



ΤΟΜΕΙΣ ΟΠΟΥ ΑΝΗΚΟΥΝ ΟΙ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ

- Ενέργεια
- Μεταφορές
- Τραπεζικούς τομείς
- Χρηματοπιστωτικά ιδρύματα
- Υγειονομικούς τομείς
- Υδρευση
- Διαχείριση λυμάτων
- Ψηφιακές υποδομές
- Δημόσια Διοίκηση
- Διάσπαρτα
- Επισιτιστικούς τομείς

ΟΙ ΚΥΡΙΕΣ ΑΠΕΙΛΕΣ ΓΙΑ ΤΙΣ ΚΡΙΣΙΜΕΣ ΥΠΟΔΟΜΕΣ

- Εχθρική στρατιωτική ενέργεια
- Τρομοκρατική επίθεση
- Εγκληματική ενέργεια
- Κυβερνοεπίθεση
- Υβριδικές απειλές
- Κακόβουλη χρήση νέων τεχνολογιών
- Εκ των έσω απειλή
- Φυσικές καταστροφές
- Τεχνολογικές καταστροφές και ατυχήματα
- Παραπληροφόρηση - επικοινωνιακή χειραγώγηση
- Ανθρώπινη αμέλεια

ΧΡΟΝΟΛΟΓΙΟ ΠΡΟΒΛΗΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ ΣΤΗΝ ΕΥΡΩΠΗ

2015 ΟΥΚΡΑΝΙΑ
Κυβερνοεπίθεση στο δίκτυο ηλεκτρικής ενέργειας

2016 ΒΕΛΓΙΟ
Τρομοκρατικές επιθέσεις στο αεροδρόμιο Zaventem και στο μετρό των Βρυξελλών

2021 ΓΕΡΜΑΝΙΑ, ΒΕΛΓΙΟ
Μεγάλες πλημμύρες προκαλούν ζημιές σε υποδομές ενέργειας, μεταφορών και ύδρευσης

2021 ΙΣΠΑΝΙΑ, ΙΤΑΛΙΑ
Μεγάλες πυρκαγιές προκαλούν ζημιές σε δίκτυα ηλεκτρισμού και τηλεπικοινωνιών

2022 Σαμποτάζ
και υποθαλάσσια δολιοφθορά στους αγωγούς Nord Stream

2025 ΣΕΠ. ΒΕΛΓΙΟ, ΓΕΡΜΑΝΙΑ ΚΑΙ ΒΡΕΤΑΝΙΑ
Κυβερνοεπίθεση σε λογισμικό check-in επηρεάζει τα συστήματα αεροδρομίων

2025 ΣΕΠ. ΔΑΝΙΑ
Υπέρηχη drones πάνω από το αεροδρόμιο της Κοπεγχάγης και του Οσλό προκαλεί κίνδυνο για την ασφάλεια της εναέριας κυκλοφορίας και προκαλεί καθυστερήσεις και διακοπή λειτουργίας

Το blackout στο FIR Αθηνών έφερε ξανά στη συζήτηση το ζήτημα της ασφάλειας των κρίσιμων υποδομών. Από το 2022 και κυρίως μετά την εισβολή της Ρωσίας στην Ουκρανία και την απειλή από τη Ρωσία για την ευρωπαϊκή ασφάλεια, η συγκεκριμένη προτεραιότητα προσεγγίζεται κυρίως μέσα από το πλαίσιο των υβριδικών απειλών. Με χαρακτηριστικές περιπτώσεις τις κυβερνοεπιθέσεις σε συστήματα web check-in που επηρέασαν μεγάλα ευρωπαϊκά αεροδρόμια, τις υπερπτήσεις drones που οδήγησαν σε καθυστερήσεις και ακυρώσεις πτήσεων, αλλά και το blackout στην Ισπανία και στην Πορτογαλία.

Η στοχοποίηση των κρίσιμων υποδομών έχει καίρια θέση και στο πλαίσιο των πολεμικών συγκρούσεων, κάτι που είδαμε χαρακτηριστικά και πολλές φορές στον πόλεμο στην Ουκρανία. Όπως για παράδειγμα στις 25 Δεκεμβρίου 2024, όταν η Ρωσία εξέπελυσε επίθεση με 78 πυραύλους και 106 drones εναντίον θερμοηλεκτρικών και υδροηλεκτρικών σταθμών σε διάφορες περιοχές της Ουκρανίας, προκαλώντας πρόβλημα ηλεκτροδότησης σε περισσότερους από 100.000 πολίτες. Αντίστοιχα, στα μέσα Νοεμβρίου 2025, η Ουκρανία πραγματοποίησε επιθέσεις με drones και πυραύλους σε πετρελαϊκές υποδομές της Ρωσίας στο Νοβοροσίσκ, προκαλώντας ζημιές σε δεξαμενές καυσίμων και εγκαταστάσεις φόρτισης, οδηγώντας σε προσωρινή διακοπή των εξαγωγών πετρελαίου και άνοδο των τιμών του αργού πετρελαίου.

Η ίδια η ΕΕ, με αφορμή τη δολιοφθορά στους αγωγούς Nord Stream έτρεξε γρήγορα τις θεσμικές της πρωτοβουλίες, με αιχμή τις διδυμες Οδηγίες CER – για την ανθεκτικότητα των κρίσιμων οντοτήτων –

Καμπανάκι για τις κρίσιμες υποδομές

Η συζήτηση για τα ζητήματα ασφάλειας φούντωσε ξανά μετά το blackout στο FIR Αθηνών



ΤΟΥ ΤΡΙΑΝΤΑΦΥΛΛΟΥ ΚΑΡΑΤΡΑΝΤΟΥ

και NIS II – για ένα κοινό υψηλό επίπεδο κυβερνοασφάλειας στην Ένωση. Από αυτό το σημείο η φράση ανθεκτικότητα κρίσιμων οντοτήτων έχει γίνει mantra για όσους ασχολούνται με το ζήτημα.

Τι περιλαμβάνει όμως αυτό το τεχνοκρατικό σχήμα; Ας ξεκινήσουμε με τη μετάβαση από την υποδομή στην οντότητα, η οποία δεν έγινε για λόγους εντυπωσιασμού, αλλά γιατί οι ευρωπαϊκές υποδομές και κυρίως τα δίκτυα, στην εποχή της 4ης βιομηχανικής επανάστασης, έχουν γίνει περισσότερο διασυνδεδεμένες και αλληλεξαρτώμενες, γεγονός που τις καθιστά ισχυρότερες και αποτελεσματικότερες, αλλά και πιο εύλατες σε περίπτωση περιστατικού. Είναι σημαντικό πως οι υποδομές, εκτός από το φυσικό πεδίο, έχουν πλέον και ένα ξεκάθαρο ψηφιακό, κάτι που οδήγησε την ΕΕ στη μετάβαση στην έννοια κρίσιμες οντότητες.

Κρίσιμη λοιπόν είναι η οντότητα, δημόσια ή ιδιωτική, η οποία παρέχει μια υπηρεσία ή ένα αγαθό, καθοριστικής σημασίας για τη διατήρηση ζωτικών κοινωνικών λειτουργιών, οικονομικών δραστηριοτήτων, της δημόσιας υγείας και ασφάλειας ή του περιβάλλοντος. Ως εκ τούτου, η διακοπή λειτουργίας ή η καταστροφή μιας κρίσιμης οντότητας μπορεί να έχει σημαντικό αντίκτυπο για μια χώρα. Για παράδειγμα, κρίσιμες οντότητες στην περίπτωση της Ελλάδας είναι, μεταξύ άλλων, η ΔΕΗ, το Λιμάνι του Πειραιά, το Διεθνές Αεροδρόμιο Ελευθέριος Βενιζέλος, η ΔΕΕΦΑ, η ΕΥΔΑΠ, η ΣΤΑΣΥ, η Helleniq Energy κ.ά. Δεν είναι όμως η πρώτη φορά που η ΕΕ, αλλά και τα κράτη της Δύσης ασχολούνται με τις κρίσιμες υποδομές. Οι επιθέσεις της 11ης Σεπτεμβρίου στις ΗΠΑ που βασίστηκαν στη χρήση αεροπλάνων ως όπλων των τρομοκρατών, αλλά και οι επιθέσεις της 11ης Μαρτίου 2004 στο σιδηροδρομικό δίκτυο της Μαδρίτης, έφεραν στη δημόσια συζήτηση, με τον πλέον δραματικό τρόπο, την ασφάλεια των μεταφορών. Σύντομα, τόσο η ΕΕ, όσο και οι ΗΠΑ, ενέταξαν την ασφάλεια των μεταφορών στο ευρύτερο πεδίο των κρίσιμων υποδομών.

Η ασφάλεια λοιπόν των κρίσιμων υποδομών είναι ένα από τα πλέον ραγδαία αναπτυσσόμενα πεδία της δημόσιας πολιτικής και της πολιτικής ασφάλειας και προστασίας, στο οποίο η ΕΕ έχει κάνει σημαντικά βήματα τα τελευταία χρόνια, καθώς εξέδωσε την πρώτη σχετικά Οδηγία το 2008. Ωστόσο, δεν είναι μία εύκολη διαδικασία, καθώς προϋποθέτει την εμπλοκή και τη συνεργασία πολλών και διαφορετικών φορέων του Δημοσίου, αλλά και του ιδιωτικού τομέα. Είναι χαρακτηριστικό πως σε αρκετές περιπτώσεις πολλές χώρες δεν έχουν προσδιορίσει τις



κρίσιμες υποδομές τους, ενώ και όπου αυτές έχουν προσδιοριστεί, υπάρχουν σημαντικές διαφοροποιήσεις μεταξύ των χωρών.

Οι τρομοκρατικές επιθέσεις που συγκλόνισαν τα κράτη - μέλη της ΕΕ κατά την περίοδο 2015 - 2016, και ορισμένες εξ αυτών είχαν ως στόχο αεροδρόμια, μετρό και τρένα, κατέστησαν την προστασία των κρίσιμων υποδομών πρώτη προτεραιότητα. Η εξέλιξη όμως των απειλών, με την ραγδαία αύξηση των κινδύνων στον τομέα της κυβερνοασφάλειας και ο συνδυασμός τους με τις υβριδικές απειλές, αλλά και τη λεγόμενη «απειλή εκ των έσω» (insider threat), οδήγησαν και στη μετεξέλιξη του ευρωπαϊκού πλαισίου ασφάλειας των κρίσιμων υποδομών και η ΕΕ υιοθέτησε το πρόταγμα της ανθεκτικότητας.

Από το πιο στατικό σχήμα της προστασίας περάσαμε στον στόχο της ανθεκτικότητας, η οποία περιλαμβάνει και την προστασία και την οποία η ΕΕ ορίζει ως την ικανότητα μιας κρίσιμης οντότητας να προλαμβάνει, να προστατεύει, να αντισταθεί, να αντιστέκεται, να μετριάξει, να απορροφά, να προσαρμόζεται και να ανακάμπτει από κάθε συμβάν που έχει τη δυνατότητα να διαταράξει σημαντικά ή που διαταράσσει την παροχή της βασικής υπηρεσίας της. Η μετάβαση αυτή είναι λογική τόσο από την εξέλιξη των απειλών, αλλά και του υψηλού βαθμού διασύνδεσης και αλληλεξάρτησης λόγω των τεχνολογικών αλλαγών, όσο και από τις κρίσεις των τελευταίων ετών. Ο μηχανισμός διαχείρισης κρίσεων της ΕΕ έχει πλέον προσαρμοστεί στην πραγματικότητα των πολυκρίσεων, για αυτό και η Ένωση έχει συνολικά θέσει ως προτεραιότητα το δίπολο Ετοιμότητα (Readiness) και Ανθεκτικότητα (Resilience). Δεν είναι άλλοστε τυχαίο πως ο τομέας των κρίσιμων υποδομών είναι βασική προτεραιότητα σε όλες τις στρατηγικές στους τομείς της άμυνας και της ασφάλειας που δημοσίευσε η ΕΕ το 2025 (Λευκή Βίβλος για την Ευρωπαϊκή Άμυνα, Στρατηγική για την Ένωση Ετοιμότητας, Στρατηγική για την Εσωτερική Ασφάλεια), όσο και στο πλαίσιο του Προγράμματος SAFE.

ΥΒΡΙΔΙΚΕΣ ΚΑΙ ΑΛΛΕΣ ΑΠΕΙΛΕΣ

Η πλέον πρόσφατη Στρατηγική της ΕΕ, αυτή για την Εσωτερική Ασφάλεια, παρέχει το πλέγμα των απειλών για την εσωτερική ασφάλεια, το οποίο αφορά και τις κρίσιμες οντότητες: υβριδικές απειλές και άλλες εκθρικές ενέργειες, Κυβερνοαπειλές και κυβερνοεπιθέσεις, Κακόβουλη χρήση των αναδυόμενων τεχνολογιών, «Οπλοποίηση» της Μετανάστευσης, Κακόβουλες παρεμβάσεις και εξαρτήσεις στις εφοδιαστικές αλυσίδες, Χημικές - Βιολογικές - Ραδιενεργές και Πυρηνικές (ΧΒΡΠ) απειλές, Σοβαρό και Οργανωμένο Εγκλημα, Βίαιος Εξτρεμιζμός και Τρομοκρατία, Παραπληροφόρηση. Σε αυτές πρέπει να προσθέσουμε τις φυσικές καταστροφές και τα τεχνολογικά ατυχήματα, την ανθρωπινή αμέλεια και το σαμποτάζ εκ των έσω.

Ειδικότερα οι υβριδικές απειλές συνιστούν έναν από τους πλέον σύνθετους και δύσκολους κινδύνους για τις κρίσιμες υποδομές. Συνδυάζοντας κυβερνοεπιθέσεις, οικονομική πίεση, επιχειρήσεις παραπληροφόρησης και πράξεις φυσικής δολιοφθοράς, αξιοποιούν τόσο συγκαλυμμένες όσο και ανοικτές μεθόδους με στόχο την αποσταθεροποίηση. Εκμεταλλευόμενες τη βαθιά διασύνδεση βασικών συστημάτων - όπως η ενέργεια, η

Η ΕΛΛΑΔΑ είναι μια χώρα που έχει για χρόνια παρουσιάσει υστέρηση στο ζήτημα των κρίσιμων υποδομών. κυρίως στην εκπόνηση μιας ολιστικής εθνικής πολιτικής και στον ορισμό ενός κεντρικού σημείου ευθύνης και ελέγχου. Αυτό όμως δεν σημαίνει πως δεν έχουν γίνει όλα αυτά τα χρόνια βήματα για την ενίσχυση της ασφάλειας, κυρίως στους τομείς της ενέργειας, των μεταφορών, αλλά και των ψηφιακών υποδομών, κυρίως από το 2020 και μετά

γαλείων και πρακτικών, τα οποία ενισχύουν αμοιβαία τον αντίκτυπό τους. Κεντρικό ρόλο διαδραματίζουν οι κυβερνοεπιθέσεις, που στοχεύουν τόσο τα πληροφοριακά συστήματα όσο και τα συστήματα επιχειρησιακής τεχνολογίας σε κρίσιμους τομείς, όπως τα δίκτυα ηλεκτρικής ενέργειας, οι εγκαταστάσεις επεξεργασίας νερού και οι χρηματοπιστωτικές υπηρεσίες. Παράλληλα, η οικονομική εξαναγκαστική πίεση αξιοποιεί διαταραχές στις εφοδιαστικές αλυσίδες ή χρηματοοικονομικά εργαλεία με στόχο την αποδυνάμωση της ανθεκτικότητας των υποδομών. Ιδιαίτερη σημασία έχει και ο πληροφοριακός πόλεμος μέσω της συστηματικής διασποράς παραπληροφόρησης που διαβρώνει την εμπιστοσύνη των πολιτών και επηρεάζει τη διαδικασία λήψης αποφάσεων. Τέλος, η φυσική δολιοφθορά, όπως άμεσες επιθέσεις σε κρίσιμες εγκαταστάσεις ή παρεμβάσεις σε θάλασσες υποδομές, συχνά συνδυάζεται με κυβερνοτακτικές, πολλαπλασιάζοντας τον αποσταθεροποιητικό της αντίκτυπο.

Στο στόχαστρο των υβριδικών απειλών βρίσκονται και οι κρίσιμοι τομείς που στηρίζουν την ορατή λειτουργία της κοινωνίας και της οικονομίας. Ιδιαίτερη σημασία έχει ο ενεργειακός τομέας, με τα δίκτυα ηλεκτρικής ενέργειας και τους αγωγούς να αποτελούν κρίσιμα σημεία υψηλής ευπάθειας. Αντίστοιχα, οι υποδομές ύδρευσης και αποχέτευσης, όπως οι μονάδες επεξεργασίας και τα δίκτυα διανομής, αποτελούν δυνητικούς στόχους με άμεσες επιπτώσεις στη δημόσια υγεία. Ο τομέας της υγείας, και ειδικότερα τα νοσοκομεία και τα ψηφιακά αρχεία υγείας, έχει αναδειχθεί σε προνομιακό πεδίο επιθέσεων, λόγω της ζωτικής σημασίας και της αυξημένης ψηφιακής εξάρτησής του. Παράλληλα, ο χρηματοπιστωτικός τομέας, συμπεριλαμβανομένων των συστημάτων πληρωμών, βρίσκεται στο επίκεντρο απειλών που μπορούν να κλονίσουν την οικονομική σταθερότητα. Σημαντικούς κινδύνους αντιμετωπίζουν επίσης οι μεταφορές, τόσο στον αέρα όσο και στη θάλασσα και στην ξηρά, καθώς και οι ψηφιακές υποδομές, όπως τα δίκτυα επικοινωνιών και οι υπηρεσίες υπολογιστικού νέφους, οι οποίες αποτελούν τη ραχοκοκλιά της σύγχρονης διασυνδεδεμένης οικονομίας.

ΠΟΣΟ ΠΡΟΕΤΟΙΜΑΣΜΕΝΗ ΕΙΝΑΙ Η ΕΛΛΑΔΑ;

Η Ελλάδα είναι μια χώρα που έχει για χρόνια παρουσιάσει υστέρηση στο ζήτημα των κρίσιμων υποδομών, κυρίως στην εκπόνηση μιας ολιστικής εθνικής πολιτικής και στον ορισμό ενός κεντρικού σημείου ευθύνης και ελέγχου. Αυτό όμως δεν σημαίνει πως δεν έχουν γίνει όλα αυτά τα χρόνια βήματα για την ενίσχυση της ασφάλειας, κυρίως στους τομείς της ενέργειας, των μεταφορών, αλλά και των ψηφιακών υποδομών, κυρίως από το 2020 και μετά. Σημαντικό ρόλο σε αυτή την προετοιμασία διαδραμάτισε το Κέντρο Μελετών Ασφάλειας (ΚΕΜΕΑ) του υπουργείου Προστασίας του Πολίτη, το οποίο έχει υλοποιήσει σειρά εκπαιδευτικών και ασκήσεων, με τη συμμετοχή στελεχών από τις ίδιες τις κρίσιμες υποδομές. Μια διαδικασία που συνέβαλε καθοριστικά στο να καλλιεργηθεί μια κουλτούρα ασφάλειας, η οποία είναι ιδιαίτερως σημαντική για την εφαρμογή του νέου πλαισίου που θέτει η Οδηγία CER.

Σε αυτό το πλαίσιο, η Ελλάδα είναι μια από τις λίγες χώρες που ενσωμάτωσαν πλήρως την Οδηγία για την Ανθεκτικότητα των Κρίσιμων Οντοτήτων με τον Νόμο 5236 που ψηφίστηκε τον Οκτώβριο του 2025. Σύμφωνα με τον Νόμο, η αρμοδιότητα της ανθεκτικότητας των κρίσιμων οντοτήτων ανήκει στο υπουργείο Προστασίας του Πολίτη, όπου και ιδρύθηκε μια νέα Γενική Γραμματεία με κύρια αποστολή την προστασία των κρίσιμων οντοτήτων. Οι αρμοδιότητες της Γενικής Γραμματείας περιλαμβάνουν τη σύνταξη Εθνικής Στρατηγικής και αξιολόγησης κινδύνων, τον προσδιορισμό των κρίσιμων οντοτήτων, την εποπτεία εφαρμογής του Νόμου από τις κρίσιμες οντότητες, τη συνδρομή προς τις οντότητες σε εκπαιδευτικό και συμβουλευτικό επίπεδο, τον καθορισμό των υποχρεώσεών τους και τη θέσπιση μέτρων για επίτευξη υψηλού επιπέδου ανθεκτικότητας και όπου χρειάζεται την επιβολή κυρώσεων. Είναι η πρώτη φορά που η χώρα αποκτά ένα ολιστικό και συνεκτικό θεσμικό πλαίσιο για μια τόσο περίπλοκη και κρίσιμη δημόσια πολιτική, όπως είναι αυτή της ανθεκτικότητας των κρίσιμων οντοτήτων.

Ο σχεδιασμός πολιτικής για την ανθεκτικότητα των κρίσιμων οντοτήτων είναι μια δύσκολη και απαιτητική άσκηση που πρέπει, μεταξύ άλλων, να περιλαμβάνει τον καθορισμό των εθνικών κρίσιμων υποδομών ανά τομέα ακολουθώντας τη λογική της Οδηγίας CER, τη δημιουργία ψηφιακής εθνικής βάσης δεδομένων, τον καθορισμό εθνικών standards ασφάλειας υποδομών και διαδικασιών ελέγχου και πιστοποίησης της εφαρμογής τους, τις συνέργειες με την ακαδημαϊκή και την ερευνητική κοινότητα, τόσο για την ανάδειξη μελλοντικών τάσεων, όσο και για τον καλύτερο σχεδιασμό ασφάλειας, την αξιοποίηση μεθοδολογιών foresight για τις μελέτες επικινδυνότητας, τη χρήση νέων τεχνολογικών εργαλείων και συστημάτων έγκαιρης προειδοποίησης για την ενίσχυση της ασφάλειας και την αποτροπή των κινδύνων και τέλος την ενίσχυση των συνεργειών δημοσίου και ιδιωτικού τομέα.

ύδρευση, το χρηματοπιστωτικό σύστημα και οι μεταφορές - επιδιώκουν να υπονομεύσουν την κοινωνική εμπιστοσύνη, λειτουργώντας συστηματικά κάτω από το πλαίσιο της παραδοσιακής πολεμικής σύγκρουσης. Οι ενέργειες αυτές, δύσκολα ανιχνεύσιμες και ακόμη δυσκολότερα αποδιδόμενες ως προς την ευθύνη, αξιοποιούν ψηφιακές ευπάθειες και αδυναμίες στις εφοδιαστικές αλυσίδες για την πρόκληση στρατηγικής αποδιοργάνωσης, με άμεσες επιπτώσεις στη λειτουργία κρίσιμων υπηρεσιών και στη συνολική ανθεκτικότητα των κρατών. Οι υβριδικές απειλές εκδηλώνονται μέσα από έναν συνδυασμό συμπληρωματικών ερ-



Ο Τρανσφύλλιος Καρπαράτος, έρ Ευρωπαϊκής Ασφάλειας και Νέων Απειλών, είναι επιστημονικός συνεργάτης ΕΛΙΑΜΕΠ