
Η ΨΗΦΙΑΚΗ ΡΑΧΟΚΟΚΑΛΙΑ ΤΗΣ ΕΥΡΩΠΗΣ: ΓΙΑΤΙ Η ΑΣΦΑΛΗΣ ΣΥΝΔΕΣΙΜΟΤΗΤΑ ΑΝΑΔΕΙΚΝΥΕΤΑΙ ΤΩΡΑ ΣΕ ΒΑΣΙΚΟ ΠΥΛΩΝΑ ΑΜΥΝΑΣ

1. Περίληψη

Η ασφάλεια της Ευρώπης είναι πλέον αλληλένδετη με την ασφάλεια της συνδεσιμότητάς της. Βασικές εθνικές υπηρεσίες, όπως τα νοσοκομεία, τα ενεργειακά δίκτυα, τα δίκτυα μεταφορών, οι εφοδιαστικές αλυσίδες, οι χρηματοπιστωτικές αγορές και τα συστήματα διοίκησης και ελέγχου των ενόπλων δυνάμεων, βασίζονται όλες στην ανθεκτική ψηφιακή συνδεσιμότητα. Εάν αυτή διαταραχθεί ή διακυβευτεί, οι συνέπειες μπορούν να επεκταθούν πέραν των ορίων ενός μεμονωμένου τομέα, με συνέπεια την υπονόμευση της οικονομικής σταθερότητας και της αμυντικής ετοιμότητας.

Ο πόλεμος στην Ουκρανία απέδειξε ότι η στρατιωτική δράση μπορεί να πλήξει σοβαρά τις υποδομές συνδεσιμότητας. Ταυτόχρονα, όταν αυτή συνεχίζεται, συμβάλλει καθοριστικά στην ικανότητα μιας χώρας να αντισταθεί. Η σύγκρουση ανέδειξε τα ψηφιακά δίκτυα ως στοιχεία στρατηγικής σημασίας, καθώς όχι μόνο συμβάλλουν στη διατήρηση της ασφάλειας, αλλά και στην αποτελεσματική αντιμετώπιση των υβριδικών και ηλεκτρονικών επιθέσεων.

Παρόλα αυτά, σε επίπεδο πολιτικής και επενδυτικών επιλογών, η συνδεσιμότητα συχνά εξακολουθεί να αντιμετωπίζεται ως ένα απλό αγαθό της αγοράς, και όχι ως βασικός συντελεστής της ευρωπαϊκής άμυνας. Οι αρμοδιότητες παραμένουν κατακερματισμένες μεταξύ πολιτικών και στρατιωτικών αρχών, ευρωπαϊκών και εθνικών φορέων, καθώς και μεταξύ δημόσιου και ιδιωτικού τομέα. Σημαντικές επενδύσεις είτε καθυστερούν είτε υποχρηματοδοτούνται, ενώ ο συντονισμός κατά τη διάρκεια κρίσεων παραμένει αποσπασματικός. Η αντιμετώπιση αυτών των προκλήσεων απαιτεί ένα φιλοεπενδυτικό και καινοτόμο πλαίσιο, που βασίζεται σε μια συνεκτική και συστηματική πολιτική σε ολόκληρη την Ευρώπη.

Η Ευρώπη καλείται να επιλέξει. Αν εξακολουθήσει να αντιμετωπίζει τη συνδεσιμότητα ως μια υπηρεσία κοινής ωφέλειας χαμηλού κόστους, διατρέχει τον κίνδυνο να εκθέσει τους πολίτες της, τους δημοκρατικούς θεσμούς και τους συμμάχους της σε ολοένα και σοβαρότερες απειλές. Αντιθέτως, αν την αναγνωρίσει ως βασικό συστατικό στοιχείο της συλλογικής της ασφάλειας, θα μπορέσει να ενδυναμώσει σημαντικά μία από τις βασικές γραμμές άμυνάς της απέναντι στις σύγχρονες μορφές πολέμου.

Το διακύβευμα είναι σαφές, όπως προκύπτει από τις πρόσφατες αξιολογήσεις της ανταγωνιστικότητας της Ευρώπης από τους Enrico Letta και Mario Draghi, καθώς και από την έκθεση του Sauli Niinistö σχετικά με την πολιτική και στρατιωτική ετοιμότητα. Χωρίς σημαντικές επενδύσεις σε ασφαλή, πανευρωπαϊκή συνδεσιμότητα, η Ευρώπη θα παραμείνει ευάλωτη στις υβριδικές απειλές. Η Ευρωπαϊκή Επιτροπή έχει ήδη επισημάνει την ανάγκη για πρόσθετες επενδύσεις ύψους 200 δισ. ευρώ, ώστε να επιτευχθούν οι στόχοι συνδεσιμότητας έως το 2030.¹

Προκειμένου η συνδεσιμότητα να αναδειχθεί σε κεντρικό πυλώνα της ευρωπαϊκής ασφάλειας, οι ηγέτες καλούνται να αναλάβουν δράση σε πέντε βασικούς τομείς.

α. Αναγνώριση της ασφαλούς συνδεσιμότητας ως στρατηγικού πλεονεκτήματος για την ασφάλεια, με την ενσωμάτωση της στις εθνικές στρατηγικές ασφάλειας, στον σχεδιασμό της ΕΕ και του ΝΑΤΟ, καθώς και στις αμυντικές δυνατότητες.

β. Θεσμοθέτηση μόνιμων και αξιόπιστων μηχανισμών συνεργασίας μεταξύ κυβερνήσεων, παρόχων και συμμάχων, για τον συντονισμό της απόκρισης σε κρίσεις, την ανταλλαγή πληροφοριών, την προστασία υποθαλάσσιων, δορυφορικών και ψηφιακών υποδομών, καθώς και την ενίσχυση της διασυνοριακής ανθεκτικότητας σε πανευρωπαϊκό επίπεδο.

γ. Κάλυψη των επενδυτικών κενών σε ψηφιακές υποδομές ζωτικής σημασίας, όπου οι δυνάμεις της αγοράς από μόνες τους δεν διασφαλίζουν την απαιτούμενη ανθεκτικότητα. Η Ευρώπη οφείλει να αξιοποιήσει κίνητρα και εναρμονισμένες πολιτικές που ενθαρρύνουν την προστασία των δικτύων, μεταξύ άλλων μέσω της επικείμενης Πράξης για τα Ψηφιακά Δίκτυα (Digital Networks Act).

δ. Εδραίωση της στρατηγικής ανοιχτότητας, μέσα από συνεργασίες με αξιόπιστους συμμάχους, όπως το Ηνωμένο Βασίλειο, με στόχο την από κοινού ανάπτυξη τεχνολογιών ζωτικής σημασίας και την εναρμόνιση προτύπων που θωρακίζουν την ασφάλεια και την τεχνολογική κυριαρχία της Ευρώπης.

ε. Επένδυση στην ψηφιακή συμπερίληψη και παιδεία, ώστε οι πολίτες να είναι σε θέση να αναγνωρίσουν την παραπληροφόρηση και να διατηρούν την εμπιστοσύνη τους στους δημοκρατικούς θεσμούς, ενισχύοντας τη συνολική κοινωνική ανθεκτικότητα της Ένωσης.

Με αυτή την προσέγγιση, η Ευρώπη μπορεί να αξιοποιήσει τα εκτεταμένα και ανθεκτικά δίκτυά της ως στρατηγικό πλεονέκτημα: αποτρέποντας απειλές, εδραιώνοντας συμμαχίες και προστατεύοντας την ασφάλεια και την ευημερία των πολιτών της.

2. Εισαγωγή – Το νέο παράδειγμα της ασφάλειας στην Ευρώπη

Για περισσότερο από τρεις δεκαετίες μετά τη λήξη του Ψυχρού Πολέμου, το σενάριο μιας σύγκρουσης μεγάλης κλίμακας εντός της ευρωπαϊκής ηπείρου έμοιαζε απίθανο. Ο πόλεμος στην Ουκρανία, οι συχνότερες ψηφιακές και υβριδικές απειλές και ο γεωπολιτικός ανταγωνισμός που συνεχώς κλιμακώνεται, έχουν οδηγήσει την Ευρώπη να επανεξετάσει την ασφάλειά της.

Ο διακρατικός πόλεμος υψηλής έντασης έχει κάνει την επανεμφάνισή του στην ευρύτερη γειτονιά της Ευρώπης, ενώ οι υβριδικές απειλές, όπως οι κυβερνοεπιθέσεις, οι δολιοφθορές σε υποδομές ζωτικής σημασίας και η παραπληροφόρηση με στόχο την αποσταθεροποίηση των δημοκρατικών θεσμών, αποτελούν πλέον καθημερινό φαινόμενο σε ολόκληρη την ήπειρο. Το 2025, οι παγκόσμιες κυβερνοεπιθέσεις αυξήθηκαν κατά 21%, ενώ, σύμφωνα με το Διεθνές Ινστιτούτο Στρατηγικών Μελετών (IISS), οι ρωσικές επιχειρήσεις δολιοφθοράς κατά ευρωπαϊκών υποδομών ζωτικής σημασίας παρουσίασαν αύξηση της τάξης του 246% την περίοδο 2023-2024.²

Η Ευρωπαϊκή Επιτροπή έχει ήδη τονίσει ότι η τρέχουσα αστάθεια καθιστά επιτακτική την αύξηση των επενδύσεων στην αμυντική καινοτομία, καθώς και στις ψηφιακές υποδομές, συμπεριλαμβανομένων τεχνολογιών όπως η τεχνητή νοημοσύνη, οι κβαντικοί υπολογιστές και οι ασφαλείς επικοινωνίες.³ Αντιστοίχως,

το NATO προέτρεψε τα μέλη του να διαθέτουν το 1,5% του ΑΕΠ τους για τη θωράκιση της συνολικής ανθεκτικότητας, δίδοντας έμφαση και στην προστασία σημαντικών ψηφιακών υποδομών.⁴

Στρατηγικά κείμενα, όπως η Έκθεση Niinistö του 2024 για την ετοιμότητα της Ευρώπης, προτείνουν τη διάθεση του 20% του συνολικού προϋπολογισμού της ΕΕ σε τομείς που αφορούν την ασφάλεια και τη διαχείριση κρίσεων.⁵ Παράλληλα, η έρευνα του Ευρωβαρομέτρου για το 2025 καταγράφει την ισχυρή επιθυμία των πολιτών για έναν πιο ενεργό ρόλο της ΕΕ στους τομείς ασφάλειας και της άμυνας.⁶ Συμπερασματικά, τα στοιχεία αυτά επιβεβαιώνουν ότι η ασφάλεια της Ευρώπης συνδέεται αδιάρρηκτα με τις υποδομές που θεμελιώνουν τις οικονομίες και τις κοινωνίες της. Υπό αυτό το πρίσμα, η ασφαλής συνδεσιμότητα, μαζί με τις τηλεπικοινωνιακές υποδομές που την καθιστούν εφικτή, θα αποτελέσει καθοριστικό παράγοντα για το κατά πόσο η νέα αυτή στρατηγική φιλοδοξία μπορεί να μετουσιωθεί σε ουσιαστική επιχειρησιακή ικανότητα.

3. Η συνδεσιμότητα ως πυλώνας στρατηγικής ισχύος και ασφάλειας

Παραδοσιακά, η συνδεσιμότητα είχε αντιμετωπιστεί ως μηχανισμός οικονομικής ανάπτυξης, μέσω της παροχής υπηρεσιών και της διασύνδεσης των πολιτών. Παρόλο που αυτό διατηρεί τη σημασία του, η συνδεσιμότητα σήμερα συνιστά επίσης, αναπόσπαστο συστατικό της κοινωνικής ανθεκτικότητας και της αμυντικής ετοιμότητας.

α. Η συνδεσιμότητα ως η ραχοκοκαλιά της κοινωνικής ανθεκτικότητας

Οι βασικές υπηρεσίες της Ευρώπης, από τα ενεργειακά δίκτυα και τις μεταφορές έως τα νοσοκομεία και τη δημόσια διοίκηση, εξαρτώνται από την ψηφιακή συνδεσιμότητα.

Σε περιόδους κρίσεων, όπως οι φυσικές καταστροφές ή οι κυβερνοεπιθέσεις, η συνδεσιμότητα επιτρέπει τον συντονισμό των υπηρεσιών έκτακτης ανάγκης, τους πολίτες να έχουν πρόσβαση σε βοήθεια και τις αρχές να προσφέρουν καθοδήγηση και να διασφαλίζουν τη δημόσια τάξη. Η πανδημία COVID-19 ανέδειξε τον ρόλο της ψηφιακής ανθεκτικότητας, καθώς επέτρεψε σε εκατομμύρια Ευρωπαίους να εργάζονται εξ αποστάσεως, διασφαλίζοντας τη συνέχεια βασικών υπηρεσιών ακόμη και όταν οι παραδοσιακοί μηχανισμοί λειτουργίας είχαν ανασταλεί.

Όταν, ωστόσο, η συνδεσιμότητα διακόπτεται, οι επιπτώσεις επεκτείνονται ταχύτατα σε σημαντικούς και αλληλοεξαρτώμενους τομείς. Προσομοιώσεις φυσικών καταστροφών καταδεικνύουν ότι η εύρυθμη λειτουργία των νοσοκομείων εξαρτάται από τη διαθεσιμότητα των ζωτικής σημασίας υποδομών. Όταν αυτές τίθενται εκτός λειτουργίας, διακυβεύεται άμεσα η παροχή επείγουσας φροντίδας και περίθαλψης.⁷

Τα πρόσφατα γεγονότα αποκαλύπτουν πώς η διακοπή λειτουργίας σε διάφορα επίπεδα υποδομών μπορεί να έχει διατμηματικές και διασυνοριακές συνέπειες.

- Τον Απρίλιο του 2025, η πολύωρη διακοπή ρεύματος στην Ιβηρική χερσόνησο εκτιμάται ότι κόστισε στην Ισπανία το 0,1% του τριμηνιαίου ΑΕΠ της.⁸ Οι αναλυτές επεσήμαναν τις εκτεταμένες επιπτώσεις της διακοπής αυτής σε υποδομές ζωτικής σημασίας, όπως οι μεταφορές, το λιανικό εμπόριο και η βιομηχανική δραστηριότητα.⁹
- Μια ακόμη περίπτωση ήταν η επίθεση στον δορυφόρο Viasat το 2022. Αν και στόχος ήταν η Ουκρανία, η επίθεση διέκοψε την ευρυζωνική σύνδεση στο διαδίκτυο για χιλιάδες χρήστες σε όλη την Ευρώπη και

προκάλεσε την απώλεια της δυνατότητας απομακρυσμένης παρακολούθησης ανεμογεννητριών στη Γερμανία.¹⁰

- Επίσης, οι παρεμβολές GPS στη Βαλτική επηρέασαν την πολιτική αεροπορία και τη ναυσιπλοΐα, επιβεβαιώνοντας ότι επιθέσεις σε κρίσιμα ψηφιακά σήματα μπορούν να μετατραπούν σε πραγματικές απειλές για τη δημόσια ασφάλεια.

Η συνδεσιμότητα αποτελεί θεμέλιο της κοινωνικής συνοχής. Εκστρατείες παραπληροφόρησης επιτρέπουν στο εχθρικό μέτωπο να υπονομεύει την εμπιστοσύνη στους θεσμούς και να αποσταθεροποιεί τις κοινωνίες, φαινόμενο που συνεχίζει να παρατηρείται στην Ευρώπη, ιδιαίτερα κατά τη διάρκεια της εκλογικής περιόδου. Πρόσφατη έρευνα του ΟΗΕ και του Παγκόσμιου Οικονομικού Φόρουμ κατατάσσουν την παραπληροφόρηση και τη χειραγώγηση της κοινής γνώμης μεταξύ των πλέον σοβαρών βραχυπρόθεσμων απειλών για τη δημοκρατία, γεγονός που καθιστά σαφές τον λόγο που η ασφαλής συνδεσιμότητα λειτουργεί ως απαραίτητη ασπίδα για την κοινωνία.¹¹

Η συνδεσιμότητα επιτρέπει στις οικονομίες να λειτουργούν, στις κυβερνήσεις να εξυπηρετούν τους πολίτες με αποδοτικό τρόπο και στους ίδιους τους πολίτες να επικοινωνούν μεταξύ τους. Συνιστά ένα από τα θεμελιώδη συστήματα, όπως η ενέργεια, οι μεταφορές και ο χρηματοοικονομικός τομέας, επί των οποίων βασίζονται πολλές άλλες υπηρεσίες. Σήμερα, η ψηφιακή ραχοκοκαλιά της Ευρώπης περιλαμβάνει χερσαίες οπτικές ίνες, κινητά δίκτυα, υποθαλάσσια καλώδια, δορυφορικές συνδέσεις, data centres και υπηρεσίες cloud. Τα τηλεπικοινωνιακά δίκτυα έχουν από καιρό αναγνωριστεί ως κρίσιμες εθνικές υποδομές. Ωστόσο, αυτό που έχει αλλάξει είναι αφενός ο βαθμός εξάρτησης άλλων κρίσιμων τομέων από αυτά, και αφετέρου η πολυπλοκότητα των εμπλεκόμενων τεχνολογιών.

β. Η συνδεσιμότητα ως νευραλγικό στοιχείο της αμυντικής ετοιμότητας

Οι σύγχρονες ένοπλες δυνάμεις βασίζονται σε ασφαλή, υψηλής χωρητικότητας τηλεπικοινωνιακά δίκτυα για επιχειρησιακές λειτουργίες όπως η διοίκηση και ο έλεγχος, η εφοδιαστική υποστήριξη και η συλλογή πληροφοριών. Σύμφωνα με μελέτη του Chatham House για τα συστήματα διοίκησης, ελέγχου και επικοινωνιών του NATO, «η επικοινωνία αποτελεί έναν από τους τρεις βασικούς άξονες κάθε στρατηγικής αποτροπής», ενώ οποιαδήποτε διακοπή στα δίκτυα επικοινωνίας επιφέρει «σοβαρές επιπτώσεις στην ικανότητα άσκησης διοίκησης και ελέγχου».¹²

Κινητά και σταθερά δίκτυα μεταφέρουν πολύτιμα δεδομένα μεταξύ αισθητήρων, μη επανδρωμένων συστημάτων και υπευθύνων λήψης αποφάσεων στο πεδίο. Για παράδειγμα, το Πολεμικό Ναυτικό της Πορτογαλίας χρησιμοποίησε ιδιωτικό δίκτυο 5G της Vodafone για δοκιμές με drones και μη επανδρωμένα σκάφη, επιτρέποντας για πρώτη φορά στα πλοία να τα συντονίζουν σε πραγματικό χρόνο, χωρίς την ανάγκη σύνδεσης με επίγειο κέντρο ελέγχου.¹³

Στη Φινλανδία, η κυβερνητική Έκθεση Εθνικής Άμυνας του 2024, ανέφερε ότι «οι Φινλανδικές Ένοπλες Δυνάμεις ενίσχυσαν τη συνεργασία τους με τηλεπικοινωνιακούς παρόχους και άλλους εταίρους», οδηγώντας σε καινοτομίες όπως το διασυνοριακό δίκτυο 5G slicing για στρατιωτική χρήση.¹⁴ Αυτά τα παραδείγματα αναδεικνύουν ότι η σύγχρονη στρατιωτική ικανότητα εξαρτάται από ασφαλή και υψηλής απόδοσης δίκτυα επικοινωνίας, πολλά από τα οποία σχεδιάζονται, αναπτύσσονται και λειτουργούν από ιδιώτες παρόχους.

Το NATO αναγνωρίζει ότι η ανθεκτική πολιτική επικοινωνία αποτελεί αναπόσπαστο στοιχείο της εθνικής ανθεκτικότητας, καθώς οι ένοπλες δυνάμεις εξαρτώνται από πολιτικά δίκτυα για λειτουργίες όπως η χρήση μη επανδρωμένων αεροπορικών συστημάτων (UAS), τα οποία απαιτούν υψηλό εύρος ζώνης και εξαιρετικά χαμηλό χρόνο απόκρισης για ανταλλαγή δεδομένων σε πραγματικό χρόνο.¹⁵ Η *Λευκή Βίβλος της Ευρωπαϊκής Επιτροπής*

για την Ευρωπαϊκή Άμυνα επισημαίνει επίσης ότι τεχνολογίες όπως η τεχνητή νοημοσύνη, το υπολογιστικό νέφος (cloud computing) και η ασφαλής συνδεσιμότητα μετασχηματίζουν τον τρόπο διεξαγωγής των πολεμικών επιχειρήσεων, ενεργοποιώντας την ανάπτυξη αυτόνομων συστημάτων, όπως drones, ρομποτικά μέσα και χερσαία οχήματα.

Όπως επισημαίνεται στην έκθεση Agel για τις *Τηλεπικοινωνίες ως θεμέλιο της Ευρωπαϊκής Άμυνας*: «Οι σύγχρονες ένοπλες δυνάμεις στηρίζονται στην ψηφιακή υποδομή για σχεδόν κάθε βασική τους λειτουργία...Χωρίς ισχυρές τηλεπικοινωνιακές δυνατότητες, μια συντονισμένη και αποτελεσματική ευρωπαϊκή αμυντική αρχιτεκτονική είναι δομικά αδύνατη».¹⁶

Μαθήματα από την Ουκρανία

Από τον Φεβρουάριο του 2022, το παράδειγμα της Ουκρανίας προσφέρει σημαντικά διδάγματα για την Ευρώπη σχετικά με τον ρόλο της συνδεσιμότητας κατά τη διάρκεια μιας επίκαιρης σύγκρουσης. Από την πρώτη ημέρα της εισβολής, η Ρωσία επιχειρήσε να καταστρέψει τα ουκρανικά δίκτυα μέσω φυσικών επιθέσεων, κυβερνοεπιθέσεων και ηλεκτρονικού πολέμου. Ωστόσο, οι πάροχοι της χώρας εργάστηκαν αδιάκοπα για να διατηρήσουν τη συνέχεια της λειτουργίας της συνδεσιμότητας, με πολύ καλύτερα αποτελέσματα από τα αναμενόμενα. Με βάση την εμπειρία του συνεργάτη μας, Vodafone Ukraine, πολλοί παράγοντες οδήγησαν στην ψηφιακή ανθεκτικότητα.

- 1. Τεχνολογική πολυμορφία και επιχειρησιακή εφεδρεία.** Τα δίκτυα της Ουκρανίας στηρίχθηκαν σε ένα μείγμα πολλαπλών τεχνολογιών, εναλλακτικών οδεύσεων και παρόχων, συνδυάζοντας κινητή, σταθερή, υποθαλάσσια και δορυφορική συνδεσιμότητα. Η προσέγγιση αυτή εξασφάλισε εναλλακτικές λύσεις αποκατάστασης, επιτρέποντας την επαναφορά της λειτουργίας εντός ολίγων ωρών από την πρόκληση ζημιών στις υποδομές
- 2. Ταχεία αποκατάσταση υποδομών.** Η Vodafone Ukraine προχώρησε στην εγκατάσταση περισσότερων από 3.000 γεννητριών και σταθμών βάσης με φωτοβολταϊκά συστήματα, διασφαλίζοντας τη λειτουργία του 90% των σημείων πρόσβασης, ακόμη και κατά τη διάρκεια εκτεταμένων διακοπών ρεύματος.
- 3. Στενή συνεργασία δημόσιου και ιδιωτικού τομέα.** Η συστηματική επικοινωνία μεταξύ των ουκρανικών αρχών και των παρόχων είχε ως αποτέλεσμα τις άμεσες και συντονισμένες ενέργειες για την αντιμετώπιση των περιστατικών, καθώς και τη παροχή αξιόπιστων πληροφοριών μέσω SMS, συμβάλλοντας ουσιαστικά στην αντιμετώπιση της παραπληροφόρησης κατά τη διάρκεια του πολέμου.
- 4. Ευέλικτο ρυθμιστικό πλαίσιο.** Οι ρυθμιστικές αρχές διευκόλυναν την απρόσκοπτη επιχειρησιακή συνέχεια, επιτρέποντας τη χρήση φάσματος εκτάκτου ανάγκης, την περιαγωγή (roaming) και την ταχεία ανάπτυξη προσωρινών υποδομών.
- 5. Κυβερνοασφάλεια.** Προληπτικά μέτρα για την ενίσχυση της ανθεκτικότητας κατέστησαν δυνατή την αδιάλειπτη λειτουργία του δικτύου της Vodafone κατά την κυβερνοεπίθεση στο δίκτυο της Kyivstar το 2023, διασφαλίζοντας τη διατήρηση της συνδεσιμότητας για εκατομμύρια πολίτες.
- 6. Καινοτομία εν μέσω κρίσης.** Ένα νέο εργαστήριο Έρευνας και Ανάπτυξης, σε συνεργασία της Vodafone Ukraine και του Εθνικού Αεροναυπηγικού Πανεπιστημίου, εστιάζει στις τεχνολογίες 5G, κυβερνοασφάλειας, συστημάτων drone και κινητών διαστημικών επικοινωνιών. Η πρωτοβουλία αυτή ενισχύει τη συνεργασία μεταξύ βιομηχανίας και ακαδημαϊκής κοινότητας, συμβάλλοντας στην τεχνολογική κυριαρχία της Ουκρανίας και στις ευρωπαϊκές λύσεις για ασφαλή, ανθεκτική συνδεσιμότητα.

Το αποτέλεσμα ήταν ότι η Ουκρανία κατάφερε να διατηρήσει την ικανότητα συντονισμού της άμυνάς της, να εξασφαλίσει την αδιάλειπτη λειτουργία των απαραίτητων υπηρεσιών και να διατηρήσει την επικοινωνία με

τους πολίτες της. Η συνδεσιμότητα αναδείχθηκε ως καθοριστικός πυλώνας της συνολικής της ανθεκτικότητας και της ικανότητάς της για αντίσταση.

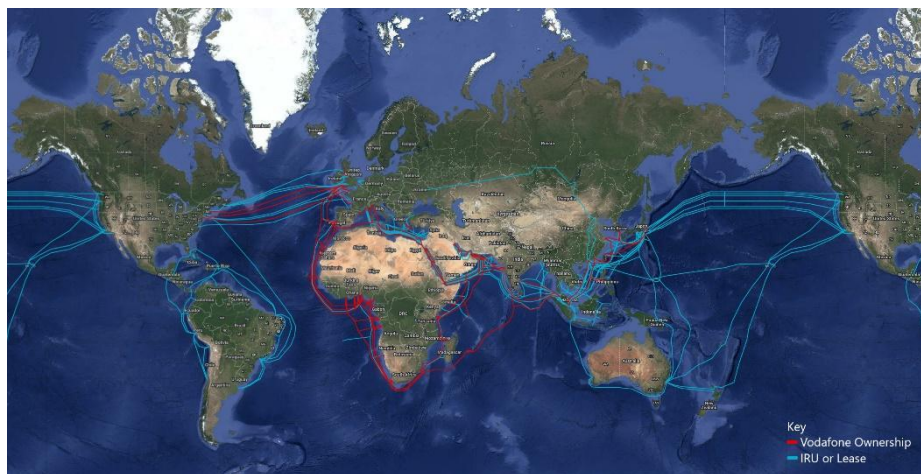
4. Ο κομβικός ρόλος των παρόχων συνδεσιμότητας στην ευρωπαϊκή ασφάλεια

Οι αντίπαλοι κατανοούν τη σημασία της συνδεσιμότητας και το ίδιο κάνουν και οι πάροχοι που την υπερασπίζονται καθημερινά. Οι υβριδικές επιθέσεις κατά των ανοικτών κοινωνιών περιλαμβάνουν συστηματικά προσπάθειες διακοπής, υποβάθμισης ή παραβίασης δικτύων και υπηρεσιών. Πάροχοι όπως η Vodafone βρίσκονται στην πρώτη γραμμή, επενδύοντας διαρκώς στην ανθεκτικότητα, στην άμεση ανταπόκριση σε καταστάσεις κρίσεων και στην προσαρμογή, με σκοπό την προστασία των κρίσιμων ευρωπαϊκών συστημάτων σε φυσικό, ψηφιακό και δορυφορικό επίπεδο.

α. Προστασία φυσικών υποδομών

Τα υποθαλάσσια καλώδια, οι σταθμοί προσαυγιάλωσης, τα επίγεια δίκτυα οπτικών ινών, οι κεραιές κινητής τηλεφωνίας και τα data centers αποτελούν ελκυστικούς στόχους. Περίπου το 97% της παγκόσμιας διακίνησης δεδομένων του διαδικτύου πραγματοποιείται μέσω υποθαλάσσιων καλωδίων, τα οποία μεταφέρουν καθημερινά περίπου 8,5 τρισεκατομμύρια ευρώ σε χρηματοοικονομικές συναλλαγές.¹⁷ Τα καλωδιακά συστήματα καταγράφουν κάθε χρόνο 150 έως 200 βλάβες, ακόμη και χωρίς να είναι αποτέλεσμα εχθρικών παρεμβάσεων. Τρία κράτη μέλη της ΕΕ, η Ιρλανδία, η Μάλτα και η Κύπρος, βασίζονται εξ ολοκλήρου στα υποθαλάσσια καλώδια για τη συνδεσιμότητά τους. Όλα αυτά εξηγούν γιατί η εφεδρεία, η δυνατότητα επισκευής και οι σταθμοί προσαυγιάλωσης έχουν τόσο μεγάλη σημασία.

Για την αντιμετώπιση αυτών των κινδύνων, οι ευρωπαϊκοί πάροχοι, συμπεριλαμβανομένης της Vodafone, εστιάζουν στη θωράκιση της ανθεκτικότητας. Οι σχετικές παρεμβάσεις περιλαμβάνουν τη διαφοροποίηση των διαδρομών συνδεσιμότητας, τη διεύρυνση της πλεονάζουσας χωρητικότητας σε κομβικά σημεία διασύνδεσης, τη θωράκιση ουσιαστικών υποδομών, την ενδυνάμωση της ενεργειακής αυτονομίας και των δυνατοτήτων αποκατάστασης, καθώς και τον σχεδιασμό εναλλακτικών οδών για απομακρυσμένες ή δυσπρόσιτες περιοχές. Οι εθνικές κυβερνήσεις και οι σύμμαχοι αναγνωρίζουν ολοένα και περισσότερο τη σημασία αυτών των ζητημάτων, όπως αποδεικνύεται από τη στρατηγική συνεργασία του NATO στον τομέα των υποθαλάσσιων υποδομών και τις πρόσφατες δεσμεύσεις στη Βόρεια Θάλασσα για την προστασία των υποθαλάσσιων ενεργειακών και ψηφιακών πόρων. Η στενή συνεργασία με τις αρμόδιες αρχές και άλλους παρόχους κρίσιμων υποδομών συμβάλλει στον καθορισμό προτεραιοτήτων για την αποκατάσταση βλαβών και στην προστασία βασικών υποδομών σε περίπτωση κρίσης.



Το δίκτυο υποθαλάσσιων καλωδίων της Vodafone. Η Vodafone διαχειρίζεται ένα από τα εκτενέστερα δίκτυα υποθαλάσσιων καλωδίων στην Ευρώπη, προσφέροντας ασφαλή και ανθεκτική συνδεσιμότητα σε περισσότερες από 100 χώρες. Κατέχει και διαχειρίζεται τα δύο καλώδια που συνδέουν την Ευρώπη (μέσω του Ηνωμένου Βασιλείου και της Γαλλίας) με τις Ηνωμένες Πολιτείες και είναι εταίρος στην ανάπτυξη του 2Africa, του μεγαλύτερου υποθαλάσσιου καλωδιακού συστήματος στον κόσμο.¹⁸

β. Αντιμετώπιση των κυβερνοεπιθέσεων

Οι κυβερνοεπιθέσεις γίνονται ολοένα πιο εκτεταμένες και σύνθετες, ενώ επιφέρουν συνέπειες σε κυβερνήσεις, επιχειρήσεις και στους πολίτες. Στη Γερμανία, για παράδειγμα, το κυβερνοέγκλημα και η δολιοφθορά κόστισαν στις εταιρείες 267 δις. ευρώ το 2024.¹⁹

Η κυβερνοεπίθεση του 2022 κατά της Vodafone Πορτογαλίας αναδεικνύει τη σημασία του μεγέθους και της αξιοποίησης των πανευρωπαϊκών δυνατοτήτων.²⁰ Αν και στόχος των επιθέσεων ήταν η διακοπή των υπηρεσιών, η Vodafone επανέφερε τη λειτουργία των δεδομένων κινητής τηλεφωνίας και των διασυνδέσεων μεταξύ παρόχων μέσα σε οκτώ ώρες, κινητοποιώντας και συντονίζοντας πόρους από το σύνολο των ευρωπαϊκών της επιχειρήσεων και από την παγκόσμια ομάδα ασφάλειας.²¹ Η άμεση αναπόκριση επιβεβαιώνει τη σημασία των οικονομικών κλίμακας, της τεχνογνωσίας και της διακρατικής συνεργασίας στην αντιμετώπιση των σύγχρονων υβριδικών απειλών.

γ. Δορυφορική συνδεσιμότητα για ασφάλεια και ανθεκτικότητα

Η συνδεσιμότητα σημαίνει πολλά περισσότερα από ένα σύνολο καλωδίων και κεραιών. Οι δορυφορικές επικοινωνίες καθώς και τα σήματα θέσης, πλοήγησης και συγχρονισμού, όπως το GPS, είναι ζωτικής σημασίας σε τομείς όπως η αεροπλοΐα, η ναυσιπλοΐα και οι εφοδιαστικές αλυσίδες. Καθώς τηλεπικοινωνιακοί πάροχοι όπως η Vodafone ενσωματώνουν τη δορυφορική συνδεσιμότητα στα επίγεια δίκτυα, η Ευρώπη οφείλει να δώσει προτεραιότητα στην ασφάλεια αυτών των συστημάτων. Η κοινοπραξία SatCo της Vodafone, στο πλαίσιο ενός ανοικτού μοντέλου λειτουργίας σε επίπεδο χονδρικής, υποστηρίζει τους παρόχους στη διατήρηση της επιχειρησιακής συνέχειας κατά τη διάρκεια φυσικών καταστροφών ή διακοπών δικτύου. Με αυτόν τον τρόπο επισφραγίζεται η συνεχής λειτουργία των υπηρεσιών έκτακτης ανάγκης, εξασφαλίζοντας στους πολίτες πρόσβαση στη συνδεσιμότητα.²²

Η ασφάλεια των δορυφορικών επικοινωνιών αποκτά ολοένα και μεγαλύτερη σημασία. Τα τελευταία χρόνια παρατηρείται σημαντική αύξηση περιστατικών παρεμβολής, παραποίησης και παρεμπόδισης σημάτων GPS. Στην περιοχή της Βαλτικής, έχουν καταγραφεί επανειλημμένα περιστατικά που επηρεάζουν τη λειτουργία αεροσκαφών και πλοίων. Ενδεικτικά, η Σουηδική Υπηρεσία Μεταφορών ανέφερε 733 περιστατικά παρεμβολών και διακοπών μόνο για το διάστημα Ιανουαρίου-Αυγούστου 2025.²³

Ο τομέας των τηλεπικοινωνιών προετοιμάζεται για μελλοντικές απειλές, πρωτοστατώντας στην υιοθέτηση προτύπων ασφαλείας επόμενης γενιάς, όπως η μετα-κβαντική κρυπτογράφηση. Στο πλαίσιο αυτό, η συνεργασία της Vodafone με την IBM στοχεύει στην ενίσχυση της ανθεκτικότητας των συστημάτων ΤΠΕ έναντι των προκλήσεων που αναμένεται να προκαλέσουν οι κβαντικοί υπολογιστές. Η επένδυση αυτή αναδεικνύει την τεχνολογική υπεροχή της ευρωπαϊκής βιομηχανίας η οποία μπορεί να αποτελέσει θεμέλιο για μια πιο ισχυρή και θωρακισμένη ευρωπαϊκή άμυνα.

5. Γεφυρώνοντας το χάσμα μεταξύ ετοιμότητας και ανθεκτικότητας στην Ευρώπη

Οι φορείς που διαχειρίζονται υποδομές ζωτικής σημασίας επενδύουν σημαντικά στην ανθεκτικότητα. Από την ενσωμάτωση εφεδρικής χωρητικότητας και τη συγκρότηση ομάδων άμεσης επέμβασης, έως την προσαρμογή των τεχνολογιών ανίχνευσης και περιορισμού απειλών, που συνεχώς αναπτύσσονται.

Η διατήρηση αυτού του πλεονεκτήματος προϋποθέτει ένα υποστηρικτικό θεσμικό πλαίσιο, ικανό να προάγει τις μακροπρόθεσμες επενδύσεις στην ασφάλεια, να ενθαρρύνει την καινοτομία και να διευκολύνει τη συνεργασία με τις κυβερνήσεις και αξιόπιστους παρόχους.

Η ασφάλεια της συνδεσιμότητας δεν μπορεί να αποτελεί αποκλειστική ευθύνη των παρόχων. Όπως επισημαίνει και η Έκθεση Niinistö του 2024, η ετοιμότητα για να είναι αποτελεσματική προϋποθέτει μια ολιστική προσέγγιση σε επίπεδο κοινωνίας, στο πλαίσιο της οποίας οι υποδομές επικοινωνίας εντάσσονται οργανικά στον σχεδιασμό τόσο του πολιτικού όσο και του στρατιωτικού τομέα.²⁴

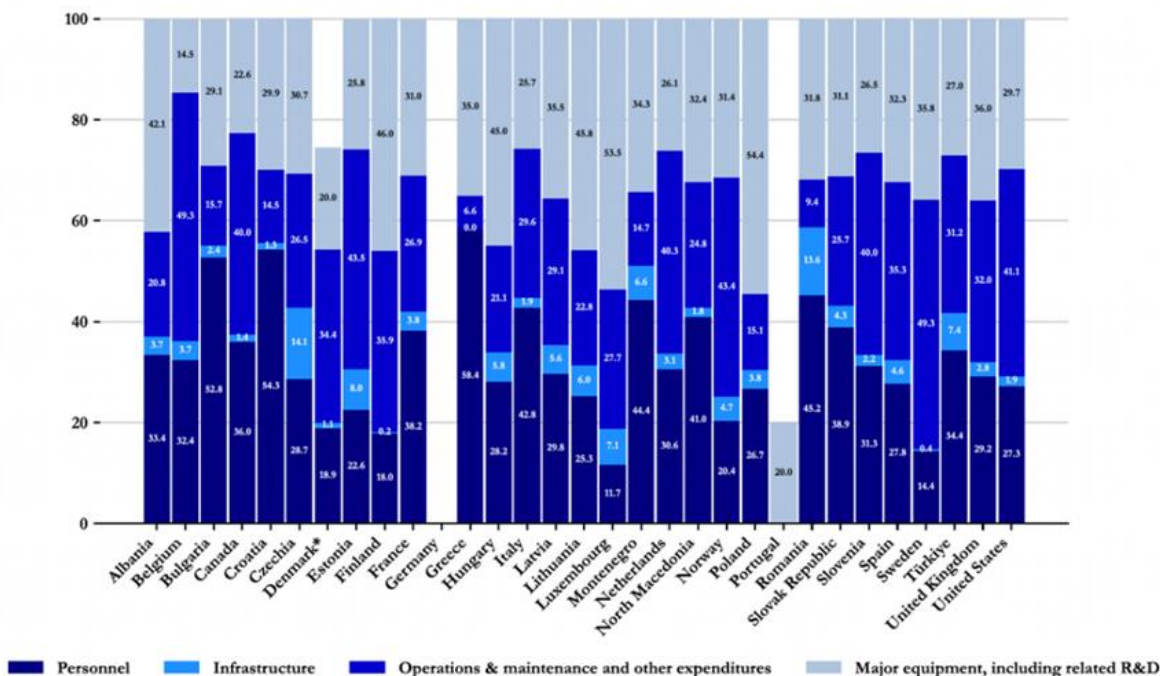
Η ανάγκη για πολιτική δράση καθίσταται πλέον επιτακτική. Η έκθεση AreI, με τίτλο «Much More than a Network», αναδεικνύει το διαρθρωτικό επενδυτικό κενό που καταγράφεται στα ευρωπαϊκά δίκτυα επικοινωνιών. Η Ευρωπαϊκή Επιτροπή εκτιμά ότι απαιτούνται πρόσθετες επενδύσεις ύψους 200 δισ. ευρώ για την επίτευξη των στόχων συνδεσιμότητας έως το 2030. Η τεχνολογία συνδεσιμότητας αποτελεί έναν από τους ελάχιστους τομείς του ψηφιακού οικοσυστήματος στους οποίους η Ευρώπη εξακολουθεί να διατηρεί ισχυρή παγκόσμια παρουσία. Ωστόσο, το ανταγωνιστικό αυτό πλεονέκτημα απειλείται, εάν δεν διαμορφωθεί ένα βιώσιμο και μακροπρόθεσμο μοντέλο ανάπτυξης και επενδύσεων. Όπως επισημαίνεται στην έκθεση AreI, δεν μπορεί να υπάρξει αξιόπιστη άμυνα χωρίς μια πραγματικά πανευρωπαϊκή, ασφαλή και ανθεκτική αγορά στις τηλεπικοινωνίες. Είτε θα στηριχθούν η μία στην άλλη, είτε θα αποδυναμωθούν ταυτόχρονα.

Μακροπρόθεσμα, ο κατακερματισμός σε ολόκληρη την Ευρώπη θα εξασθενίσει την ικανότητα του κλάδου να ανταποκρίνεται αποτελεσματικά σε νέες απειλές, ενώ θα περιορίσει την καινοτομία και θα παρεμποδίσει την κλίμακα επενδύσεων που απαιτείται για τη δημιουργία ασφαλών και διττής χρήσης δικτύων. Οι ψηφιακές υποδομές απαιτούν πανευρωπαϊκό συντονισμό με αξιόπιστους εταίρους, όχι απλώς εθνικές στρατηγικές, για την αντιμετώπιση διασυνοριακών, κρατικά υποστηριζόμενων απειλών. Η στενότερη συνεργασία μεταξύ ΕΕ και Ηνωμένου Βασιλείου είναι ιδιαίτερα σημαντική, καθώς και οι δύο πλευρές αντιμετωπίζουν κοινές απειλές και διαθέτουν συμπληρωματικές δυνατότητες.

Η αναγνώριση της συνδεσιμότητας ως πόρου στρατηγικής σημασίας για την ασφάλεια, καθώς και ως θεμελιώδους άξονα της κοινωνικής ανθεκτικότητας, επιβάλλει στην Ευρώπη την ενσωμάτωση αυτών των νέων δεδομένων στον στρατηγικό της σχεδιασμό και στις επενδυτικές της πολιτικές, αποφεύγοντας παράλληλα την επιβολή περιττών κανονιστικών επιβαρύνσεων.

Γράφημα 8: Κύριες Κατηγορίες Αμυντικών Δαπανών (%) 2025e
(ποσοστό επί του συνόλου των αμυντικών δαπανών)

Graph 8: Main Categories of defence expenditure (%) 2025e
(percentage of total defence expenditure)



Notes: Data as at 3 June 2025, based on 2021 prices and exchange rates. Figures for 2025 are estimates. For those Allies that did not provide estimates for 2025, the respective estimates are shown as blank. * Denmark has declared that it has allocated more than 20% of defence expenditure to major equipment.

Το γράφημα του NATO παρουσιάζει τις βασικές κατηγορίες αμυντικών δαπανών μεταξύ των Συμμάχων (στοιχεία για το 2024 και εκτιμήσεις για το 2025).²⁵ Οι υποδομές εξακολουθούν να αποτελούν τη μικρότερη κατηγορία, η οποία περιορίζεται σε στρατιωτικές κατασκευές και κοινές εγκαταστάσεις του NATO. Ωστόσο, οι Σύμμαχοι έχουν δεσμευθεί να διαθέτουν το 1,5% του ΑΕΠ τους για την ενίσχυση της ανθεκτικότητας, συμπεριλαμβανομένης της προστασίας υποδομών ζωτικής σημασίας. Η δέσμευση αυτή συνεπάγεται τόσο την αύξηση όσο και την αναδιάρθρωση των αμυντικών δαπανών.

6. Στρατηγικές Συστάσεις προς την Ηγεσία της Ευρώπης

Τα στρατηγικά πλεονεκτήματα της Ευρώπης συνοψίζονται στους εξής άξονες: στην παρουσία τεχνολογικά πρωτοπόρων παρόχων και προμηθευτών, στα εκτενή δίκτυα και στην αναγνώριση της καθοριστικής σημασίας που ενέχει η ανθεκτικότητα. Καθώς οι απειλές γίνονται ολοένα πιο σύνθετες και στοχευμένες, η Ευρώπη οφείλει να αποφύγει την επιβολή πρόσθετου κανονιστικού φόρτου. Αντιθέτως, επιβάλλεται να συμπράξει με αξιόπιστους παρόχους, προκειμένου να ενσωματώσει οργανικά τη συνδεσιμότητα στις αμυντικές της υποδομές.

Πέντε προτεραιότητες ξεχωρίζουν για τους Ευρωπαίους ηγέτες:

α. Ενσωμάτωση της ασφαλούς συνδεσιμότητας στην εθνική στρατηγική ασφάλειας

Η ασφαλής συνδεσιμότητα θα πρέπει να αναγνωρίζεται ρητά ως πόρος στρατηγικής σημασίας στις εθνικές στρατηγικές, στα στρατηγικά έγγραφα της ΕΕ και στον σχεδιασμό του NATO. Τόσο η ΕΕ όσο και το NATO αναγνωρίζουν ήδη τη σημασία των δικτύων επικοινωνίας για την ανθεκτικότητα. Πλέον, οφείλουν να τα αντιμετωπίζουν ως βασικές επιχειρησιακές δυνατότητες. Αυτό συνεπάγεται την ενσωμάτωση της ψηφιακής υποδομής ως κύριο δομικό τμήμα στις αλυσίδες εφοδιασμού και στον αμυντικό σχεδιασμό, καθώς και τη διασφάλιση ότι οι επενδύσεις στη συνδεσιμότητα αποκτούν την ίδια προτεραιότητα με τις υπόλοιπες δαπάνες για την άμυνα και την ενίσχυση της ανθεκτικότητας.

β. Ενδυνάμωση της πανευρωπαϊκής συνεργασίας και των συμπράξεων μεταξύ κυβερνήσεων και παρόχων

Ο αποσπασματικός συντονισμός δεν επαρκεί πλέον. Για την αποτελεσματική αντιμετώπιση των υβριδικών απειλών, κυβερνήσεις και πάροχοι χρειάζονται επίσημους μηχανισμούς συνεργασίας που να συνδέουν εθνικές, ευρωπαϊκές και NATOικές δομές. Οι μηχανισμοί αυτοί θα πρέπει να περιλαμβάνουν διασυνοριακά φόρουμ διαχείρισης κρίσεων, κοινά πρωτόκολλα αναφοράς περιστατικών και τακτικές κοινές ασκήσεις, ώστε να διασφαλίζεται η συντονισμένη ανταπόκριση σε όλα τα στάδια εν όψει ενός επικείμενου συμβάντος.

Οι ηγέτες οφείλουν να δώσουν προτεραιότητα στη συνεργασία με αξιόπιστους παρόχους που διαθέτουν διασυνοριακές δυνατότητες. Δεδομένου ότι οι υβριδικές απειλές υπερβαίνουν τα εθνικά σύνορα, η ανθεκτικότητα εξαρτάται από εταίρους των οποίων το μέγεθος βελτιώνει σημαντικά την ανίχνευση, την απόκριση και τη διαρκή παροχή υπηρεσιών.

Η ηγεσία της ΕΕ και των κρατών μελών οφείλει να ενισχύσει τον πανευρωπαϊκό συντονισμό για την προστασία υποδομών δικτύου ζωτικής σημασίας, όπως είναι τα υποθαλάσσια καλώδια, οι δορυφόροι και τα κυβερνοσυστήματα. Για παράδειγμα, είναι επιτακτική η ανάπτυξη κοινής ικανότητας απόκρισης για τα υποθαλάσσια καλώδια, ενώ απαιτείται και η ανάπτυξη μηχανισμών επισκευής υπό ευρωπαϊκή εποπτεία. Η πανευρωπαϊκή συνεργασία οφείλει επίσης να επεκταθεί στον τομέα των δορυφορικών επικοινωνιών, στην ενδυνάμωση της ανθεκτικότητας των χερσαίων σταθμών και στην καθιέρωση ενιαίων προτύπων και πιστοποιήσεων στον τομέα της κυβερνοασφάλειας.

γ. Επένδυση στην ανθεκτικότητα εκεί που οι αγορές δεν επαρκούν

Παρόλο που οι ανταγωνιστικές αγορές μπορούν να προωθήσουν την καινοτομία, εντούτοις, ο κατακερματισμός του ευρωπαϊκού τηλεπικοινωνιακού τομέα και η πληθώρα παρόχων μικρής εμβέλειας παρεμποδίζουν την υλοποίηση επενδύσεων στην επιχειρησιακή εφεδρεία και στη θωράκιση της προστασίας υποδομών ζωτικής σημασίας. Οι κυβερνήσεις καλούνται να εντοπίσουν τις οδούς και τους κόμβους υψηλής σημασίας, όπου απαιτείται μεγαλύτερη ανθεκτικότητα, και να αξιοποιήσουν στοχευμένα εργαλεία χρηματοδότησης, εγγυήσεις και ρυθμιστικά κίνητρα για την κάλυψη του επενδυτικού κενού. Παράλληλα, οι πολιτικοί ηγέτες οφείλουν να αναγνωρίσουν και να στηρίξουν τις επενδυτικές πρωτοβουλίες των παρόχων στον τομέα της ασφάλειας και της ανθεκτικότητας, μεταξύ άλλων, διασφαλίζοντας τη σταθερότητα, τη συνέπεια και την προβλεψιμότητα του ρυθμιστικού πλαισίου σε ολόκληρη την Ευρωπαϊκή Ένωση.

δ. Υιοθέτηση μιας στρατηγικά ανοιχτής προσέγγισης στην τεχνολογική κυριαρχία

Οι Ευρωπαίοι ηγέτες αναγνωρίζουν ότι ο έλεγχος επί των κρίσιμων ψηφιακών υποδομών αποτελεί απαραίτητη προϋπόθεση για τη μακροπρόθεσμη ασφάλεια της Ευρώπης. Η τεχνητή νοημοσύνη, το cloud computing και η προηγμένη συνδεσιμότητα συνιστούν θεμελιώδεις τεχνολογίες για τη σύγχρονη άμυνα.

Επί του παρόντος, περιορισμένος αριθμός μη ευρωπαϊκών παρόχων δεσπόζει στην αγορά των υπηρεσιών cloud και της τεχνητής νοημοσύνης. Το γεγονός αυτό οδήγησε σε επιτακτικές εκκλήσεις για την ενίσχυση εγχώριων, κυρίαρχων λύσεων ευρωπαϊκής εμβέλειας. Ωστόσο, η εν λόγω φιλοδοξία οφείλει να μετριάζεται ρεαλιστικά. Η διακοπή της πρόσβασης σε αυτές τις τεχνολογίες θα επιβραδύνει σημαντικά τον ψηφιακό μετασχηματισμό και θα υποσκάψει την παραγωγικότητα. Αντίθετα, η Ευρώπη πρέπει να υιοθετήσει μια προσέγγιση άμβλυνσης κινδύνου και όχι αποκλεισμού, ενισχύοντας τον έλεγχο χωρίς να απομονωθεί από την παγκόσμια καινοτομία αιχμής. Αντί να επικεντρώνεται στην έδρα μια εταιρείας, η προσέγγιση της στρατηγικής κυριαρχίας πρέπει να δίνει προτεραιότητα στις τοπικές επενδύσεις, στην Έρευνα και Ανάπτυξη, τη δημιουργία θέσεων εργασίας και τη μεταφορά τεχνογνωσίας εντός Ευρώπης. Ενθαρρύνοντας τις εταιρείες να αναπτύσσουν και να διατηρούν τις ικανότητές τους στην ευρωπαϊκή επικράτεια, η ΕΕ ενισχύει τη βιομηχανική της βάση, τις εφοδιαστικές αλυσίδες και τη μακροπρόθεσμη ανταγωνιστικότητά της, διασφαλίζοντας ταυτόχρονα την οικονομική της ασφάλεια.

Η μελλοντική ασφάλεια της Ευρώπης και των συμμάχων της θα εξαρτηθεί από την ικανότητά της να αναπτύσσει τεχνολογίες αιχμής σε αναδυόμενους τομείς, όπως η προηγμένη συνδεσιμότητα, η κβαντική ασφάλεια και η κυβερνοασφάλεια. Για τον σκοπό αυτό, η Ευρώπη πρέπει να οικοδομήσει συνεργασίες με χώρες που μοιράζονται το ίδιο όραμα, όπως είναι η Ιαπωνία, η Νότια Κορέα και το Ηνωμένο Βασίλειο, για την από κοινού ανάπτυξη βασικών τεχνολογιών, την κοινή χρήση πόρων και την εναρμόνιση των σχετικών προτύπων.

Οι διαχρονικές συνεργασίες της Ευρώπης στους τομείς της άμυνας, της ασφάλειας και της οικονομίας πρέπει να αναπροσαρμοστούν, ώστε να ανταποκρίνονται στις νέες συνθήκες ενός πολέμου που διεξάγεται πλέον σε πολλαπλά και αλληλένδετα πεδία. Οι επενδύσεις οφείλουν να εναρμονιστούν αναλόγως. Η πρόσφατη διμερής συμφωνία μεταξύ Γερμανίας και Ηνωμένου Βασιλείου για την ενίσχυση της συνεργασίας στον τομέα της άμυνας και των τεχνολογιών ζωτικής σημασίας συνιστά ένα εύγλωττο παράδειγμα αυτής της κατεύθυνσης.

ε. Ενίσχυση της κοινωνικής ανθεκτικότητας μέσω του ψηφιακού εγγραμματισμού

Εν όψει της κλιμάκωσης του πολέμου της πληροφορίας στην Ευρώπη, η επένδυση στην ψηφιακή ένταξη και την ψηφιακή παιδεία θα θωρακίσει τους πολίτες, επιτρέποντάς τους να αναγνωρίζουν την παραπληροφόρηση, να ανθίστανται στη χειραγώγηση και να διατηρούν την εμπιστοσύνη τους στους δημοκρατικούς θεσμούς σε περιόδους κρίσης. Η έκθεση της Vodafone με τίτλο «A Bridge Across Communities» (Σεπτέμβριος 2025) παραθέτει περισσότερες λεπτομέρειες σχετικά με τη σημασία της δημοκρατικής ανθεκτικότητας και τους τρόπους με τους οποίους η Ευρώπη μπορεί να την ενδυναμώσει.²⁶

7. Συμπέρασμα-Ένας νέος πυλώνας της Ευρωπαϊκής Άμυνας

Η ασφαλής συνδεσιμότητα είναι το θεμέλιο πάνω στο οποίο στηρίζονται σήμερα η άμυνα, η ανθεκτικότητα και η ευημερία της Ευρώπης. Εάν δεν δοθεί η απαραίτητη προσοχή το πεδίο αυτό ενδέχεται να μετατραπεί σε εστία στρατηγικής τρωτότητας.

Ενώ οι αντίπαλοι επιδιώκουν να εντοπίσουν και να πλήξουν τις ψηφιακές αρτηρίες των ανοικτών κοινωνιών, η Ευρώπη δεν μπορεί πλέον να προσεγγίζει τη συνδεσιμότητα ως μια δευτερεύουσα υπηρεσία που παρέχεται με γνώμονα αποκλειστικά το χαμηλότερο δυνατό κόστος. Τα δίκτυα, τα δεδομένα και οι υπηρεσίες οφείλουν να αντιμετωπίζονται με την ίδια στρατηγική προσήλωση που διέπει την άμυνα στην ξηρά, τη θάλασσα, τον αέρα, το διάστημα και τον κυβερνοχώρο.

Η Ευρώπη διαθέτει κορυφαίους παρόχους, τεχνολογίες αιχμής, παράδοση διατλαντικής συνεργασίας, καθώς και απaráμιλλη τεχνογνωσία στη διαμόρφωση ρυθμιστικών πλαισίων και διεθνών προτύπων. Η πρόκληση και ταυτόχρονα η ευκαιρία, είναι η αξιοποίηση αυτών των πλεονεκτημάτων στο πλαίσιο μιας τολμηρής και ολοκληρωμένης στρατηγικής, η οποία θα αναδείξει την ασφαλή συνδεσιμότητα σε ακρογωνιαίο λίθο της στρατηγικής ισχύος της Ευρώπης.

Το ευρωπαϊκό πλαίσιο ασφάλειας απαιτεί ριζική αναθεώρηση. Η συνδεσιμότητα οφείλει να αποτελέσει δομικό στοιχείο του κεντρικού σχεδιασμού, υποστηριζόμενη από μηχανισμούς διασυννοριακού συντονισμού και ανθεκτικότητας σε περιόδους κρίσης. Η θωράκιση έναντι υβριδικών απειλών και η θεσμοθέτηση της σύμπραξης μεταξύ δημόσιου και ιδιωτικού τομέα θα αποδειχθούν καθοριστικής σημασίας για τη διασφάλιση της μακροπρόθεσμης σταθερότητας.

Οι αποφάσεις που λαμβάνονται σήμερα αναφορικά με το μοντέλο επενδύσεων, κανονιστικής ρύθμισης και συνεργασίας στον τομέα της συνδεσιμότητας, θα καθορίσουν το επίπεδο ασφαλείας της Ευρώπης για τις επόμενες δεκαετίες. Η ασφαλής συνδεσιμότητα δεν επιτρέπεται πλέον να προσεγγίζεται ως δευτερεύουσα προτεραιότητα. Οφείλει να αναγνωριστεί ως θεμέλιος λίθος της ευρωπαϊκής άμυνας. Συνιστά την αναγκαία συνθήκη για την προστασία των πολιτών και τη θωράκιση των δημοκρατικών αξιών σε ένα διεθνές περιβάλλον που χαρακτηρίζεται από αυξανόμενη πολυπλοκότητα και επίμονες υβριδικές προκλήσεις.

8. Υποσημειώσεις

¹ European Commission, *Investment and funding needs for the Digital Decade connectivity targets*, July 2023

² Check Point Research, *Global Cyber Attacks Surge 21% in Q2 2025, Europe Experiences the Highest Increase of All Regions*, July 2025, and Charlie Edwards, Nate Seidenstein, *The scale of Russian sabotage operations against Europe's critical infrastructure*, International Institute for Strategic Studies, August 2025

³ European Commission, *White paper for European defence - Readiness 2030*, March 2025

⁴ NATO, *The Hague Summit Declaration*, June 2025

⁵ European Commission, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, October 2024

⁶ Σύμφωνα με την *έρευνα του Ευρωβαρόμετρου της άνοιξης του 2025*, η «Άμυνα και Ασφάλεια» αναδείχθηκε ως η κορυφαία προτεραιότητα που οι Ευρωπαίοι επιθυμούν να ενισχυθεί από την ΕΕ, καθώς επιλέχθηκε από το 37% των ερωτηθέντων

⁷ Poudel, A., Argyroudis, S., and Pitilakis, K, Systemic seismic risk assessment of urban healthcare system considering interdependencies to critical infrastructures. *International Journal of Disaster Risk Reduction*, 2024

⁸ Joan Faus, Post-blackout in Spain and Portugal, companies count the cost, Reuters, April 2025

⁹ El País, *What remains unknown about the massive blackout in Spain*, April 2025

¹⁰ Cyber Peace Institute, *Case Study Viasat*, June 2022

¹¹ UNESCO, *Survey on the impact of online disinformation and hate speech*, September 2023, and World Economic Forum, *The Global Risks Report 2025*, 15 January 2025

¹² Chatham House, *Ensuring cyber resilience NATO's command, control and communication systems*, July 2020

¹³ Vodafone, *Offshore connectivity extends defence capabilities, A case study with the Portuguese Navy*, January 2025

¹⁴ Government of Finland, *New Security Strategy for Society enhances Finland's comprehensive security*

¹⁵ NATO's Baseline Requirements for National Resilience (2016, updated 2023) and NATO - Topic: Resilience, civil preparedness and Article 3

¹⁶ Andrea Lamberti (Arel), *Much More than a Network Telecoms as the Bedrock of European Defence*, Single Market Lab, October 2025

¹⁷ Elisabeth Braw, *Financial institutions should prepare for subsea cable sabotage*, *Financial Times*, July 2025

¹⁸ Vodafone, *Global network resilience: a deep dive into our subsea cable infrastructure*, 18 August 2025

¹⁹ Σύμφωνα με την έκθεση «Threat Landscape 2025» της ENISA, η Ευρώπη αντιμετωπίζει ένα περιβάλλον απειλών που χαρακτηρίζεται από ολοένα και μεγαλύτερη πολυπλοκότητα και σύγκλιση, με ασαφή όρια μεταξύ κρατικών, εγκληματικών και χακτιβιστικών δραστηριοτήτων, την ευρεία χρήση της τεχνητής νοημοσύνης, καθώς και από το έγκλημα στον κυβερνοχώρο που στοχεύει τις δημόσιες διοικήσεις και τις υποδομές ζωτικής σημασίας. Πηγές: ENISA, *Threat Landscape 2025*, Οκτώβριος 2025, και Bitkom, *Study Corporate Security 2024*, 2024.

²⁰ Vodafone, *Case study incident, Vodafone Portugal*, February 2022

²¹ Άλλες υπηρεσίες ανακτήθηκαν στις επόμενες 48 ώρες (βλ. Vodafone Group, *Cyber Security Factsheet 2023*, < <https://reports.investors.vodafone.com/view/919554535/> >) και υπόθεση μελέτης, Vodafone Portugal, *ibid.*)

²² Vodafone, *Vodafone and AST SpaceMobile choose Luxembourg as joint venture headquarters to drive European-wide space-based mobile broadband coverage*, 30 June 2025

²³ Franciszek Besztej/jk, *Sweden warns of almost daily GPS jamming in Baltic region, traced to Russia*, TVP World, September 2025

²⁴ European Commission, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, *ibid.*

²⁵ NATO, *Defence Expenditure of NATO Countries (2014-2025)*, August 2025

²⁶ Vodafone, *Digital inclusion key to tackling Europe's €1.3 trillion digital transformation gap*, September 2025