϋπολογισμό της ΕΕ για την περίοδο 2025-2027,
2. Ενδυναμώνεται η **ανταγωνιστικότητα**, η **ανταπόκριση** και η **ανθεκτικότητα** της Αμυντικής Τεχνολογικής και Βιομηχανικής Βάσης της ΕΕ,
3. Υποβοηθείται η ανοικοδόμηση και ο εκσυγχρονισμός της **Αμυντικής Βιομηχανίας της Ουκρανίας**,
4. Παρέχονται νέα **εργαλεία** στα κ-μ της ΕΕ για τη διευκόλυνση της συνεργασίας τους,
5. Εξασφαλίζεται η **διαθεσιμότητα** και ο **εφοδιασμός** αμυντικών

προϊόντων σε σταθερή βάση, έγκαιρα και στις απαιτούμενες ποσότητες.

Εικόνα 4: Ενημερωτικό Φυλλάδιο της ΕΕ για το Ευρωπαϊκό Πρόγραμμα Αμυντικής Βιομηχανίας
Πηγή: https://defence-industry-space.ec.europa.eu/european-defence-industry-programme-factsheet_en

Στο σημείο αυτό αξίζει να τονιστεί ότι μέσω της Ευρωπαϊκής Αμυντικής Βιομηχανικής Στρατηγικής και του Ευρωπαϊκού Προγράμματος Αμυντικής Βιομηχανίας υποβοηθείται η επίτευξη των στόχων που έχει θέσει η ΕΕ στην τρίτη κατά σειρά Στρατηγική Ασφάλειας (Security Strategy) της ΕΕ –η πρώτη δημοσιεύτηκε το 2003 (European Security Strategy, ESS) και η δεύτερη το 2016 (European Union Global Strategy, EUGS)– με την ονομασία **Στρατηγική Πυξίδα** (Strategic Compass), οι οποίοι είναι ομαδοποιημένοι στους ακόλουθους τέσσερις πυλώνες:

Εικόνα 5: Οι 4 Πυλώνες της Στρατηγικής Πυξίδας
Πηγή: https://www.eeas.europa.eu/sites/default/files/documents/2022-03-21_strategic_compass-factsheet.pdf

1. **ΔΡΩ** (ACT), ο οποίος προβλέπει μεταξύ άλλων τη δημιουργία μίας Ευρωπαϊκής Δύναμης Ταχείας Ανάπτυξης (EU Rapid Deployment Capacity, EURDC), τη διεξαγωγή κοινών στρατιωτικών ασκήσεων σε ξηρά και θάλασσα, την ενίσχυση της στρατιωτικής κινητικότητας και των αποστολών/επιχειρήσεων της Κοινής Πολιτικής Ασφάλειας και Άμυνας (ΚΠΑΑ), και την ταχύτερη και πιο ευέλικτη λήψη απόφασης.
2. **ΑΣΦΑΛΙΖΩ** (SECURE), ο οποίος προβλέπει μεταξύ άλλων τη δημιουργία μίας ποικιλίας Εργαλειοθηκών (για τις Υβριδικές Απειλές, την Ψηφιακή Διπλωματία και την Ξένη Χειραγώγηση Πληροφοριών & Παρέμβαση), τη δημιουργία Ομάδων Αντίδρασης Υβριδικών Απειλών, την εφαρμογή Πολιτικής Κυβερνοασφάλειας και Διαστημικής Στρατηγικής για την Ασφάλεια και την Άμυνα και τη συντονισμένη θαλάσσια παρουσία σε παγκόσμιο επίπεδο,
3. **ΕΠΕΝΔΥΩ** (INVEST), ο οποίος προβλέπει μεταξύ άλλων την αύξηση των αμυντικών δαπανών, τη βελτίωση της συνεργασίας των κ-μ, την ανάπτυξη στρατηγικών δυνατοτήτων και την προώθηση της καινοτομίας για τη μείωση της στρατηγικής εξάρτησης από άλλους δρώντες, και
4. **ΣΥΝΕΤΑΙΡΙΖΟΜΑΙ** (PARTNER), ο οποίος προβλέπει μεταξύ άλλων την ενδυνάμωση της συνεργασίας της ΕΕ με άλλους οργανισμούς όπως το NATO, ο ΟΗΕ, ο ΟΑΣΕ, η Αφρικανική Ένωση και ο ASEAN, την ανάπτυξη νέων εταιρικών σχέσεων και την στρατιωτική υποβοήθηση εταίρων μέσω του Ευρωπαϊκού Μηχανισμού Ειρήνης (European Peace Facility, EPF).

Λαμβάνοντας υπόψιν τα στοιχεία που παρουσιάστηκαν στο παρόν άρθρο σε συνδυασμό με την αυξανόμενη εμφάνιση κρίσεων που παρατηρείται στις μέρες μας, γίνεται αντιληπτό ότι **η Ευρωπαϊκή Αμυντική Βιομηχανική Στρατηγική παρέχει το απαραίτητο θεσμικό πλαίσιο για την ανάπτυξη της Αμυντικής Βιομηχανίας** των κ-μ της και τα οικονομικά εργαλεία για την υποστήριξη των αντίστοιχων μικρομεσαίων επιχειρήσεων. Η παραγωγή μέσων/συστημάτων επιθετικού χαρακτήρα (όπως τα κάθε λογής όπλα) συμβάλλει στην ενίσχυση των στρατιωτικών ικανοτήτων των κ-μ ώστε να μπορεί η ΕΕ να λειτουργεί ως πάροχος ασφάλειας (security provider), ενώ η αντίστοιχη παραγωγή μέσων/συστημάτων αμυντικού χαρακτήρα (όπως τα ραντάρ) στην ενίσχυση της ανθεκτικότητας, καθώς αυξάνουν την επιβιωσιμότητα έναντι των απειλών.

Επιπλέον, η ενίσχυσης της Αμυντικής Βιομηχανίας και η συνεργασία με άλλα κράτη συμβάλλει στην τόνωση της οικονομίας, την ανάπτυξη της επιχειρηματικότητας και τη διαφοροποίηση των πόρων, αυξάνοντας με τον τρόπο αυτό την **οικονομική ασφάλεια** των κ-μ και την **οικονομική ανθεκτικότητα** των αντίστοιχων επιχειρήσεων –οι οποίες μάλιστα όπως τονίζεται στο υπόψιν έγγραφο σε αρκετά κ-μ υπολειτουργούν– καθώς μπορούν να αντιμετωπίσουν ευκολότερα τις μεταβαλλόμενες συνθήκες της αγοράς αλλά και ενδεχόμενες κρίσεις που ίσως προκύψουν.

Τέλος, διαπιστώνεται ότι **ο τομέας της Αμυντικής Βιομηχανίας αποτελεί ένα πολλά υποσχόμενο πεδίο όσον αφορά τις σπουδές και την επαγγελματική απασχόληση των νέων**, τόσο σε ερευνητικό επίπεδο όσο και σε επίπεδο πρωτογενούς ή δευτερογενούς παραγωγής, συμβάλλοντας με τον τρόπο αυτό στη **μείωση της ανεργίας**. Σε κάθε περίπτωση, η Ευρωπαϊκή Αμυντική Βιομηχανική Στρατηγική αποτελεί μία θετική πρωτοβουλία της ΕΕ, ενδεικτική του τρόπου προσαρμογής της στις επικρατούσες συνθήκες, γεγονός που επισημαίνεται από τον **Josep Borrell** (Ύπατος Εκπρόσωπος της ΕΕ για θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας/Αντιπρόεδρος της Ευρωπαϊκής Επιτροπής) στην ακόλουθη δήλωσή του:

«Πρέπει να ενισχύσουμε την αμυντική βιομηχανική και τεχνολογική μας βάση. Αυτό δεν ήταν σαφές σε κανέναν πριν από τον επιθετικό πόλεμο της Ρωσίας κατά της Ουκρανίας, αλλά τώρα έχει γίνει κοινή λογική. Είναι απαραίτητη προϋπόθεση αν θέλουμε να είμαστε σε θέση να ενισχύσουμε την αμυντική μας ικανότητα σε ένα τεταμένο γεωπολιτικό πλαίσιο».

ΕΝΔΕΙΚΤΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Κουκάκης, Γ. (2022). "Προς τα που δείχνει η Στρατηγική Πυξίδα της Ευρωπαϊκής Ένωσης;". Κέντρο Διεθνών Στρατηγικών Αναλύσεων. Ερευνητική Εργασία No.78. https://www.doi.org/10.13140/RG.2.2.11656.70406 (28/04/2024).

European Union External Action. (2024, March 16). "European Union Rapid Deployment Capacity". https://www.eeas.europa.eu/eeas/european-union-rapid-deployment-capacity_en (28/04/2024).

European Union External Action. (2024, March 11). "Time to strengthen European defence industry". https://www.eeas.europa.eu/eeas/time-strengthen-european-defence-industry_en (28/04/2024).

Koukakis, G. (2023). Permacrises and Polycrises: Outlining the Contemporary Security Environment through References to Strategic Documents of Regional and International Actors. HAPSc Policy Briefs Series, 4(2), 55–64. https://doi.org/10.12681/hapscpbs.36661 (28/04/2024).

Koukakis, G. (2023). Resilience: Highlighting its Importance for Security and Development through References to (National) Security Strategic Documents of International Actors. HAPSc Policy Briefs Series, 4(1), 77–87. https://doi.org/10.12681/hapscpbs.35186 (28/04/2024).

Koukakis, G. (2024). "The First Ever 2024 European Defence Industrial Strategy: Background, Challenges and Future Considerations Regarding the European Security and Defense". HERMES Institute of International Affairs, Security & Geoeconomy. Ocassional Paper 2/2024. https://www.doi.org/10.13140/RG.2.2.27247.44961 (28/04/2024).

Ελληνική Δημοκρατία/Υπουργείο Εξωτερικών. (2024, Μάρτιος 14). "Κοινή Πολιτική Ασφάλειας και Άμυνας (ΚΠΑΑ)". https://www.mfa.gr/exoteriki-politiki/i-ellada-stin-ee/kpaa.html (28/04/2024).

Ένθετο Γ:
Το Βήμα των Ομιλητών μας
Ενεργειακή Μετάβαση

Μήνυμα Εκδότη

Το Βήμα των Ομιλητών μας - Ενεργειακή Μετάβαση

Άγγελος Παγκράτης
Ιδρυτής και Πρόεδρος ΔΕ της ΑΛΛΗΛΟΝ, Εκδότης του e-Άλληλον
Πρώην Επιτετραμμένος της ΕΕ στις ΗΠΑ και πρώην πρέσβης της ΕΕ στην Αργεντινή και στον Παγκόσμιο Οργανισμό Εμπορίου
Angelos Pangratis | LinkedIn

Δημοσιεύουμε στο παρόν ένθετο διαφάνειες από PowerPoint δύο ομιλητών μας οι οποίες προσφέρουν: **1ον. Οπτική κατανόηση**: Οι χάρτες και τα δεδομένα για τις περιοχές έρευνας υδρογονανθράκων παρουσιάζονται αποτελεσματικά με τη χρήση οπτικών υλικών. **2ον. Ιστορική τεκμηρίωση**: πρόκειται για ιστορικά ντοκουμέντα, τα οποία αποδεικνύουν με σαφήνεια τη σημασία των μέχρι σήμερα ερευνών στον ελληνικό χώρο, σε ξηρά και σε θάλασσα. **3ον. Επιβεβαίωση μεγέθους**: Η Ελλάδα διαθέτει τόσο σημαντικά αποθέματα ώστε η εκμετάλλευσή τους θα μπορούσε να εκτινάξει την ελληνική οικονομία.

Ο **κ. Ζεληλίδης**, στην παρουσίασή του, αναφέρεται στις εντυπωσιακές έρευνες της ομάδας του για την ύπαρξη «πεδίων υδρογονανθράκων από την Κεντρική Ελλάδα (Μεσοελληνική Αύλακα) έως τα Διαπόντια Νησιά, τη δυτική Ελλάδα και την Κρήτη, μέχρι και την Κάρπαθο». Παράλληλα, επισημαίνει την ύπαρξη υδριτών στην περιοχή του Καστελόριζου. Αντίστοιχα, ο **κ. Γεωργίου** αναφέρεται σε εκτεταμένες μελέτες της κρατικής αρχής ΕΔΕΥΕΠ και του Ινστιτούτου Ενέργειας ΝΑ Ευρώπης (ΙΕΝΕ). Όσον αφορά τον όγκο αυτών των αποθεμάτων, τονίζει: «Όλες οι δημοσιευμένες μελέτες από πετρελαϊκές και τεχνικές εταιρείες, ακαδημαϊκούς φορείς και ινστιτούτα συμφωνούν ότι η ανακάλυψη και εκμετάλλευση κοιτασμάτων φυσικού αερίου είναι εφικτή, σε ποσότητες ικανές όχι μόνο να καλύψουν τις ανάγκες της χώρας, αλλά και να ανταποκριθούν σε μεγάλο μέρος των ευρωπαϊκών αναγκών, αντικαθιστώντας τις εισαγωγές από τη Ρωσία». Επίσης παρουσιάζει ακριβώς την επίσημη εκτίμηση των αποθεμάτων αυτών. Η εκτίμηση αυτή δείχνει ότι ο ορυκτός πλούτος που διαθέτει η χώρα, είναι τόσο σημαντικός ώστε η αξιοποίηση του θα μπορούσε να συμβάλει τα μέγιστα στην ανατροπή της τωρινής πορείας φτωχοποίησης της χώρας και των πολιτών της, βελτιώνοντας καθοριστικά τις προοπτικές οικονομικής ανάπτυξης και βοηθώντας έτσι και στην αντιμετώπιση φαινομένων όπως η φυγή νέων επιστημόνων στο εξωτερικό και η δραματική τωρινή υπογεννητικότητα. Αντ' αυτού όμως, κυριαρχούν τα τελευταία χρόνια φαινόμενα όπως: ασάφεια κυβερνητικών προθέσεων και δηλώσεων, νομοθετικά κενά που επιτρέπουν την εύκολη προσφυγή διαφόρων σωματείων εναντίον ερευνών, γραφειοκρατία και βραδύτητα στις διοικητικές και δικαστικές διαδικασίες, έλλειψη υποδομών ,όπως λιμάνια που δεν είναι έτοιμα να εξυπηρετήσουν τις ανάγκες των εξορύξεων, και άλλα τέτοια φαινόμενα που δημιουργούν υπερβολική ανασφάλεια για τον επενδυτή και δίνουν ένα συνολικό μήνυμα **έλλειψης πολιτικής βούλησης**.

Η τωρινή κατάσταση εγείρει ένα **τεράστιο θέμα δημοκρατίας** και υποστηρίζει την ανάγκη διαμόρφωσης μιας **διακομματικής εθνικής στρατηγικής** τουλάχιστον εν μέρει εμπνευσμένης από το παράδειγμα της Νορβηγίας όπως αναφέρουμε και στο αρχικό μήνυμα του εκδότη του τεύχους τούτου.

Η διαχρονική εξέλιξη των ερευνων υδρογονανθράκων στην Ελλάδα

Αβραάμ Ζεληλίδης
Καθηγητής Τμήματος Γεωλογίας Πανεπιστημίου Πατρών
Αβραάμ Ζεληλίδης | Facebook

Περίληψη

Στην παρουσίαση που ακολουθεί περιγράφονται σταθμοί των ερευνών μας στην Ελλάδα, στα πλαίσια της αναζήτησης πεδίων υδρογονανθράκων, από την Κεντρική Ελλάδα (Μεσοελληνική Αύλακα), και σε όλο το μήκος και πλάτος της δυτικής Ελλάδας και Κρήτης (από τα Διαπόντια νησιά μέχρι την Κάρπαθο). Οι έρευνες ξεκίνησαν το 1995 και συνεχίζονται μέχρι και σήμερα και έχουν αναδειχτεί περιοχές με πολύ μεγάλο δυναμικό, τόσο υγρών όσο και αερίων υδρογονανθράκων, ενώ αναδεικνύονται και οι υδρίτες του Καστελόριζου.

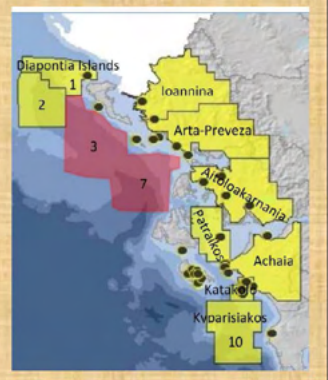
Mesozoic oil-prone and Cenozoic gas-prone source rocks have been identified.

Mesozoic **source rocks** include organic-rich intervals in 1. Triassic evaporites; 2. marls at the base of the Early Jurassic (Lower Toarcian) Ammonitico Rosso; 3. the Early to Middle Jurassic (Toarcian – Aalenian) Lower Posidonia beds; 4. the Upper Posidonia beds [Late Jurassic (Callovian – Tithonian)]; and 5. the Vigla Shales Member of the Vigla Limestone [Late Cretaceous (Cenomanian – Turonian)]. Cenozoic gas-prone source rocks include organic-rich intervals in Paleogene (Eocene–Oligocene) and Neogene (Aquitanian–Burdigalian) submarine fan deposits of the Pindos foreland basin.

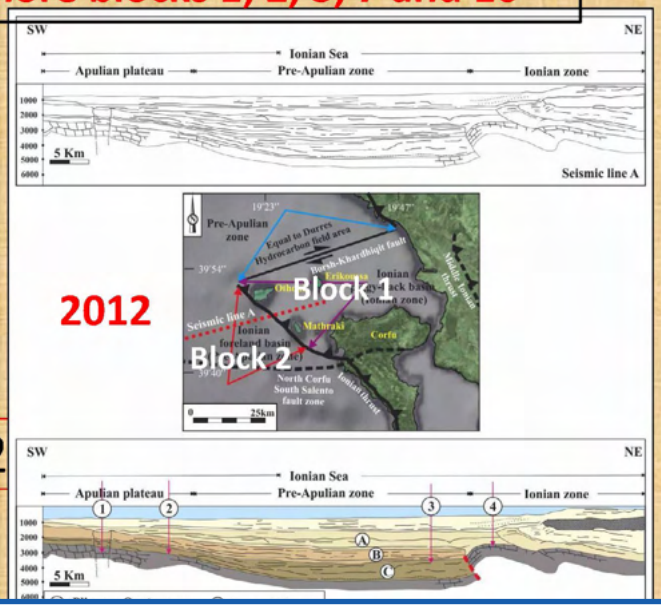
Potential **reservoir rocks** include 1. the Early Jurassic (Liassic) Pantokrator limestones, 2. the Early Cretaceous (Berriasian) Vigla limestones, 3. Upper Cretaceous (Senonian) limestones, 4. Paleocene – Eocene limestones, and 5. sand-rich intervals in the Eocene – Oligocene and post-Alpine successions.

Triassic evaporites have the best **seal potential**. However mud-rich intervals in the Eocene – Oligocene foreland basin succession, together with upper Miocene and Pliocene marls (e.g. the seals at the Katakolo oilfield) are also regarded as potential cap rocks. A closer evaluation of the details of seals in Albanian traps may determine which is more prevalent, either flysch or evaporites in assessing risk.

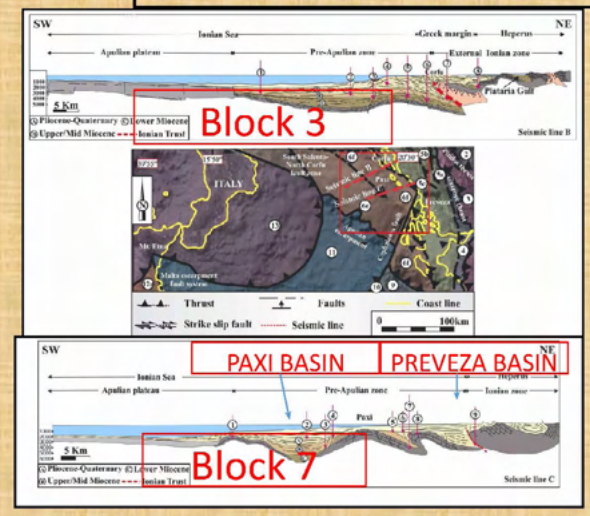
3. Offshore blocks 1, 2, 3, 7 and 10



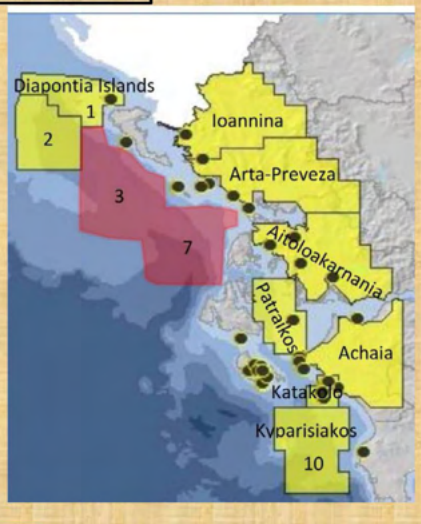
Blocks 1 & 2



Offshore blocks 3 and 7

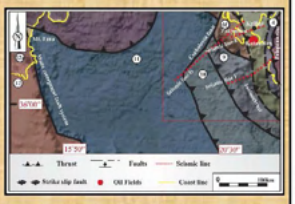


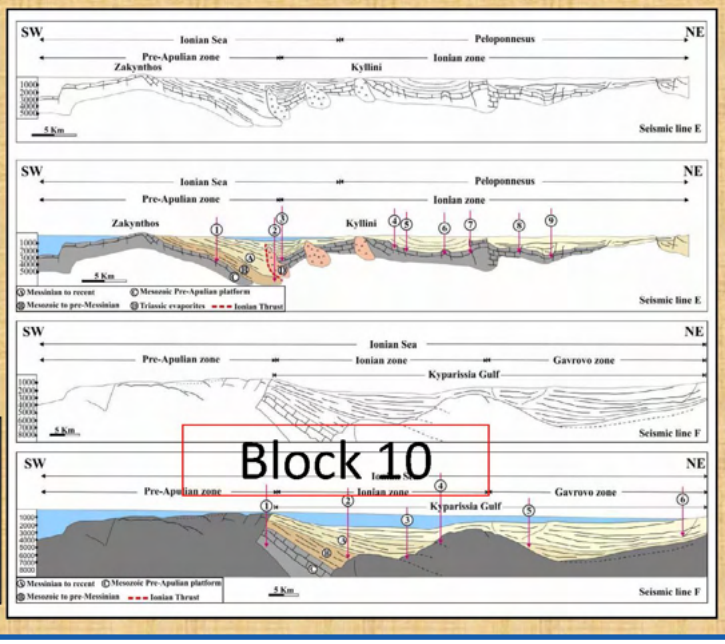
2012

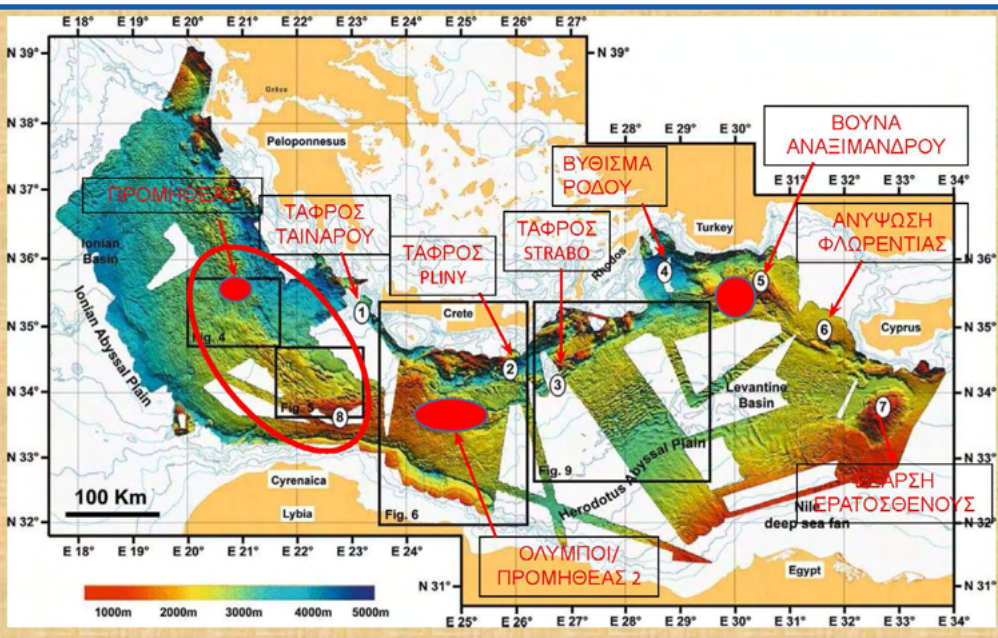


Maravelis et. al., 2012

Maravelis et. al., 2012 **2012**







Μορφο-βαθυμετρικός χάρτης της Μεσογείου, από MediMap Group, Loubrieu

Στη λεκάνη της Λεβαντίνης βρέθηκαν:

1.5 τρις μ3 φυσικού αερίου, από τα 3.4 τρις μ3 φυσικού αερίου που πρέπει να υπάρχουν και επίσης βρέθηκαν 3 δισ. βαρέλια αργού πετρελαίου από τα 1.8 δισ. βαρέλια που έλεγε η Αμερικανική Γεωλογική Υπηρεσία, το 2010.

Η Κύπρος βρήκε μόνο στο οικόπεδο 12 την **Αφροδίτη** (4.2 τρις TCF = 120 δις μ3) και την **Αθηνά** (8 τρις TCF = 220 δις μ3) που ανήκουν στα **δυτικά περιθώρια της λεκάνης της Λεβαντίνης.**

Στη λεκάνη του Ηροδότου και στο ανατολικό της Τμήμα στην ΑΟΖ της Κύπρου βρέθηκαν:

Γλαύκος (οικόπεδα 10, 5-8τρις TCF=140-220 δις m3), **Καλυψώ** (οικόπεδο 6, 10τρις TCF = 280 δις μ3), **Κρόνος 1** (οικόπεδο 6, 2.5 τρις TCF = 70 δις m3), **η νέα γεώτρησή Ζευς 1 (2-3 τρις TCF). στο ύβωμα του ΕΡΑΤΟΣΘΕΝΗ**

κοίτασμα Ονησίφορος στο οικόπεδο 11

Συνολικά στην ΝΑ Μεσόγειο βρέθηκαν 90 τρις TCF/35 = **2.3 τρις μ3.**

Κύπρος μέχρι τώρα: 18TCF = 600 δις m3,
Αίγυπτος: Ζορ, νότια του 11, 30τρις TCF = περίπου 1 τρις μ3,
Ισραήλ: Λεβιάθαν (22τρις TCF περίπου 600 δις μ3), Ταμάρ (7.1τρις TCF περίπου 200 δις μ3).

Στον Κώνο του Νείλου **βρέθηκαν μόνο <2 τρισ μ3 φυσικού αερίου, από τα 6.4 τρισ μ3** που θεωρείται ότι υπάρχουν.

Από τα κοιτάσματα που βρέθηκαν μέχρι σήμερα το Σύνολο του ανακαλυφθέντος βιογενούς φυσικού αερίου ανέρχεται σε 1.5 τρις μ3.

Στην ΑΟΖ της Κύπρου αναμένεται να υπάρχουν κατά την εταιρεία SPECTRUM, περίπου άλλα 3 τρις μ3 βιογενούς φυσικού αερίου.

Στη Μεσογειακή Ράχη, που αρχίζει από την Κεφαλονιά και τελειώνει στην Κύπρο δεν έχει γίνει μέχρι σήμερα γεώτρηση.

Στη Μεσογειακή Ράχη που βρίσκεται εντός της Ελληνικής ΑΟΖ εντοπίστηκαν από την ΕΔΕΥ το 2018:
26 κοραλλιογενείς ύφαλοι με μέγεθος ίσο η πολύ μεγαλύτερο, ακόμα και 4 φορές, του Ζορ.
Από αυτούς έχουν δοθεί 16 στόχοι στα ΕΛΠΕ που είναι δυτικά του κόλπου της Κυπαρισσίας, μπλοκ 10, και 14 και στην κοινοπραξία των Exxon-Mobil και ΕΛΠΕ, δυτικά και νοτιοδυτικά της Κρήτης.

Εκτιμάται ότι οι 16 στόχοι έχουν αθροιστικά 2.4 τρις μ3 βιογενούς φυσικού αερίου.

Το σήμερα και …. το ΑΥΡΙΟ

- Οι προϋποθέσεις της πολιτείας:

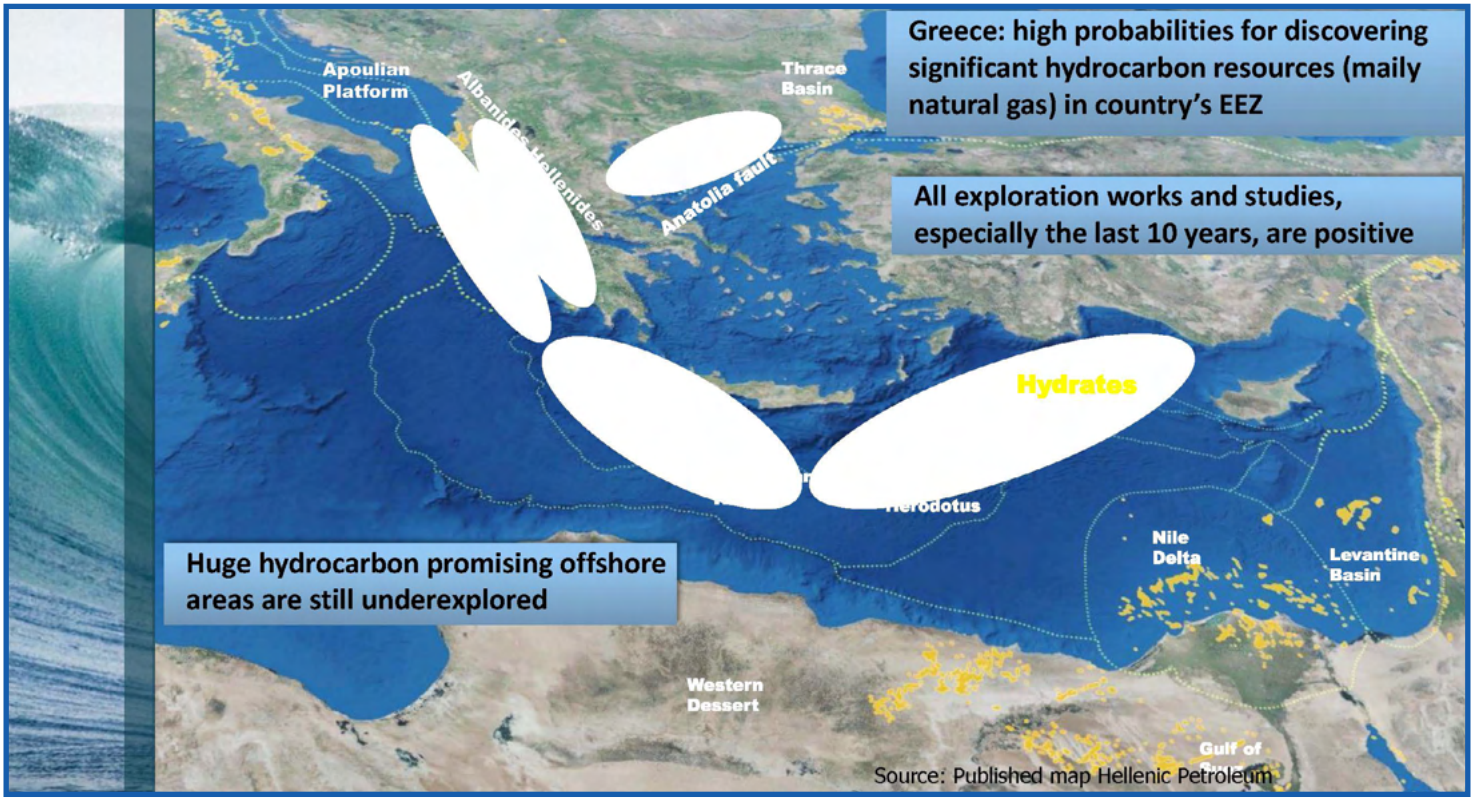
1. Ενεργοποιήθηκαν 6 περιοχές (5 θαλάσσιες και μια χερσαία) (οικόπεδα: 2, 3-7, 10, Δ και ΝΔ της Κρήτης + Γιάννενα)
2. Ψάχνουμε μόνο για αέριο
3. Θα έχουμε εικόνα από τα σεισμικά στο τέλος του 2023

- Τα ΔΕΝ και τα ΠΡΕΠΕΙ του αφηγήματος:

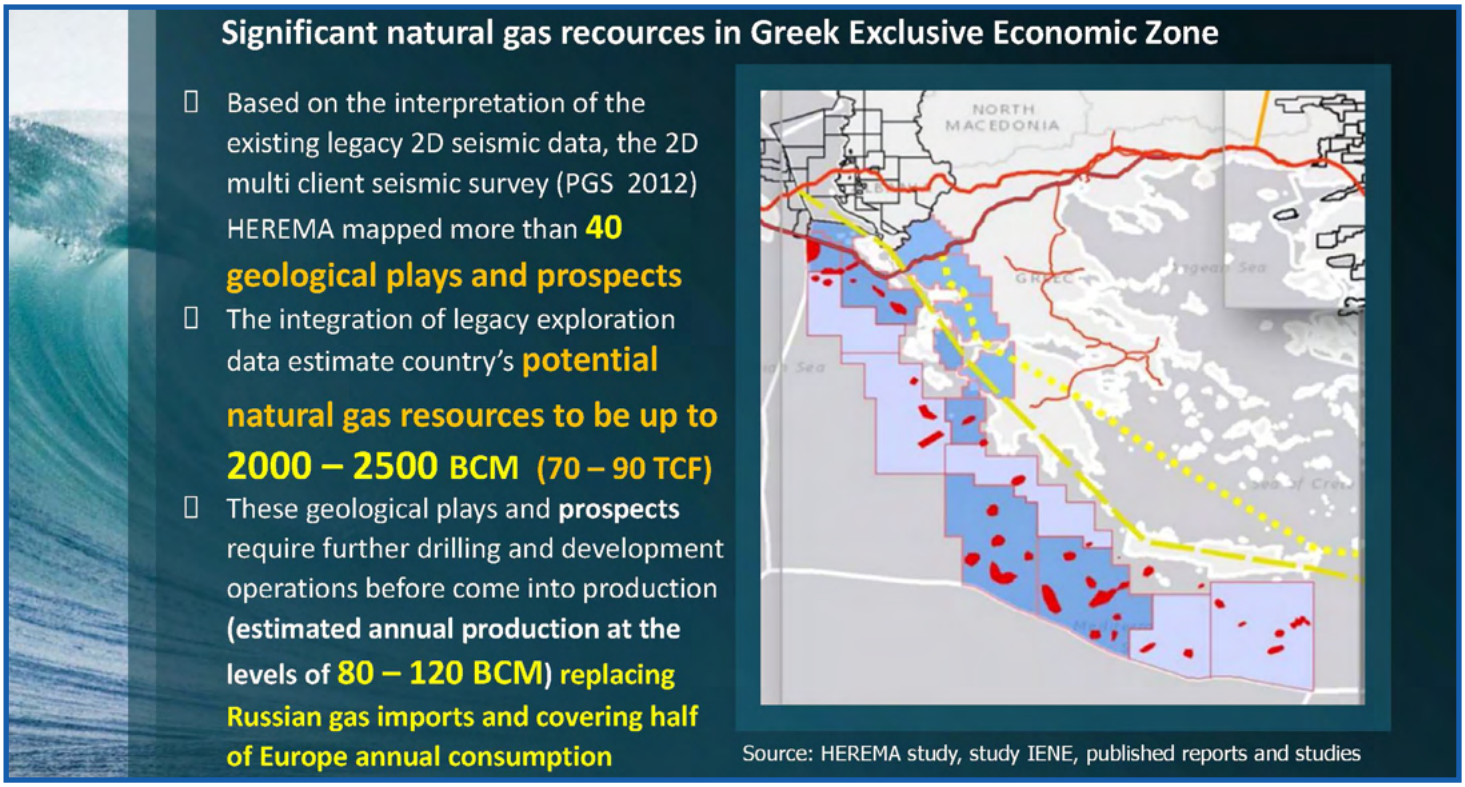
1. Εγκαταλείφθηκε ο Πατραϊκός αφού ΔΕΝ περιλαμβάνεται στο αφήγημα, γιατί έχει μόνο πετρέλαιο!!!! ΓΙΑΤΙ;;;; Ποια είναι η αλήθεια; ΔΕΝ υπάρχει αέριο; Δεν ήταν συμβασιοποιημένη η περιοχή;
2. Στα οικόπεδα 2, Δυτικά και Νοτιοδυτικά της Κρήτης… ολοκληρώθηκαν οι 3D σεισμικές έρευνες. Προσφυγές στο ΣτΕ με 4 αναβολές. Θα δούμε για το 2025?
3. Αν βρεθεί πετρέλαιο στα Γιάννενα; Ίδιες γεωλογικές συνθήκες με τον Πατραϊκό.
4. Αποχώρησαν οι μεγάλες εταιρείες (REPSOL, TOTAL). ΓΙΑΤΙ;
5. Οι ευθύνες του αφηγήματος μεταφέρθηκαν στην ΕΔΕΥ. Δηλαδή εγώ τους διώχνω (η εξουσία) και εσύ τους ξαναφέρνεις (η υπηρεσία μου!!)… ΑΛΙΜΟΝΟ
6. 2024: Έμμεση εγκατάλειψη του οικοπέδου 10 στον Κυπαρρισιακό (θα το μάθουμε σύντομα) ΓΙΑΤΙ θα οριοθετήσουμε θαλάσσιο πάρκο.
7. 2024: Θα εγκαταλείψουμε και το οικόπεδο στα Ιωάννινα γιατί δεν το θέλουν οι «προστάτες» του περιβάλλοντος και γιατί ξαφνικά θα μάθουμε ότι έχει πετρέλαιο.

Greek and Cypriot natural gas resources for stability, peace and prosperity of the countries in Europe and SE Med

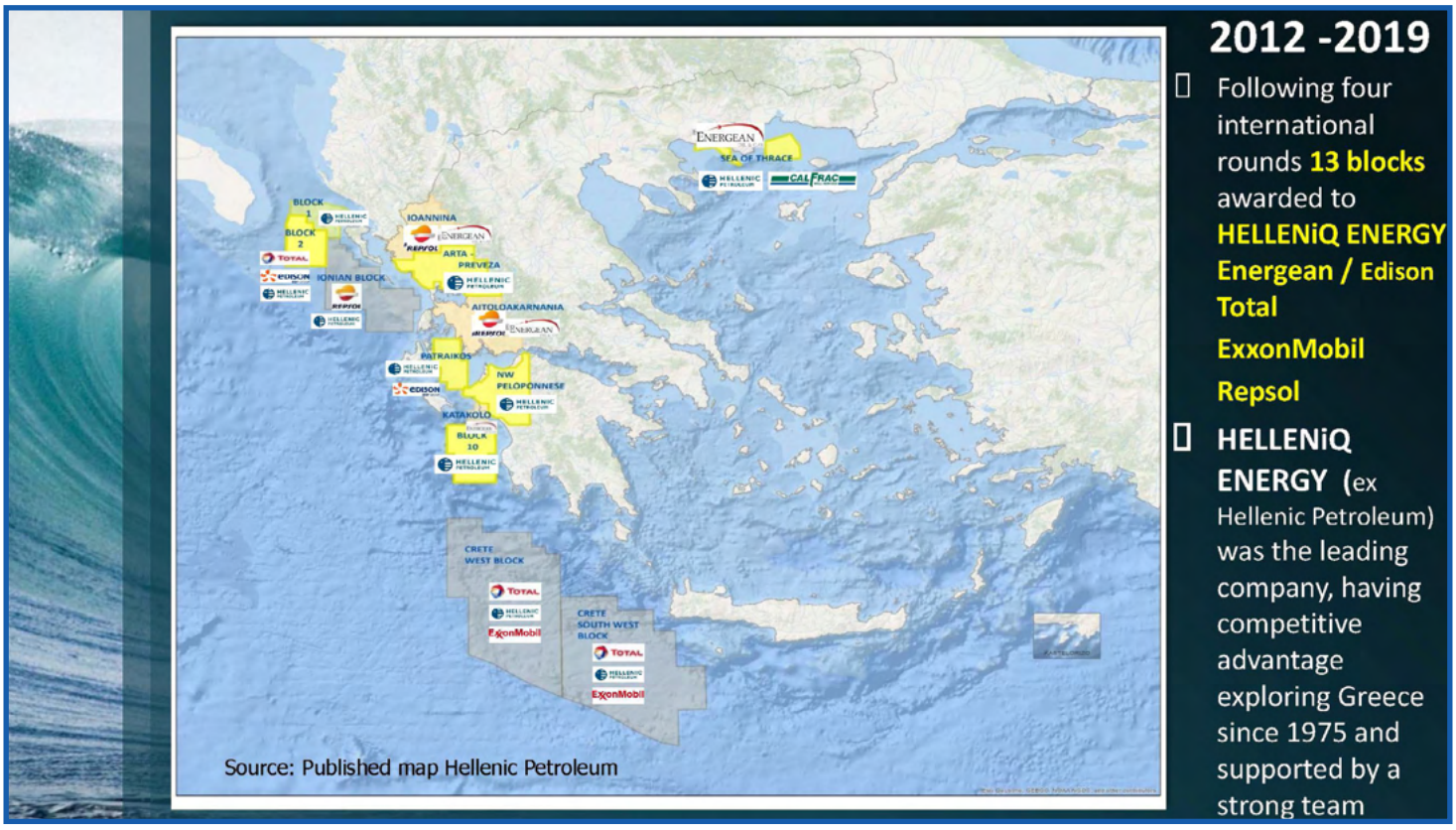
Yannis Grigoriou
IENE partner
VP Continental Europe Energy Council



Τα μέχρι σήμερα αποτελέσματα των ερευνών υδρογονανθράκων στην Ελλάδα, παρά τις όποιες παλινωδίες και καθυστερήσεις του Ελληνικού Δημοσίου, είναι απολύτως θετικά για την ύπαρξη σημαντικών κοιτασμάτων κυρίως φυσικού αερίου στο θαλάσσιο χώρο. Όλες ανεξαιρέτως οι δημοσιευθείσες μελέτες από πετρελαϊκές και τεχνικές εταιρείες, ακαδημαϊκούς φορείς και ινστιτούτα ταυτίζονται ότι είναι εφικτή η ανακάλυψη και παραγωγή κοιτασμάτων φυσικού αερίου σε ποσότητες που θα καλύπτουν όχι μόνο τις ανάγκες της χώρας αλλά θα είναι δυνατόν να καλύψουν πολύ μεγάλο ποσοστό από τις ανάγκες των ευρωπαϊκών χωρών, αντικαθιστώντας τις εισαγωγές φυσικού αερίου από την Ρωσία. Χαρακτηριστικά αναφέρονται πρόσφατες μελέτες της κρατικής αρχής ΕΔΕΥΕΠ για την καταγραφή περισσότερων από 25 γεωλογικών στόχων και του Ινστιτούτου Ενέργειας ΝΑ Ευρώπης (IENE) για εν δυνάμει αποθέματα φυσικού αερίου περίπου 2000 - 2500 BCM (ετήσια παραγωγή 80-100 BCM) στις θαλάσσιες περιοχές Ιονίου πελάγους, πέριξ της Κρήτης, Θερμαϊκού κόλπου κλπ.

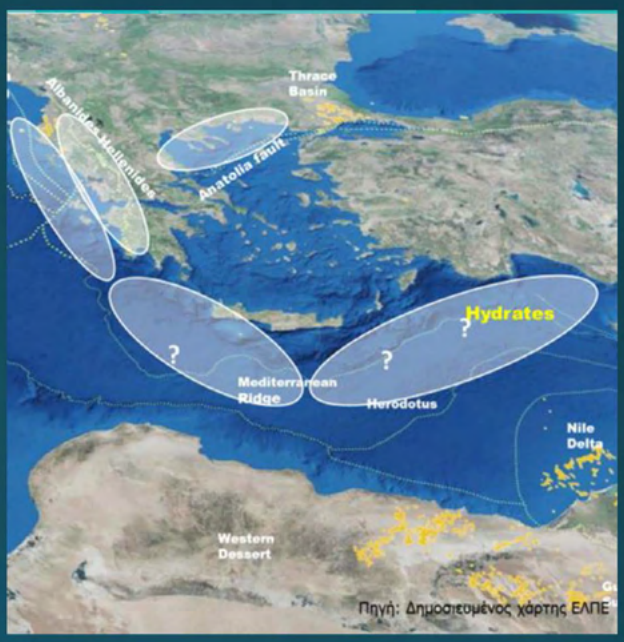


Οι έρευνες επικεντρώνονται σήμερα σε περιοχές του Ιονίου, της Κρήτης και της Ηπείρου, από σημαντικές εταιρείες (ExxonMobil, Energean, HellenIQ Energy), οι οποίες με βάση τα αποτελέσματα γεωλογικών και γεωφυσικών δισδιάστατων και τρισδιάστατων σεισμικών ερευνών είναι πολύ κοντά να προσδιορίσουν θέσεις γεωτρήσεων που θα εκτελεστούν τα επόμενα δύο – τρία χρόνια. Παράλληλα η αγορά περιμένει το έμπρακτό ενδιαφέρον από το Ελληνικό Δημόσιο με την προκήρυξη νέων περιοχών για έρευνα και την υποστήριξη των τρεχουσών ερευνητικών εργασιών.

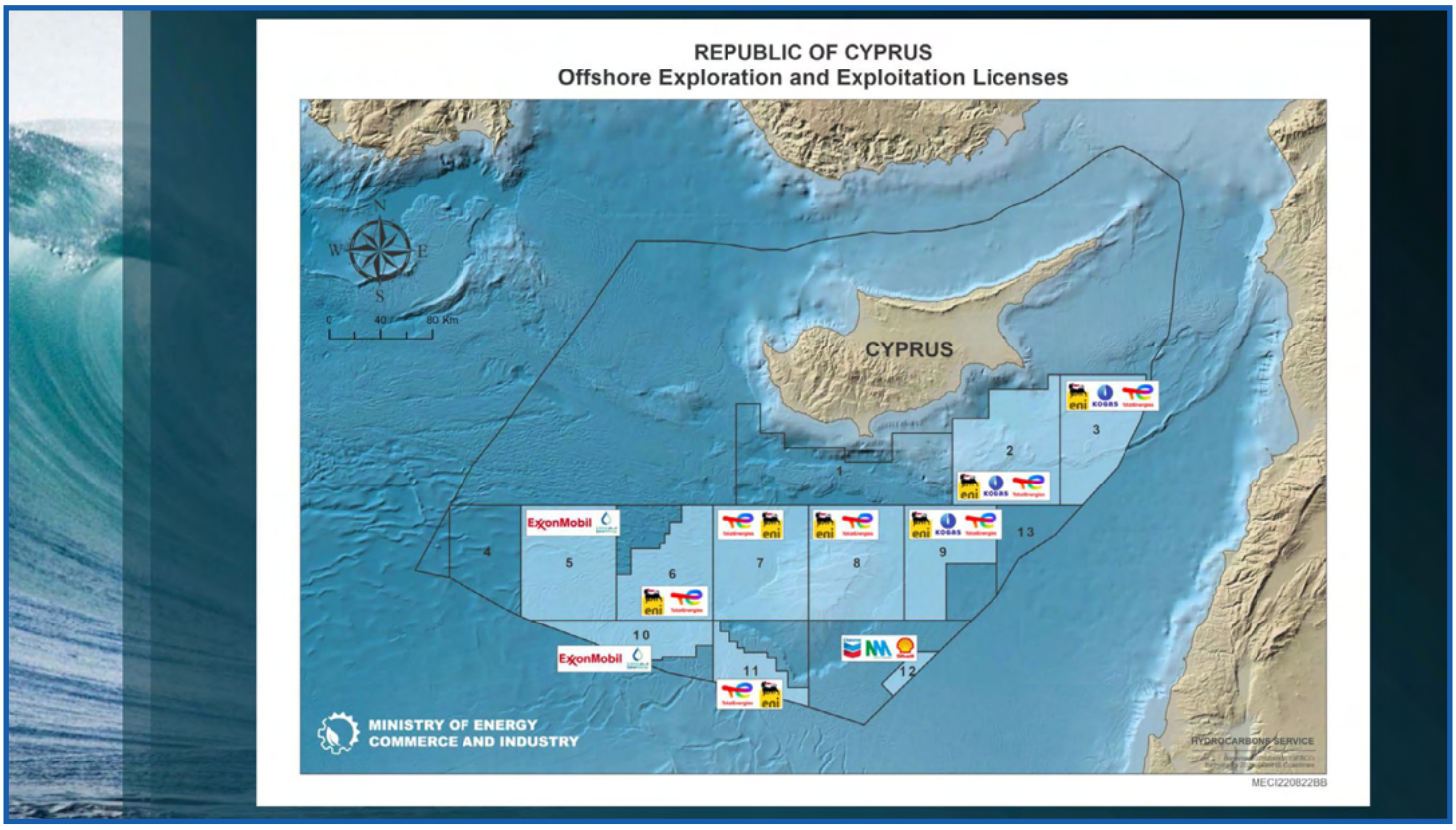


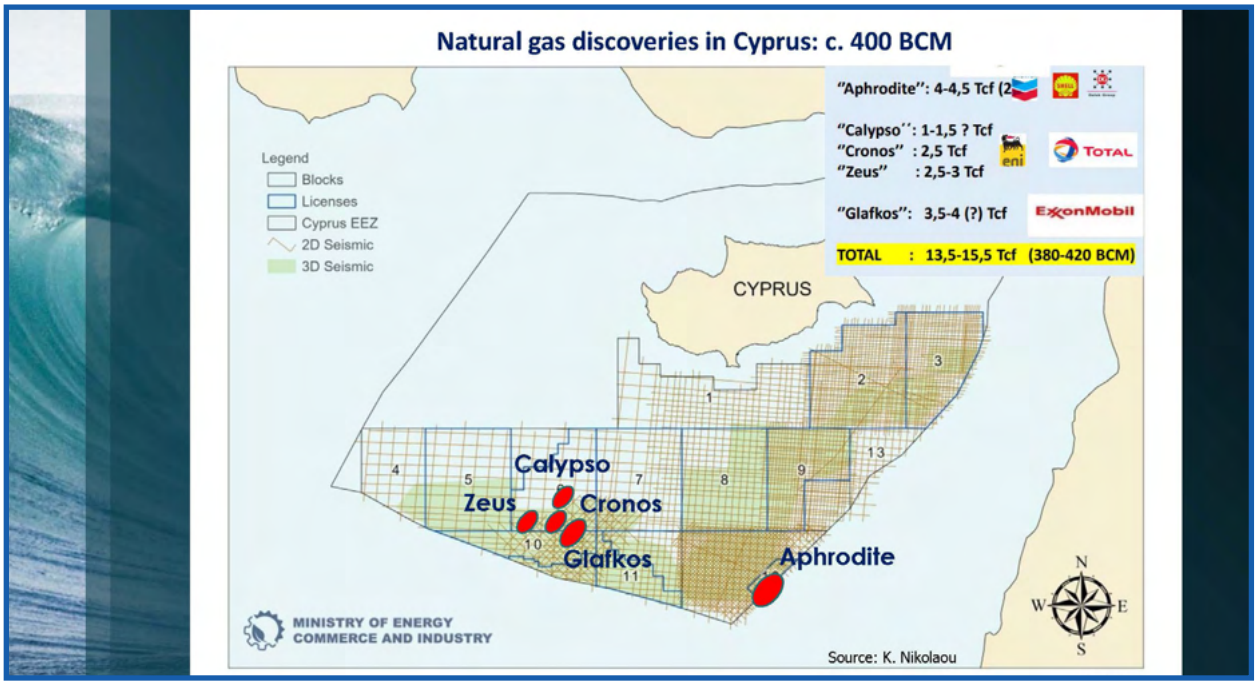
Market is expecting Greek State to continue supporting exploration

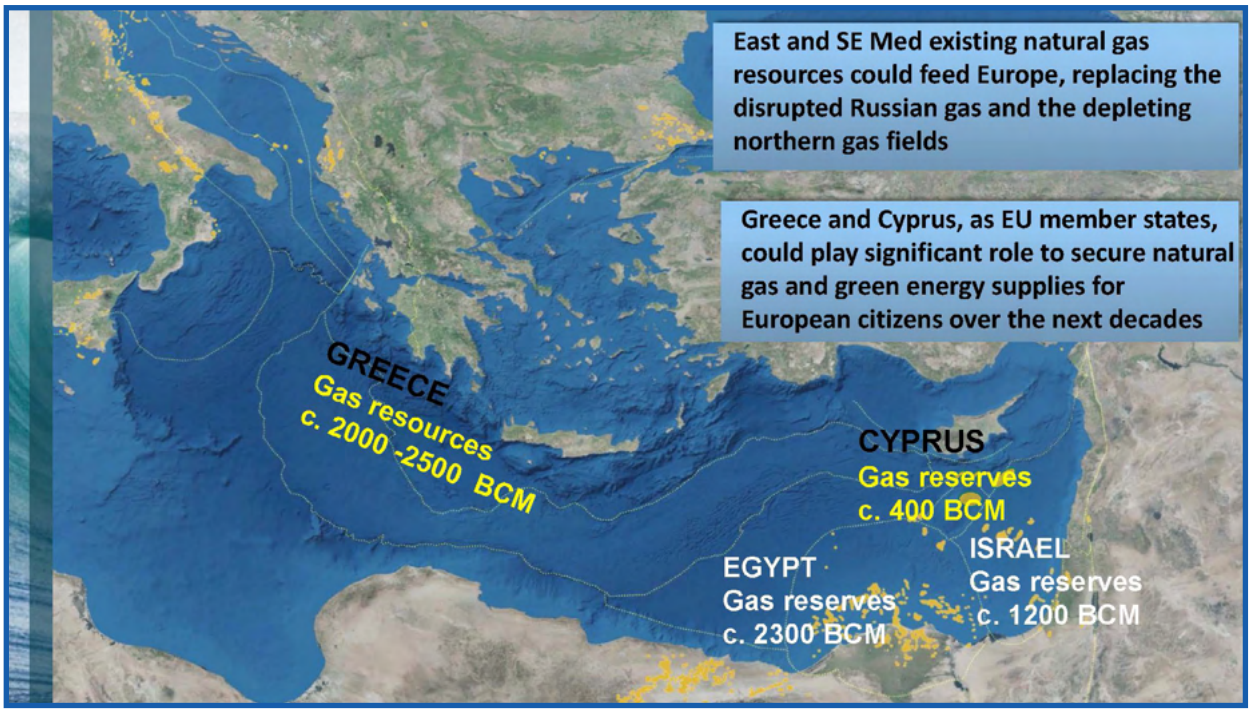
- **PM** two years ago (April 2022) **encouraged oil companies to proceed exploration** works declaring that the relevant projects will be of "national interest"
- **Numerous oil companies** (supermajors and independent Europeans) **are interested to enter the country** looking for farm in existing blocks and/or new acreage opportunities
- ***Lack of continuity and consistency***
  Contradicting statements from the government: no oil production will be allowed – **no more acreage** will be explored – **new offshore natural parks** are on licensed areas (block 10)
- **Greek State did not proceed to release new acreage** as it was declared since 2019 (new rounds – open door procedure) either in N. Aegean or in W. Greece

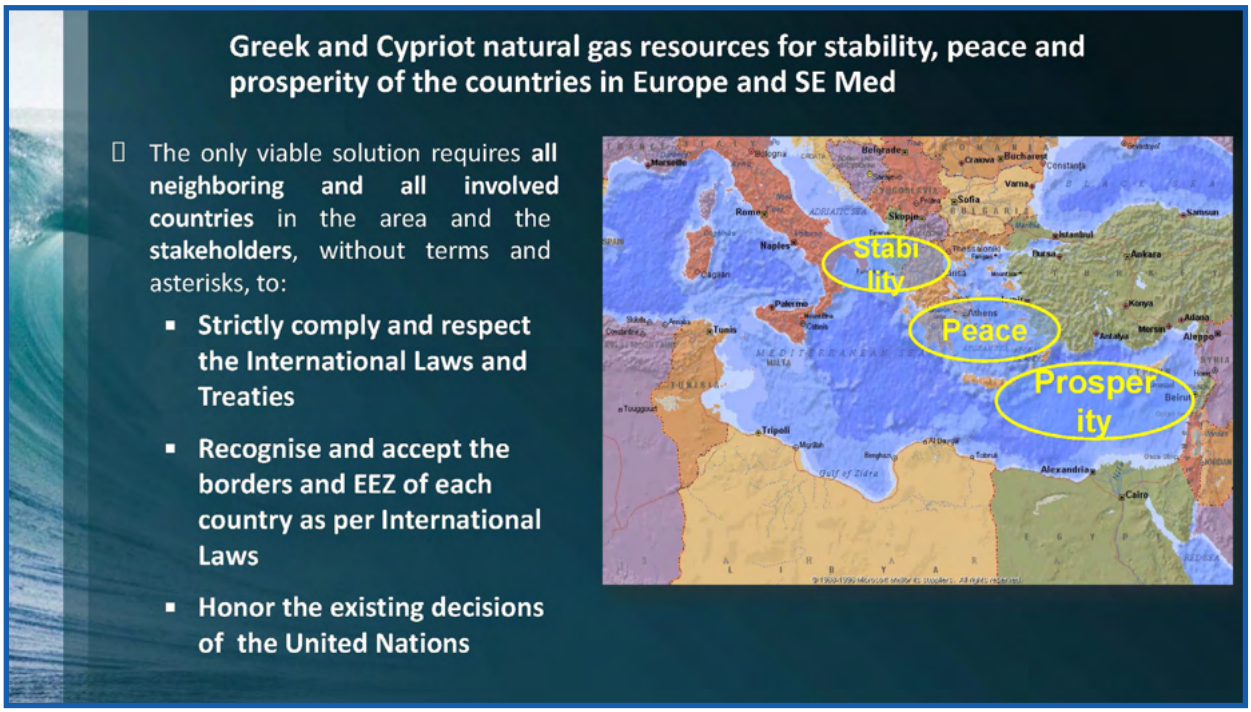


Εντέλει η περιοχή της ΝΑ Μεσογείου, με τα ήδη ανακαλυφθέντα κοιτάσματα φυσικού αερίου σε Κύπρο, Αίγυπτο, Ισραήλ και τις αναμενόμενες ανακαλύψεις και στον Ελλαδικό χώρο, είναι σε θέση να αναδειχθεί σε ενεργειακό τροφοδότη της ευρύτερης περιοχής και της Ευρωπαϊκής Ένωσης με το φυσικό αέριο, ως μεταβατικό καύσιμο οδεύοντας προς τους στόχους της απανθρακοποίησης του 2050.




Natural gas discoveries in Cyprus: c. 400 BCM
"Aphrodite": 4-4,5 Tcf (2
"Calypso": 1-1,5 ? Tcf
"Cronos" : 2,5 Tcf
"Zeus" : 2,5-3 Tcf
"Glafkos": 3,5-4 (?) Tcf
TOTAL : 13,5-15,5 Tcf (380-420 BCM)
Legend
Blocks
Licenses
Cyprus EEZ
2D Seismic
3D Seismic
CYPRUS
Calypso
Zeus
Cronos
Glafkos
Aphrodite
MINISTRY OF ENERGY COMMERCE AND INDUSTRY
Source: K. Nikolaou


East and SE Med existing natural gas resources could feed Europe, replacing the disrupted Russian gas and the depleting northern gas fields
Greece and Cyprus, as EU member states, could play significant role to secure natural gas and green energy supplies for European citizens over the next decades
GREECE
Gas resources
c. 2000 -2500 BCM
CYPRUS
Gas reserves
c. 400 BCM
ISRAEL
Gas reserves
c. 1200 BCM
EGYPT
Gas reserves
c. 2300 BCM


Greek and Cypriot natural gas resources for stability, peace and prosperity of the countries in Europe and SE Med
The only viable solution requires all neighboring and all involved countries in the area and the stakeholders, without terms and asterisks, to:
Strictly comply and respect the International Laws and Treaties
Recognise and accept the borders and EEZ of each country as per International Laws
Honor the existing decisions of the United Nations
Stabi lity
Peace
Prosper ity

Μέντορες επιχειρηματικότητας

Ηλίας Καλλίτσης

- Project manager και market operations στην Toyota Material Handling Europe
- Προσφέρει καθοδήγηση σε όσους πραγματοποιούν τα πρώτα τους βήματα στην αγορά εργασίας ή ήδη εργάζονται
- Βέλγιο

Δανιήλ Σουριανός

- Technology Consultant στην KPMG
- Προσφέρει καθοδήγηση σε νέους με STEM ενδιαφέρον και Seed Start-Ups
- Κύπρος

Άγγελος Κότιος

- Πρώην Πρύτανης Πανεπιστημίου Πειραιώς
- Παροχή συμβουλών σε όσους επαγγελματίες ενδιαφέρονται να ξεκινήσουν επιχειρηματικές δραστηριότητες και επιχειρηματίες, ιδιοκτήτες επιχειρήσεων ή διευθυντές που αναζητούν νέα χρηματοδοτικά εργαλεία για την προώθηση της επιχείρησής τους ή των καινοτόμων δραστηριοτήτων τους.
- Ελλάδα

Ζωή Παπαχαράλαμπους

- Ιδρυτής και Πρόεδρος της LDK Consultants
- Προσφέρει συμβουλές σε νέους επαγγελματίες που αναζητούν ευκαιρίες για εργασία και επιχειρηματίες που αισθάνονται την ανάγκη να συζητήσουν για την επαγγελματική τους πορεία και την πιθανή αλλαγή σταδιοδρομίας
- Ελλάδα

Μέντορες σπουδών και καριέρας

Κλημεντίνη Διακομανώλη

- Στέλεχος της Ευρωπαϊκής Επιτροπής
- Συμβουλές σε νέους που σπουδάζουν ή ασχολούνται με την Επικοινωνία
- Βέλγιο

Παναγιώτης Καλαβρός

- Talent Acquisition Specialist στο NATO
- Προσφέρει καθοδήγηση σε νέους που σκέφτονται την αλλαγή καριέρας
- Βέλγιο

Ροδούλα Τρακάδα

- Υπεύθυνη Marketing στη JDE Peet's
- Προσφέρει συμβουλές σε όσους θέλουν να απασχοληθούν στον τομέα του Marketing και σε επαγγελματίες που θέλουν να χρησιμοποιήσουν marketing εργαλεία για την προώθηση των δραστηριοτήτων τους
- Ελλάδα

Άλκης Σταυρίδης

- Σύμβουλος επιχειρήσεων στην ΑΙΧΜΗ Α.Ε.
- Προσφέρει καθοδήγηση σε νέους και εν δυνάμει επιχειρηματίες
- Ελλάδα

Μέντορες καριέρας

Δημήτρης Γούλιας

- Οικονομικός Αναλυτής στη SEVE Greek Exporters' Association
- Προσφέρει καθοδήγηση σε όσους αναζητούν μία διεθνή καριέρα, σχετικά με τον τομέα της Βιομηχανίας 4.0
- Ελλάδα

Ελένη Μπουλαμάτση

- Σύμβουλος ψυχικής υγείας και καριέρας στις Mikrokosmos
- Προσφέρει καθοδήγηση σε νέους που δραστηριοποιούνται στις εξωτερικό
- Ιταλία

Αναστασία Ρωμανού

- Ερευνήτρια στη NASA
- Προσφέρει συμβουλές για νέους που θέλουν να αποκτήσουν μία καριέρα στις ΗΠΑ
- ΗΠΑ

Κώνσταντίνος Σαχπάζης

- Επίκουρος Καθηγητής στο Ελληνικό Ανοικτό Πανεπιστήμιο
- Προσφέρει καθοδήγηση σε μηχανικούς και φοιτητές που θέλουν να προχωρήσουν τις ακαδημαϊκές τους σπουδές
- Ελλάδα

Young mentors

Μαρία Χριστοφίλη

- Δικηγόρος στο Ελληνικό Κοινοβούλιο
- Προσφέρει καθοδήγηση σε νέους στους τομείς προσωπικής ανάπτυξης και αναζήτηση καριέρας
- Ελλάδα

Πασχάλης Σταμπούλης

- Ειδικός στο Τμήμα Ανάπτυξης Ανθρώπινου Δυναμικού στην OTE Group of Companies (HTO)
- Προσφέρει καθοδήγηση σε νέους απόφοιτους, που αναζητούν το πρώτο τους βήμα στον επιχειρηματικό κόσμο και φοιτητές που προσπαθούν να κατανοήσουν την αγορά και ποια επαγγελματική πορεία να ακολουθήσουν
- Ελλάδα

George Raskovic

- Σύμβουλος Επιχειρήσεων στην Παγκόσμια Τράπεζα
- Προσφέρει καθοδήγηση σε οποιονδήποτε ενδιαφέρεται να ακολουθήσει μια εκπαιδευτική και/ή επαγγελματική πορεία στη Νομική, ειδικά όσοι ενδιαφέρονται για το δίκαιο της ΕΕ και το δίκαιο του ανταγωνισμού
- Ελλάδα

Νικόλας Βαρβέρης

- Ως Certified Senior Coach, Certified Adult Lifelong Learning Trainer και Start upper προσφέρει καθοδήγηση σε νέους επαγγελματίες και φοιτητές που ενδιαφέρονται να κάνουν καριέρα στη Διοίκηση και Ανάπτυξη Επιχειρήσεων
- Ελλάδα

Αντί Επιλόγου
Θέτοντας προτεραιότητες στον ωκεανό των υποχρεώσεων

Χρήστος Μπεζιρτζόγλου
Μέντορας Καριέρας ΑΛΛΗΛΟΝ
Στέλεχος Ευρωπαϊκής Επιτροπής
Christos Bezirtzoglou | Linkedin

Περίληψη

Το ερώτημα που θέτουμε συχνά στον εαυτό μας είναι « Πώς μπορούμε να βάλουμε σε σειρά τις υποχρεώσεις, τις ανάγκες και τις επιλογές μας; » Η απάντηση είναι να φτιάξουμε ένα προσωπικό στρατηγικό πλάνο και να χρησιμοποιήσουμε τα κατάλληλα εργαλεία διαχείρισης προτεραιοτήτων σε ατομικό επίπεδο, ως μέλη μιας ομάδας και ως ηγετικά στελέχη.

Θα ξεκινήσω αναφέροντας ένα απόσπασμα από την ομιλία του Brian Dyson στο Georgia Tech Institute στις 6 Σεπτεμβρίου 1991 που μίλησε μεταφορικά για τις «πέντε μπάλες της ζωής».

"Φανταστείτε τη ζωή σαν ένα παιχνίδι που κάνετε ταχυδακτυλουργικά με πέντε μπάλες που πετάτε στον αέρα προσπαθώντας να μην πέσουν. Οι πέντε μπάλες είναι: η εργασία, η οικογένεια, η υγεία, οι φίλοι, και το πνεύμα.

Σύντομα θα καταλάβετε ότι η εργασία είναι μια λαστιχένια μπάλα. Εάν σας πέσει από τα χέρια, απλώς θα αναπηδήσει.

Αλλά οι άλλες τέσσερις μπάλες - οικογένεια, υγεία, φίλοι και πνεύμα - είναι κατασκευασμένες από γυαλί. Εάν σας πέσει μια από τις γυάλινες μπάλες, αμετάκλητα θα γδαρθεί, θα χαραχθεί, θα ραγίσει, θα καταστραφεί, ή ακόμα και θα θρυμματιστεί. Δεν θα είναι ποτέ πια ίδιες.

Αυτό πρέπει να το συνειδητοποιήσετε και να επιδιώκετε να ζήσετε μια ισορροπημένη ζωή".

Έχοντας ως οδηγό αυτήν την μεταφορά οφείλουμε να προσπαθούμε για αρμονία και ισορροπία στη ζωή μας, δημιουργώντας το προσωπικό στρατηγικό πλάνο μας για προσωπική ανάπτυξη και επαγγελματική επιτυχία.

Μια άλλη τεχνική αυτοβελτίωσης, που στοχεύει στην προσωπική μας εξέλιξη - μιας και όλες οι αλλαγές εκπορεύονται από εμάς τους ίδιους, είναι ο « Τροχός της Ζωής » (Wheel of Life). Είναι μια οικεία έννοια σε πολλούς θρησκευτικούς και πνευματικούς πολιτισμούς, που αντιπροσωπεύει τη συνεχή κίνηση & αλλαγή στη ζωή και σχηματοποιείτε με έναν τροχό/κύκλο χωρισμένο σε οκτώ τομείς στα οποία το άτομο τοποθετεί τις οκτώ κορυφαίες προτεραιότητες που

ισχύουν στη ζωή του. Αυτοί οι τομείς είναι: Υγεία & Ευεξία, Αγάπη & Συντροφικότητα, Οικονομικά & Τρόπος ζωής, Προσωπική ανάπτυξη & Πνευματικότητα, Διασκέδαση & Προσωπικός χρόνος, Περιβάλλον & Κοινωνική προσφορά, Οικογένεια & Φίλοι, και τέλος Εργασία & Καριέρα.

Με την τεχνική αυτή μπορούμε να δούμε έναν προς έναν και συνολικά όλους τους τομείς της ζωής μας και να συνειδητοποιήσουμε πού αφιερώνουμε παραπάνω ή λιγότερη ενέργεια και χρόνο. Όλοι οι τομείς είναι αλληλένδετοι και αλληλεπιδρούν μεταξύ τους. Όταν κάτι δεν πάει καλά σε ένα τομέα, αργά ή γρήγορα θα επηρεαστούν και οι υπόλοιποι. Τότε χάνεται η ισορροπία.

Καθορίστε τους στόχους σας και επιλέξτε τις στρατηγικές σας

Η λίστα υποχρεώσεων σας φαίνεται ατελείωτη; Δεν χρειάζεστε περισσότερες ώρες την ημέρα αλλά να ιεραρχήσετε στρατηγικά τις προτεραιότητες σας, ανεξαρτήτως ποιας τεχνικής θα χρησιμοποιήσετε!

Ποιες από τις δικές σου "μπάλες της ζωής" είναι άθραυστες/λαστιχένιες και ποιες εσύ θεωρείς ότι είναι εύθραυστες/γυάλινες; Η λαϊκή σοφία λέει χαρακτηριστικά: Να έχουμε την υγειά μας και όλα θα γίνουν. Με άλλα λόγια θεωρεί ότι, εκτός από την υγεία, οι υπόλοιπες τέσσερεις μπάλες δεν είναι τόσο εύθραυστες. Πόσες φορές ανταπεξήλθαμε σε προσωπικές ή/και επαγγελματικές δυσκολίες, πόσες φορές πέσαμε και ξανασηκωθήκαμε, γιατί επιδείξαμε δύναμη ψυχής και εγρήγορση ώστε να θωρακίσουμε τις αδυναμίες (εύθραυστες μπάλες) μας.

Συμπερασματικά θα πρέπει να διαχειριζόμαστε τα επαγγελματικά μας προβλήματα αποτελεσματικά κατά τη διάρκεια των ωρών εργασίας, να αφιερώνουμε χρόνο με την οικογένειά που αγαπάμε και για να συναναστραφούμε με τους φίλους μας, και τέλος να διαθέσουμε χρόνο ώστε να ξεκουραστούμε φροντίζοντας την σωματική και πνευματική μας υγεία.

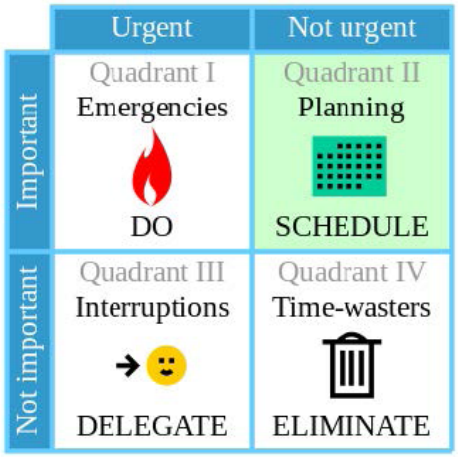
Πως μπορούμε να μοιράζουμε τον χρόνο μας ανάμεσα στους οχτώ τομείς του "τροχού της ζωής"; Για να αισθανόμαστε ισορροπία στη ζωή μας, είναι απαραίτητο να μοιράζουμε τον χρόνο μας με βάση το τι είναι σημαντικό για εμάς προσωπικά. Δεν χρειάζεται ο χρόνος να μοιράζεται ισομερώς μεταξύ των τομέων, αλλά να μην παραβλέπουμε για καιρό κάποιον. Το τι είναι σημαντικό για εμάς καθορίζεται από τους στόχους. Εάν δεν έχεις στόχους, δεν μπορείς και να κάνεις ιεράρχηση προτεραιοτήτων.[1]

Το πρόβλημα, όταν δεν υπάρχει προσωπική στρατηγική και τα κατάλληλα εργαλεία, είναι ότι οι άνθρωποι δεν μπορούν να κάνουν ρεαλιστική εκτίμηση του χρόνου και υπερεκτιμούν τις δυνατότητές τους, με αποτέλεσμα να στριμώχνουν υπερβολικά τη μέρα τους με ατέλειωτες λίστες εκκρεμών εργασιών. Το αποτέλεσμα είναι ότι είτε δεν τα προλαβαίνουν (επομένως μένουν με ένα αίσθημα ανεπάρκειας και ανικανότητας), είτε τρέχουν να τα προλάβουν και εξοντώνονται φυσικά και πνευματικά (με αποτέλεσμα να παθαίνουν κρίσεις πανικού, σύνδρομο εργασιακής εξάντλησης ή/και άλλα προβλήματα υγείας).

Εργαλεία διαχείρισης προτεραιοτήτων

Θα παρουσιάσουμε ακολούθως τα δύο καλύτερα εργαλεία για καθεμιά από τις τρεις διαφορετικές καταστάσεις (ως άτομα, ως ομάδα και ως ηγέτες) που θα χρειαστεί να θέσουμε προτεραιότητες.

Ατομικά μπορούμε να χρησιμοποιήσουμε τον « Αρχή του Αϊζενχάουερ » ή την « Μέθοδο 3-3-3 ».



Ο **Αρχή του Αϊζενχάουερ** είναι μια μέθοδος που χρησιμοποιεί τις αρχές της Σημαντικότητας (Important) και του Επείγοντος (Urgent) για την οργάνωση προτεραιοτήτων και φόρτου εργασίας. Οι εργασίες αξιολογούνται χρησιμοποιώντας τα κριτήρια Σημαντικό/Ασήμαντο και Επείγον/Μη επείγον, στη συνέχεια τοποθετούνται στα τέσσερα τεταρτημόρια ενός πίνακα αποφάσεων και αντιμετωπίζονται ως εξής:

1. *Σημαντικές και Επείγουσες* εργασίες (Emergencies -> Do) γίνονται άμεσα από εμάς τους ίδιους.
2. *Σημαντικές αλλά Μη επείγουσες εργασίες* προγραμματίζονται (Planning -> Schedule) σε εύθετο χρόνο για να γίνουν από εμάς τους ίδιους.
3. *Τα Ασήμαντα αλλά Επείγοντα* καθήκοντα ανατίθενται (Interruptions -> Delegate) σε τρίτους.
4. *Οι Μη σημαντικές και Μη επείγουσες εργασίες* απορρίπτονται (Time-wasters -> Eliminate).

Η **Μέθοδος 3-3-3** του Oliver Burkeman είναι μια τεχνική διαχείρισης χρόνου που μπορεί να βοηθήσει στην ενίσχυση της παραγωγικότητας με ιεράρχηση μεταξύ των εργασιών, εξισορροπώντας περιόδους έντονης εστίασης για δύσκολες θεματικές με ευκολότερες εργασίες και δραστηριότητες ρουτίνας. Ακολουθώντας αυτήν τη μέθοδο, θα μεγιστοποιήσετε την παραγωγικότητας διατηρώντας παράλληλα μια αίσθηση τάξης κατά την διάρκεια της εργάσιμης ημέρα σας.

1. **Τρείς Ώρες για Σοβαρή Δουλειά**: Ξεκινήστε την εργάσιμη ημέρα σας αφιερώνοντας τρεις ώρες σοβαρής δουλειάς για τα πιο σημαντικά καθήκοντά σας. Κατά τη διάρκεια αυτής της περιόδου, εστιάστε την ενέργειά σας αποκλειστικά στην εργασία που έχετε να ολοκληρώσετε, αποφεύγοντας περισπασμούς όπως μηνύματα ηλεκτρονικού ταχυδρομείου, τηλεφωνήματα ή συνομιλίες. Η εργασία αυτού του είδους μπορεί να αποφέρει σημαντική αύξηση της παραγωγικότητας.
2. **Τρεις Επείγουσες Εργασίες**: Μετά την αρχική εντατική τρίωρη συνεδρία εργασίας, αποπερατώστε τρεις άλλες επείγουσες εργασίες που δεν απαιτούν τόσες ώρες έντονης εστίασης. Αυτές μπορεί να είναι σύντομες εργασίες που παραμένουν στη λίστα υποχρεώσεων σας. Αντιμετωπίζοντάς αυτές τις εκκρεμότητες έγκαιρα, θα διατηρήσετε τη δυναμική και θα αυξήσετε την παραγωγικότητα σας.
3. **Τρεις Εργασίες Συντήρησης**: Ολοκληρώστε την ημέρα σας διαθέτοντας χρόνο για τρεις εργασίες «συντήρησης». Αυτές μπορεί να περιλαμβάνουν δραστηριότητες όπως απάντηση ηλεκτρονικών μηνυμάτων χαμηλής προτεραιότητας ή προγραμματισμός επόμενων εργασιών. Χρησιμοποιήστε αυτή την χρονική περίοδο για να αποπερατώσετε τις τελευταίες μικρές εκκρεμότητες αλλά και για να οργανωθείτε για την επόμενη ημέρα.

Στα πλαίσια μιας ομάδας μπορούμε να χρησιμοποιήσουμε την « Μέθοδο ABCDE » ή τους « Πίνακες Kanban ».

Η **Μέθοδος ABCDE** του Brian Tracy είναι μια τεχνική για την ιεράρχηση των εργασιών και την αποτελεσματική διαχείριση του χρόνου σας (αποφυγή περισπασμών), που θα σας βοηθήσει να εστιάσετε σε αυτά που πραγματικά έχουν σημασία (στις εργασίες με την μέγιστη προτεραιότητα), με αποτέλεσμα να γίνεται πιο αποδοτικοί (effective) και πιο αποτελεσματικοί (efficient).

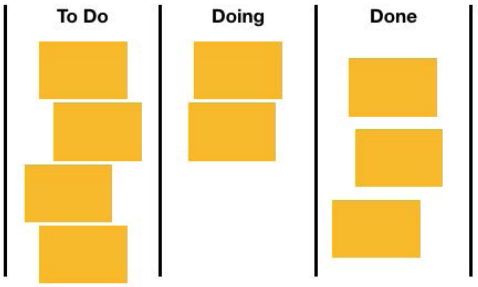
1. **A τύπου εργασία (Μέγιστη προτεραιότητα)**:
- Πολύ σημαντικά καθήκοντα για τα οποία θα υπάρξουν *σοβαρές συνέπειες* αν δεν γίνουν στην ώρα τους.

2. **Β τύπου εργασία (Υποχρεωτικά να γίνουν)**:
- Οι εργασίες τύπου Β είναι σημαντικές, αλλά έχουν *ήπιες συνέπειες* εάν δεν ολοκληρωθούν εγκαίρως.
- Ποτέ μην κάνετε μια εργασία τύπου Β όταν υπάρχει μια εργασία τύπου Α που δεν έχει ολοκληρωθεί.

3. **C τύπου εργασία (Χρήσιμο να γίνουν)**:
- Αυτού του τύπου οι εργασίες *δεν έχουν συνέπειες* είτε τις κάνετε είτε όχι.
- Δεν πρέπει να ασχοληθείτε με μια εργασία τύπου C εάν υπάρχουν εργασίες τύπου Β ή Α σε εκκρεμότητα.

4. **D (Delegate) Ανάθεση σε μέλος της ομάδας**:
- Ο κανόνας είναι να αναθέσετε όποιες εργασίες μπορείτε σε άλλο ή/και άλλα μέλη της ομάδας (που θα μπορούν να χειριστούν αποτελεσματικά) για να ελευθερώσετε δικό σας χρόνο που θα μπορέσετε να τον διαθέσετε για πιο κρίσιμες εργασίες.

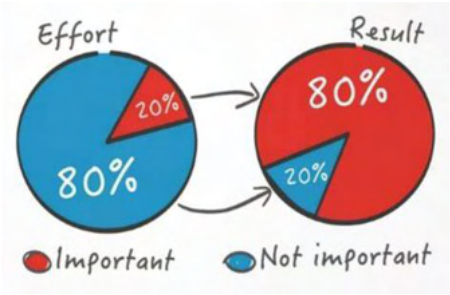
5. **E (Eliminate) Εξάλειψη**:
- Σκεφτείτε εάν ορισμένες εργασίες μπορούν να εξαλειφθούν εντελώς χωρίς αρνητικές συνέπειες. Βελτιστοποιείτε έτσι την διαχείριση και του δικού σας χρόνου και των μελών της ομάδας σας.



Οι **Πίνακες Kanban** απεικονίζουν οπτικά την εργασία στα επιμέρους διακριτά στάδια μιας διαδικασίας, χρησιμοποιώντας κάρτες για την αναπαράσταση της εργασίας και στήλες για την αναπαράσταση κάθε σταδίου της διαδικασίας. Οι κάρτες μετακινούνται από αριστερά προς τα δεξιά για να δείξουν την πρόοδο και να βοηθήσουν στον εντοπισμό σημείων συμφόρησης. Ένας πίνακας kanban μπορεί να χωριστεί σε οριζόντιες "λωρίδες" που αντιπροσωπεύουν διαφορετικά είδη εργασίας ή διαφορετικές ομάδες που εκτελούν την εργασία, για να βοηθήσουν στο συντονισμό των ομάδων και στη βελτιστοποίηση της ροής εργασίας.
Οι απλοί πίνακες έχουν στήλες για "σε αναμονή", "σε εξέλιξη" και "ολοκληρώθηκε" ή "προς υλοποίηση", "τρέχει" και "ολοκληρώθηκε". Μπορούν όμως να δημιουργηθούν και πιο σύνθετοι πίνακες kanban που υποδιαιρούν την εργασία "σε εξέλιξη" σε πολλαπλές στήλες για να απεικονίσουν τη ροή της εργασίας.

Για τους *ηγέτες* η στοχοθεσία είναι μονόδρομος και εργαλεία για τον εξορθολογισμό των προτεραιοτήτων αποτελούν ο «Κανόνας 25/5» και η «Αρχή Pareto».

Σχετικοί-Relevant και έχουν Χρονοδιάγραμμα-Time-bound) και 3) Διαγράψτε τους υπόλοιπους 20 στόχους που έχουν λιγότερη σημασία. Ο κανόνας 25/5 μπορεί να εφαρμοστεί σε προσωπικούς ή επαγγελματικούς στόχους, καθιστώντας τον μια αποτελεσματική, απλή τεχνική για την ιεράρχηση όλων των πτυχών της ζωής.



Η **Αρχή Pareto** (γνωστή επίσης ως κανόνας 80/20) είναι η ιδέα ότι το 80% των συνεπειών προέρχεται από το 20% των αιτιών. Εφαρμοσμένο στην παραγωγικότητα, σημαίνει ότι το 80% του αποτελέσματος (result) μπορεί να επιτευχθεί από το 20% της προσπάθειας (effort).

Κλείνοντας αυτή την ενότητα θα πρέπει να υπενθυμίσουμε ότι δεν υπάρχει μια τακτική για όλες τις καταστάσεις, αλλά χρειάζεται να επαναξιολογούμε τακτικά τις προτεραιότητές μας καθώς οι συνθήκες αλλάζουν συχνά. Με αυτό τον τρόπο μπορούμε να επιλέξουμε τα βέλτιστα εργαλεία για να διασφαλίσουμε ότι παραμένουμε συγκεντρωμένοι σε αυτά που έχουν μεγαλύτερη σημασία.

Επίλογος

Το πιο σημαντικό στη ζωή μας είναι να επιτύχουμε τους στόχους που έχουν τη μεγαλύτερη σημασία για εμάς. Φτιάχνοντας ένα προσωπικό στρατηγικό πλάνο και χρησιμοποιώντας τα εργαλεία που παρουσιάστηκαν, μπορούμε εύκολα να έχουμε μια επιτυχημένη σταδιοδρομία και μια ευτυχισμένη ζωή.

Συνοψίζοντας, αν δεν έχουμε στόχο και προτεραιότητες, τότε βαδίζουμε στην τύχη. Όποιο δρόμο και να πάρουμε, θα είναι καλός, αφού δεν έχουμε ιδέα πού θέλουμε να πάμε. Οπότε ξεκαθαρίζοντας τις προτεραιότητές μας θα ζήσουμε μια γεμάτη ζωή.

[1] Ενδιαφέροντα άρθρα: Ο Τροχός της Ζωής: δες τη μεγάλη εικόνα της ζωής σου - Dr. Αριστοτέλης Βάθης (therapia.gr) και Πώς θα καταλάβουμε ότι έχουμε βάλει «σωστά» τις προτεραιότητές μας | Vita.gr

“Φαίνεται πάντα αδύνατο,
μέχρι να γίνει...”

Nelson Mandela

Άλληλον

Facebook: www.facebook.com/ALLILONnet
Linkedin: www.linkedin.com/company/allilon
Twitter: @ALLILONnet

ISSN 2732-7701