ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ
ΓΡΑΦΕΙΟ ΥΠΟΥΡΓΟΥ
Δ/ΝΣΗ: Φραγκούδη 11 & Αλ. Πάντου,
Καλλιθέα Αθήνα, ΤΚ 101 63,
Τηλ.: 2109098600
E-mail: minister@mindigital.gr

ΑΡ. ΠΡΩΤ. 2563/16.12.2025

ΘΕΜΑ: «Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026 – 2030»

ΑΠΟΦΑΣΗ
Ο ΥΠΟΥΡΓΟΣ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

Έχοντας υπόψη:

1. Τις διατάξεις:

α) του ν. 5160/2024 «Ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Δεκεμβρίου 2022, σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, την τροποποίηση του Κανονισμού (ΕΕ) 910/2014 και της Οδηγίας (ΕΕ) 2018/1972, και την κατάργηση της Οδηγίας (ΕΕ) 2016/1148 (Οδηγία NIS 2) και άλλες διατάξεις» (Α΄195) και ιδίως του άρθρου 7 και της παρ. 5 του άρθρου 30 αυτού,

β) του ν. 5086/2024 «Εθνική Αρχή Κυβερνοασφάλειας και λοιπές διατάξεις» (Α΄23),

γ) του π.δ. 79/2023 «Διορισμός Υπουργών, Αναπληρωτών Υπουργών και Υφυπουργών» (Α' 131),

δ) του π.δ. 40/2020 «Οργανισμός του Υπουργείου Ψηφιακής Διακυβέρνησης» (Α' 85) και

ε) του π.δ. 81/2019 «Σύσταση, συγχώνευση, μετονο-μασία και κατάργηση Υπουργείων και καθορισμός των αρμοδιοτήτων τους - Μεταφορά υπηρεσιών και αρμοδιοτήτων μεταξύ Υπουργείων» (Α' 119).

2. Την υπό στοιχεία 34368/07.12.2020 απόφαση του Υπουργού Επικρατείας «Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020 – 2025» (ΑΔΑ: 6ΙΒΕ46ΜΤΛΠ-ΦΜ5).

3. Την υπό στοιχεία 42983 ΕΞ/16.12.2025 γνώμη του Διοικητή της Εθνικής Αρχής Κυβερνοασφάλειας.

4. Την ανάγκη επικαιροποίησης της υφιστάμενης Εθνικής Στρατηγικής Κυβερνοασφάλειας και έκδοσης νέας Εθνικής Στρατηγικής Κυβερνοασφάλειας για τα έτη 2026 – 2030.

ΑΠΟΦΑΣΙΖΟΥΜΕ

Την έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026-2030, όπως αυτή αποτυπώνεται ακολούθως, σύμφωνα με τα οριζόμενα στο άρθρο 7 του ν. 5160/2024.

Ο ΥΠΟΥΡΓΟΣ ΨΗΦΙΑΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ

ΔΗΜΗΤΡΙΟΣ ΠΑΠΑΣΤΕΡΓΙΟΥ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟ ΑΣΦΑΛΕΙΑΣ

Εθνική Στρατηγική Κυβερνοασφάλειας 2026 – 2030

Δεκέμβριος 2025

Μήνυμα Διοικητή ΕΑΚ

Ζούμε σε μια εποχή όπου η τεχνολογία δεν είναι πια αφηρημένη έννοια. Είναι το περιβάλλον μέσα στο οποίο λειτουργούμε καθημερινά. Από τις δημόσιες υπηρεσίες και τις επιχειρήσεις, μέχρι τις πιο απλές προσωπικές μας συνήθειες. Η ψηφιακή εξάρτηση μεγαλώνει και μαζί της μεγαλώνουν και οι ευκαιρίες, αλλά και οι κίνδυνοι. Το ζητούμενο δεν είναι να φοβόμαστε την τεχνολογία, αλλά να τη χρησιμοποιούμε συνειδητά και με τρόπο που ενισχύει την ασφάλεια και την ανθεκτικότητα της χώρας.

Η Εθνική Στρατηγική Κυβερνοασφάλειας 2026–2030 επιχειρεί ακριβώς αυτό. Να δημιουργήσει ένα σταθερό και εφαρμόσιμο πλαίσιο που βοηθά το κράτος, τις επιχειρήσεις και τους πολίτες να λειτουργούν με ασφάλεια σε ένα περιβάλλον που αλλάζει γρήγορα και συχνά απρόβλεπτα. Δεν πρόκειται για ένα ακόμη θεωρητικό κείμενο πολιτικής αποτελεί έναν πρακτικό οδηγό για το πώς η Ελλάδα θα διαχειριστεί τους κινδύνους στον κυβερνοχώρο τα επόμενα χρόνια.

Οι προκλήσεις είναι πολλές: προηγμένες επιθέσεις, περίπλοκα δίκτυα, εξάρτηση από ψηφιακές υπηρεσίες, νέες τεχνολογίες όπως η τεχνητή νοημοσύνη. Η απάντηση σε όλα αυτά δεν μπορεί να είναι αποσπασματική. Χρειάζεται οργανωμένη δουλειά, τεχνική γνώση, διεπιστημονική προσέγγιση, διαρκή μάθηση και συνεργασία. Χρειάζεται να συνδέσουμε το τεχνολογικό επίπεδο με το ανθρώπινο, διότι το μεγαλύτερο ποσοστό περιστατικών ξεκινά από ανθρώπινα λάθη.

Σε αυτό το πνεύμα, θα ήθελα να υπενθυμίσω μια απλή αλήθεια που συχνά λησμονούμε στο δημόσιο διάλογο γύρω από την τεχνολογία: Η τεχνολογία δεν λύνει από μόνη της προβλήματα. Μεγεθύνει τις δυνατότητες και τις αδυναμίες μας, ταυτόχρονα. Το αποτέλεσμα εξαρτάται πάντα από το πώς τη χρησιμοποιούμε.

Η Στρατηγική δίνει έμφαση σε πέντε βασικούς πυλώνες: ανθεκτικές κρίσιμες υπηρεσίες, σύγχρονο σύστημα διακυβέρνησης, καλλιέργεια δεξιοτήτων, αξιοποίηση ευρωπαϊκών συνεργασιών και πρακτικές λύσεις που μπορούν να υλοποιηθούν στην πράξη. Η επιτυχία της δεν εξαρτάται μόνο από έναν φορέα. Απαιτεί τη συμβολή της δημόσιας διοίκησης, του ιδιωτικού τομέα, των πανεπιστημίων και των πολιτών.

Η Εθνική Αρχή Κυβερνοασφάλειας έχει την ευθύνη του συντονισμού και της καθοδήγησης, αλλά και την υποχρέωση να λειτουργεί με διαφάνεια, επιστημονική τεκμηρίωση και ρεαλισμό. Δεν υπόσχεται ότι οι επιθέσεις θα σταματήσουν. Υπόσχεται όμως ότι η χώρα θα μπορεί να τις αντιμετωπίζει καλύτερα, γρηγορότερα και με μικρότερο κόστος για την κοινωνία και την οικονομία.

Αν δουλέψουμε συστηματικά και με καθαρό μυαλό, μπορούμε να χτίσουμε μια Ελλάδα που θα ωφελείται από την τεχνολογία χωρίς να απειλείται από αυτήν. Αυτός είναι ο στόχος μας για την επόμενη πενταετία.

Μιχάλης Μπλέτσας

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Πίνακας Επεξήγησης Τεχνικών Όρων

Όρος	Επεξήγηση
Ransomware (Λυτρισμικό)	Τύπος κακόβουλου λογισμικού που κρυπτογραφεί ή κλειδώνει τα αρχεία ενός υπολογιστή και απαιτεί λύτρα για να αποκαταστήσει την πρόσβαση.
Malware (Κακόβουλο Λογισμικό)	Λογισμικό ή σύνολο εντολών που σχεδιάζεται για να προκαλέσει ζημιά ή μη εξουσιοδοτημένη πρόσβαση σε συστήματα.
Infostealers	Τύποι κακόβουλου λογισμικού που σχεδιάζονται για να υποκλέπτουν ευαίσθητες πληροφορίες, όπως στοιχεία πρόσβασης (credentials), οικονομικά στοιχεία και άλλα δεδομένα προσωπικού χαρακτήρα.
Phishing / Smishing / Quishing	Εξαπάτηση χρηστών για κλοπή δεδομένων μέσω email / SMS / QR codes αντίστοιχα.
Deepfake	Οπτικοακουστικό υλικό, όπως εικόνες, video ή ήχοι, που έχουν ψηφιακά παραχθεί ή τροποποιηθεί με χρήση τεχνολογιών τεχνητής νοημοσύνης, με σκοπό την κακόβουλη χρήση ή τη διασπορά ψευδών πληροφοριών.
Distributed Denial of Service – DDoS	Είδος κυβερνοεπίθεσης, κατά το οποίο πολλαπλά παραβιασμένα συστήματα υπερφορτώνουν ένα στόχο, όπως έναν ιστότοπο ή διακομιστή, με τεράστιο όγκο δικτυακής κίνησης, ώστε να μη μπορεί να εξυπηρετήσει νόμιμους χρήστες.
Data Breach (Παραβίαση Δεδομένων)	Περιστατικό ασφάλειας κατά το οποίο μη εξουσιοδοτημένα μέρη αποκτούν πρόσβαση σε ευαίσθητες ή εμπιστευτικές πληροφορίες.
Data Leakage (Διαρροή Δεδομένων)	Ακούσια έκθεση δεδομένων λόγω λάθους ή κακής ρύθμισης συστημάτων.
Foreign Information Manipulation and Interference (FIMI)	Χειραγώγηση πληροφορίας από εξωτερικούς παράγοντες για πολιτική/κοινωνική επιρροή.
Supply Chain Attack	Επίθεση σε έναν οργανισμό μέσω της εφοδιαστικής του αλυσίδας.
Cybercrime-as-a-Service (CaaS)	Παροχή εργαλείων κυβερνοεγκλήματος ως υπηρεσία σε τρίτους (PaaS, RaaS, MaaS, DaaS).
Hackers-for-hire	Επαγγελματίες επιτιθέμενοι που «εκμισθώνουν» τις υπηρεσίες τους για τη διενέργεια κυβερνοεπιθέσεων.

Hacktivism (Χακτιβισμός)	Επιθέσεις για πολιτικούς/ιδεολογικούς λόγους, συνήθως χαμηλής τεχνικής πολυπλοκότητας.
Insider Threats (Εκ των Έσω Απειλές)	Αφορούν σε άτομα που έχουν ή είχαν εξουσιοδοτημένη πρόσβαση ή γνώση πληροφοριών για πόρους ενός οργανισμού και τα χρησιμοποιούν για να βλάψουν τον οργανισμό.
Zero-day attack	Είδος κυβερνοεπίθεσης που εκμεταλλεύεται μία προηγουμένως άγνωστη ευπάθεια σε λογισμικό, υλικό ή υλισμικό, για την οποία δεν υπάρχει ακόμη διόρθωση.

Εισαγωγή

Η προηγούμενη περίοδος στρατηγικού σχεδιασμού για την κυβερνοασφάλεια, η οποία αναπτύχθηκε στο πλαίσιο της Οδηγίας NIS1 και του ν. 4577/2018, ολοκλήρωσε τον κύκλο της σε μια εποχή έντονων τεχνολογικών και γεωπολιτικών αλλαγών. Η Ελλάδα έκανε σημαντικά βήματα προς την κατεύθυνση μιας πιο ώριμης και συνεκτικής εθνικής πολιτικής κυβερνοασφάλειας, θέτοντας τα θεμέλια για έναν ενιαίο τρόπο οργάνωσης, συνεργασίας και προστασίας των κρίσιμων λειτουργιών της χώρας στο ψηφιακό περιβάλλον.

Η νέα Εθνική Στρατηγική Κυβερνοασφάλειας 2026–2030 διαμορφώνεται στο πλαίσιο της μεταφοράς της Οδηγίας NIS2 στην εθνική έννομη τάξη και της δημοσίευσης του ν. 5160/2024, τα οποία εισάγουν ένα αυστηρότερο, εκτενέστερο και περισσότερο απαιτητικό σύστημα διακυβέρνησης κυβερνοασφάλειας. Με τη σημαντική διεύρυνση του πεδίου εφαρμογής, την ενίσχυση των υποχρεώσεων ασφάλειας και αναφοράς περιστατικών, καθώς και με νέους μηχανισμούς εποπτείας και συντονισμού, η χώρα εισέρχεται σε μία νέα φάση όπου η κυβερνοασφάλεια αντιμετωπίζεται ως κρίσιμο θεμέλιο της λειτουργίας της οικονομίας, της δημόσιας διοίκησης και της κοινωνίας συνολικά.

Ωστόσο, η Στρατηγική για την περίοδο 2026–2030 δεν περιορίζεται στη συμμόρφωση με τις απαιτήσεις του Ενωσιακού και του εθνικού δικαίου. Επιχειρεί, αποτυπώνοντας το σύγχρονο περιβάλλον απειλών, να αξιοποιήσει τα διαθέσιμα μεθοδολογικά εργαλεία υπηρετώντας πρωτίστως τις εθνικές ανάγκες, σε ένα περιβάλλον ολοένα και μεγαλύτερης εξάρτησης από διασυνδεδεμένες ψηφιακές υπηρεσίες και υποδομές. Πέρα από το κανονιστικό πλαίσιο, η στρατηγική θέτει έναν ευρύτερο προσανατολισμό: την ενίσχυση της κυβερνοανθεκτικότητας της ελληνικής κοινωνίας στο σύνολό της.

Σε αυτό το πνεύμα, εισάγει εμβληματικές δραστηριότητες που επικεντρώνονται στη γνώση, στην ευαισθητοποίηση και στην ανάπτυξη δεξιοτήτων, καθώς και στην υποστήριξη κοινωνικών ομάδων, μικρών οργανισμών, φορέων και επιχειρήσεων που έχουν αυξημένη ανάγκη καθοδήγησης για την αντιμετώπιση των κινδύνων του κυβερνοχώρου. Η προσέγγιση αυτή αναγνωρίζει ότι η κυβερνοασφάλεια δεν είναι απλώς ένα τεχνικό ή διοικητικό ζήτημα, αλλά προϋπόθεση κοινωνικής ανθεκτικότητας, ψηφιακής εμπιστοσύνης και δημοκρατικής σταθερότητας.

Με αυτές τις αρχές, η Εθνική Στρατηγική Κυβερνοασφάλειας 2026–2030 επιχειρεί να συνδυάσει ανάλυση, ρεαλισμό και φιλόδοξο σχεδιασμό, θέτοντας το πλαίσιο για μια πιο ασφαλή, ώριμη και ανθεκτική ψηφιακή Ελλάδα την επόμενη πενταετία.

1. Ανάλυση Υφιστάμενης Κατάστασης

Η υφιστάμενη κατάσταση στο πεδίο των κυβερνοαπειλών είναι εξαιρετικά δυναμική, καθώς τα κράτη και οι οργανισμοί καλούνται να ανταπεξέλθουν σε ένα συνεχώς μεταβαλλόμενο και ασταθές ψηφιακό περιβάλλον. Σε διεθνές επίπεδο, ο διαρκώς επιταχυνόμενος ψηφιακός μετασχηματισμός, η διαχείριση των επιπτώσεων της πανδημίας COVID-19 και η αναδιάταξη των γεωπολιτικών ισορροπιών έχει οδηγήσει σε κρίσιμες αλλαγές αναφορικά με τις απειλές στον κυβερνοχώρο. Ιδιαίτερα ανησυχητική είναι η αυξανόμενη χρήση προηγμένων τεχνολογιών, όπως η παραγωγική τεχνητή νοημοσύνη (AI-driven technologies) και τα μεγάλα γλωσσικά μοντέλα (LLMs), από κυβερνοεγκληματικές ομάδες έως και κρατικά υποκινούμενους φορείς, για την αυτοματοποίηση και την κλιμάκωση επιθέσεων.

Το 2022, από στρατηγικής άποψης, η κρίση Ρωσίας-Ουκρανίας σηματοδότησε μία νέα εποχή στον κυβερνοχώρο, αναδεικνύοντας τον «κυβερνοπόλεμο» (cyber warfare) και τον «χακτιβισμό» (Hacktivism) ως «όπλα» με σημαντικά αποτελέσματα στο πεδίο των συγκρούσεων. Φαινόμενα όπως ο «κυβερνοακτιβισμός» (Cyberhacktivism), οι στοχευμένες επιθέσεις σε κρίσιμες υποδομές και οι ψυχολογικές επιχειρήσεις, αποκτούν πλέον στρατηγική σημασία, καθώς εντάσσονται στο ευρύτερο πλαίσιο των υβριδικών απειλών. Παράλληλα, στις νέες ψηφιακές απειλές εντάσσονται οι λεγόμενες «επιχειρήσεις επιρροής στον κυβερνοχώρο», μέσω των οποίων επιχειρείται, με συντονισμένες ενέργειες διάδοσης ψευδών ειδήσεων (fake news), ενεργοποίησης αυτοματοποιημένων λογαριασμών (bots) και παραγωγής ψευδεπίγραφου οπτικοακουστικού υλικού (deepfakes) η χειραγώγηση της κοινής γνώμης, η υπονόμευση θεσμών, που μπορούν να φτάνουν μέχρι και σε απόπειρες αλλοίωσης κορυφαίων δημοκρατικών διαδικασιών, όπως οι εθνικές και ευρωπαϊκές εκλογές. Οι επιχειρήσεις επιρροής συνιστούν «ήπιες» μορφές κυβερνοπολέμου, καθώς, αντί να επιδιώκουν την καταστροφή ή παραβίαση κρίσιμων πληροφοριακών συστημάτων, στοχεύουν στον έλεγχο και τη διαμόρφωση της ανθρώπινης αντίληψης, ήτοι στην επίτευξη πληροφοριακής κυριαρχίας (information dominance).

Η σημασία που προσδίδει η Ε.Ε. στην αντιμετώπιση του φαινομένου των κυβερνοεπιθέσεων καθίσταται εμφανής μέσα από πλήθος πολιτικών, νομοθετικών και επιχειρησιακών πρωτοβουλιών. Η ψήφιση σειράς σημαντικών νομοθετικών και στρατηγικών πρωτοβουλιών, όπως ο Κανονισμός για την Ανθεκτικότητα στον Κυβερνοχώρο (Cyber Resilience Act), η αναθεωρημένη Οδηγία NIS2, ο Κανονισμός για τη Ψηφιακή Επιχειρησιακή Ανθεκτικότητα του Χρηματοοικονομικού τομέα (“DORA”) η Πράξη για την Αλληλεγγύη στον Κυβερνοχώρο (Cyber Solidarity Act), καθώς και το σχέδιο για τη διαχείριση περιστατικών μεγάλης κλίμακας (Cybersecurity Blueprint), αποτυπώνουν μια πιο φιλόδοξη και συντονισμένη προσέγγιση της Ε.Ε. σε επίπεδο νομοθεσίας, επιχειρησιακής ετοιμότητας και συλλογικής άμυνας στον κυβερνοχώρο. Μέσα από αυτές τις πρωτοβουλίες η ΕΕ επιδιώκει όχι μόνο να ενισχύσει την ανθεκτικότητα των κρατών-μελών και των κρίσιμων υποδομών, αλλά και να προωθήσει τη συνεργασία και την αλληλεγγύη σε ευρωπαϊκό επίπεδο, διαμορφώνοντας ένα ενιαίο στρατηγικό πλαίσιο αντιμετώπισης των κυβερνοαπειλών, το οποίο περιλαμβάνει τους βασικούς πυλώνες της πρόληψης, ανίχνευσης, αντίδρασης σε περιστατικά, καθώς και αποτροπής. Το πλαίσιο αυτό συμπληρώνεται από γενναία χρηματοδοτικά εργαλεία, αρμόδιους ευρωπαϊκούς οργανισμούς, καθώς και συντονισμένη συμμετοχή της Ε.Ε. στον διάλογο που λαμβάνει χώρα σε διεθνές επίπεδο.

Σε εθνικό επίπεδο, τα τελευταία χρόνια η Ελλάδα έχει υλοποιήσει σημαντικές θεσμικές πρωτοβουλίες στον τομέα της κυβερνοασφάλειας, σηματοδοτώντας τη μετάβαση προς μια συνολική, συνεκτική και ολοκληρωμένη εθνική πολιτική. Η ίδρυση της Εθνικής Αρχής Κυβερνοασφάλειας (ν. 5086/2024) αποτέλεσε κομβικό βήμα, καθώς καθιέρωσε έναν ενιαίο κεντρικό φορέα (lead agency) υπεύθυνο για το συντονισμό όλων των δράσεων που σχετίζονται με την προστασία του κυβερνοχώρου. Παράλληλα, ο ν. 5160/2024 θεσπίζει το εθνικό σύστημα διακυβέρνησης για την κυβερνοασφάλεια, ορίζοντας τις επιμέρους αρμόδιες Αρχές (όπως, εθνική αρμόδια αρχή συνολικά για την εφαρμογή της εθνικής πολιτικής κυβερνοασφάλειας, αρχές εποπτείας και ελέγχου, διαχείρισης περιστατικών μεγάλης κλίμακας, καθώς και τις εθνικές ομάδες απόκρισης σε περιστατικά – CSIRTs). Το πλαίσιο αυτό έθεσε για πρώτη φορά με ολοκληρωμένο τρόπο σαφείς ρόλους, αρμοδιότητες και μηχανισμούς συνεργασίας μεταξύ δημοσίων φορέων, κρίσιμων υποδομών και ιδιωτικού τομέα. Η ενσωμάτωση της Οδηγίας NIS2 στην εθνική έννομη τάξη αποτέλεσε σημαντικό ορόσημο, διευρύνοντας το πεδίο εφαρμογής της προηγούμενης Οδηγίας NIS1, επιβάλλοντας αυστηρότερες υποχρεώσεις ασφάλειας και αναφοράς περιστατικών, καθώς και ενισχύοντας σημαντικά τον πυλώνα εποπτείας και ελέγχου.

Πέραν των θεσμικών παρεμβάσεων, η Ελλάδα συμμετέχει ενεργά σε ευρωπαϊκά όργανα, προγράμματα και πρωτοβουλίες, όπως το Ευρωπαϊκό Κέντρο Ικανοτήτων για την Κυβερνοασφάλεια (ECCC), το NIS Cooperation Group, τα δίκτυα CyCLONe και CSIRTs, με στόχο την ενίσχυση της διακρατικής συνεργασίας, της ανταλλαγής πληροφοριών και της κοινής απόκρισης σε επιθέσεις μεγάλης κλίμακας. Ιδιαίτερη έμφαση δίνεται, επιπλέον, στη συνεχή εκπαίδευση και κατάρτιση του προσωπικού τόσο του δημόσιου όσο και του ιδιωτικού τομέα, στην ανάπτυξη προγραμμάτων ευαισθητοποίησης πολιτών και επιχειρήσεων, καθώς και στη δημιουργία κινήτρων για επενδύσεις στην κυβερνοασφάλεια. Μέσα από αυτές τις πρωτοβουλίες, η Ελλάδα επιχειρεί να ενισχύσει τη θεσμική της ανθεκτικότητα, να ενδυναμώσει τη στρατηγική της αυτονομία στον ψηφιακό χώρο και να συμβάλλει ενεργά στην ευρωπαϊκή αρχιτεκτονική κυβερνοασφάλειας. Ο αναγκαίος ψηφιακός μετασχηματισμός και η σημαντική πρόοδος της χώρας στον τομέα αυτό συνεπάγονται ταυτόχρονα την εξάρτηση από ψηφιακές υποδομές και καθιστούν επιτακτική την ανάγκη για συνεχή διακυβερνητικό συντονισμό, διατομεακή συνεργασία και ενεργή συμμετοχή όλων των εμπλεκόμενων φορέων, συμπεριλαμβανομένων της δημόσιας διοίκησης, του ιδιωτικού τομέα, της ακαδημαϊκής κοινότητας και της κοινωνίας των πολιτών.

Η Εθνική Στρατηγική Κυβερνοασφάλειας θεσπίζεται στο πλαίσιο της Στρατηγικής Εθνικής Ασφάλειας, όπως η τελευταία διαμορφώνεται από το Κυβερνητικό Συμβούλιο Εθνικής Ασφάλειας, και καλείται να ανταποκριθεί στις πολύπλοκες και δυναμικές απειλές, θέτοντας ρεαλιστικούς στόχους, υιοθετώντας βέλτιστες ευρωπαϊκές πρακτικές και αξιοποιώντας τις ευκαιρίες χρηματοδότησης και τεχνικής υποστήριξης που προσφέρει η Ευρωπαϊκή Ένωση. Με αυτόν τον τρόπο, η Ελλάδα προωθεί μια συνολική, συντονισμένη και στρατηγικά σχεδιασμένη προσέγγιση, που ενισχύει την ασφάλεια στον κυβερνοχώρο και τη διευρωπαϊκή συνεργασία.

1.Α Πεδίο Απειλών

Οι ετήσιες Εκθέσεις Threat Landscape του Οργανισμού της ΕΕ για την κυβερνοασφάλεια (ENISA) αναδεικνύουν τις πρωταρχικές ομάδες απειλών συνολικά για τον ευρωπαϊκό χώρο, με βάση τη συχνότητα εμφάνισής τους, καθώς και του σημαντικού αντίκτυπου που επιφέρουν. Ιδίως τα ευρήματα της πρόσφατης έκθεσης του έτους 2025[1], επιβεβαιώνουν και ενισχύουν τις διαπιστώσεις προηγούμενων ετών, αναδεικνύοντας επιπλέον νέες τάσεις και τεχνικές που καθιστούν τις απειλές αυτές ακόμη πιο σύνθετες και εξελιγμένες.

Εικόνα 1: Ευρωπαϊκό & Εθνικό Τοπίο Απειλών (ENISA & ΕΑΚ)

Τοπίο Κυβερνοαπειλών 2030

Η μελέτη του ENISA «Foresight Cybersecurity Threats for 2030»[2] αποτυπώνει τις δέκα κορυφαίες απειλές που αναμένεται να διαμορφώσουν το τοπίο κυβερνοασφάλειας έως το 2030 στον ευρωπαϊκό χώρο συνολικά. Οι εν λόγω επιθέσεις εκμεταλλεύονται την πολυπλοκότητα και τις αλληλεξαρτήσεις του σύγχρονου ψηφιακού οικοσυστήματος, καθιστώντας τις ευπάθειες δυσδιάκριτες και τις συνέπειες εκτεταμένες:

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[2]https://www.enisa.europa.eu/sites/default/files/2024-11/Cybersecurity%20Threats%20for%202030%20-%20Update%202024%20-%20Executive%20Summary_0.pdf

- Επηρεάζουν όλα τα στάδια ανάπτυξης, διανομής και ενσωμάτωσης λογισμικού, συμπεριλαμβανομένων εξωτερικών προμηθευτών, βιβλιοθηκών ανοικτού κώδικα, APIs και εργαλείων τρίτων, με στόχο να πλήξουν έμμεσα τους τελικούς οργανισμούς.
- Η έλλειψη εξειδικευμένου ανθρώπινου δυναμικού στον τομέα της κυβερνοασφάλειας συνιστά έναν από τους σημαντικότερους παράγοντες αυξημένου κινδύνου για το ευρωπαϊκό ψηφιακό οικοσύστημα. Καθώς οι κυβερνοεπιθέσεις αυξάνονται σε συχνότητα, πολυπλοκότητα και εύρος στόχων, η ζήτηση για εξειδικευμένους επαγγελματίες στην προστασία πληροφοριακών συστημάτων υπερβαίνει κατά πολύ τη διαθέσιμη προσφορά. Η διαρκής αυτή ανισορροπία μεταξύ ζήτησης και προσφοράς δεξιοτήτων επιτείνει τους κινδύνους ασφάλειας, ιδίως σε περιβάλλοντα κυβερνο-φυσικών συστημάτων, όπου διασυνδεδεμένες παραγωγικές συσκευές, ψηφιακές πλατφόρμες και κρίσιμες υποδομές αλληλεπιδρούν σε πραγματικό χρόνο.
- Η ραγδαία εξάπλωση του Διαδικτύου των Πραγμάτων (IoT) σε βιομηχανίες, υποδομές και οικιακά περιβάλλοντα δημιουργεί ένα πολυσύνθετο και συχνά μη ελεγχόμενο οικοσύστημα, στο οποίο η έλλειψη εκπαίδευσης, η μη έγκαιρη συντήρηση και η απουσία υποστήριξης για παλαιότερες συσκευές αυξάνουν την πιθανότητα διακοπής υπηρεσιών, υποκλοπής δεδομένων ή πρόκλησης φυσικών ζημιών.
- Η εκμετάλλευση μη ενημερωμένων και παρωχημένων συστημάτων σε υπερφορτωμένες ψηφιακές υποδομές συνιστά ένα από τα πλέον κρίσιμα σημεία ευπάθειας εντός του πολυτομεακού τεχνολογικού οικοσυστήματος. Το πλήθος των διασυνδεδεμένων στοιχείων σε τομείς όπως η ενέργεια, οι μεταφορές και η υγεία μπορεί να επιφέρει αλυσιδωτές επιπτώσεις σε περίπτωση επίθεσης, θέτοντας σε κίνδυνο την επιχειρησιακή συνέχεια και την ασφάλεια δεδομένων.
- Η αύξηση της ψηφιακής επιτήρησης και η προστασία της ιδιωτικότητας αποτελούν επιπλέον ζήτημα στρατηγικής σημασίας. Η αυξανόμενη χρήση τεχνολογιών αναγνώρισης προσώπου, γεωεντοπισμού και βιομετρικών δεδομένων έχει οδηγήσει στην εμφάνιση νέων απειλών για τα θεμελιώδη δικαιώματα των πολιτών.
- Η εξάρτηση από διασυνοριακούς παρόχους υπηρεσιών ICT (Information and Communication Technology) ενισχύει περαιτέρω τις ευπάθειες κρίσιμων υποδομών, καθώς οποιαδήποτε διακοπή ή παραβίαση μπορεί να προκαλέσει αλυσιδωτές συνέπειες σε καίριους τομείς όπως η ενέργεια, οι μεταφορές και η υγεία. Σε περιόδους γεωπολιτικής αστάθειας, οι υποδομές αυτές ενδέχεται να χρησιμοποιηθούν ως στρατηγικά μέσα επιρροής ή πίεσης, καθιστώντας την ανθεκτικότητα και την κυβερνοασφάλειά τους ζήτημα εθνικής και ευρωπαϊκής ασφάλειας.
- Οι αναδυόμενες απειλές περιλαμβάνουν και στρατηγικού, κοινωνικού και γεωπολιτικού χαρακτήρα κινδύνους. Οι επιχειρήσεις παραπληροφόρησης και η άνοδος των υβριδικών απειλών αποκτούν ιδιαίτερη σημασία. Οι εκστρατείες παραπληροφόρησης και επιρροής αποκτούν νέα διάσταση μέσω της τεχνητής νοημοσύνης και των τεχνολογιών deepfake, αφού η δυνατότητα δημιουργίας απολύτως πειστικών ψευδών ταυτοτήτων και περιεχομένου επιτρέπει τη μαζική χειραγώγηση της κοινής γνώμης, με σημαντικές γεωπολιτικές και κοινωνικές συνέπειες.

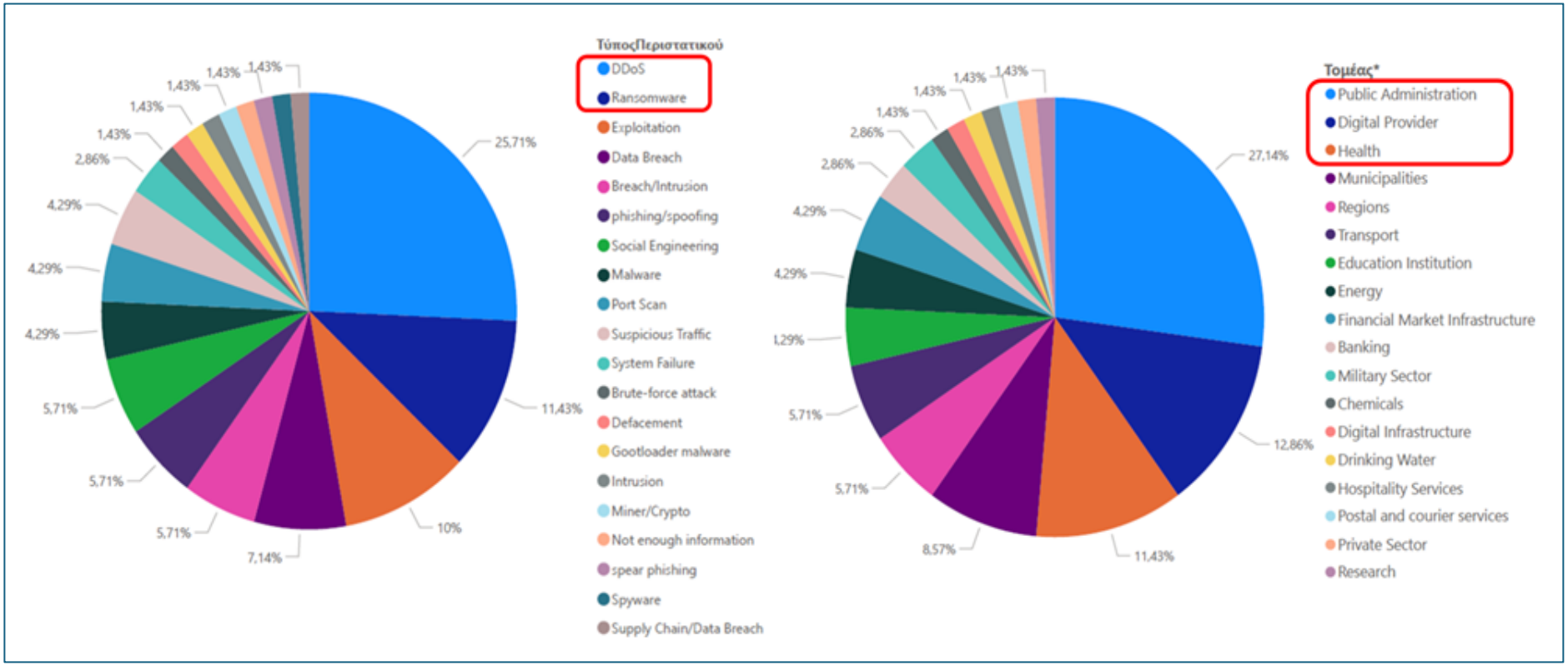
- Οι υβριδικές απειλές αποτελούν μία από τις πλέον σύνθετες και πολυδιάστατες μορφές σύγχρονου κινδύνου. Πρόκειται για συνδυασμένες επιθέσεις που εκδηλώνονται ταυτόχρονα ή σταδιακά σε ψηφιακό, φυσικό, πληροφοριακό και κοινωνικό επίπεδο, καθιστώντας δύσκολη την ανίχνευση, την απόκριση και τον εντοπισμό των υπευθύνων.
- Η διευρυμένη αξιοποίηση της τεχνητής νοημοσύνης (AI) εντείνει περαιτέρω αυτούς τους κινδύνους, καθώς η αλλοίωση δεδομένων εκπαίδευσης (data poisoning), η ενσωμάτωση προκαταλήψεων και η δημιουργία κακόβουλων εφαρμογών AI μπορούν να οδηγήσουν σε λανθασμένες αποφάσεις, παραπληροφόρηση ή στοχοποίηση πολιτών. Επιπλέον, η χρήση AI για ανάλυση συμπεριφοράς και ανάπτυξη εξελιγμένων εργαλείων κοινωνικής μηχανικής ενισχύει περαιτέρω τη δύναμη των επιτιθέμενων.
- Τέλος, οι φυσικές και περιβαλλοντικές διαταραχές αποτελούν πρόσθετο παράγοντα κινδύνου για τις κρίσιμες ψηφιακές υποδομές. Ακραία καιρικά φαινόμενα, φυσικές καταστροφές ή περιβαλλοντικές κρίσεις μπορούν να προκαλέσουν σοβαρές διακοπές λειτουργίας, αναδεικνύοντας την ανθεκτικότητα, την επιχειρησιακή ετοιμότητα και τον προληπτικό σχεδιασμό ως βασικά στοιχεία προστασίας των κοινωνιών και αποτροπής αλυσιδωτών συνεπειών σε εθνικό και διεθνές επίπεδο.

Δεδομένων των ανωτέρω, εκτιμάται ότι το μέλλον της κυβερνοασφάλειας θα διαμορφωθεί από αυξανόμενες αλληλεξαρτήσεις, πολυτομεακές προκλήσεις και σύνθετες απειλές που υπερβαίνουν τα παραδοσιακά τεχνικά όρια. Η αποτελεσματική αντιμετώπισή τους απαιτεί ενίσχυση της διεθνούς συνεργασίας, ανάπτυξη εξειδικευμένων δεξιοτήτων και συνεχή επένδυση στην τεχνολογική καινοτομία. Η διαμόρφωση ανθεκτικών και ασφαλών ψηφιακών οικοσυστημάτων αποτελεί, συνεπώς, θεμελιώδη προϋπόθεση για την προστασία των κοινωνιών και την ασφάλεια του ευρωπαϊκού ψηφιακού χώρου κατά την επόμενη δεκαετία.

Η ραγδαία αύξηση των κυβερνοεπιθέσεων επηρεάζει κρίσιμους τομείς τόσο σε ευρωπαϊκό όσο και σε εθνικό επίπεδο, καθώς οι κυβερνοεγκληματίες εκτελούν επιθέσεις μεγάλης κλίμακας, με αυξημένη ένταση και έκταση, γεγονός που εντείνει τις προκλήσεις για την κυβερνοασφάλεια. Το εθνικό τοπίο απειλών βρίσκεται σε αντιστοιχία προς την υπόλοιπη Ευρώπη, με κυριότερους στόχους τους Κυβερνητικούς Φορείς, τον Τομέα Μεταφορών και τους Ψηφιακούς Παρόχους, ενώ και ο τομέας της Υγείας χαρακτηρίζεται από υψηλό αριθμό κυβερνοεπιθέσεων. Σε ό,τι αφορά τη φύση των επιθέσεων, οι πιο διαδεδομένες μορφές είναι οι επιθέσεις τύπου DDoS και Ransomware, οι οποίες πραγματοποιούνται πλέον με πιο σύνθετες τεχνικές.

Είδος επιθέσεων και τυπολογία περιστατικών κυβερνοασφάλειας

Οι επιθέσεις τύπου DDoS & τα περιστατικά Ransomware συνεχώς αυξάνονται σε πλήθος και πολυπλοκότητα, ενώ έχουν τις μεγαλύτερες επιπτώσεις. Οι φορείς που πλήττονται περισσότερο στη χώρα μας ανήκουν στο Δημόσιο Τομέα, τους Ψηφιακούς Παρόχους, τις Μεταφορές και την Υγεία, με τις πιο εξελιγμένες επιθέσεις να στοχεύουν τους Ψηφιακούς Παρόχους.



Εικόνα 2: Καταγεγραμμένα Περιστατικά ΕΑΚ (Α' Εξάμηνο 2025)

Λογισμικό Λύτρων ή Λυτρισμικές Επιθέσεις

Οι επιθέσεις αυτού του τύπου στοχεύουν σε ένα ευρύ φάσμα κλάδων, με τους επιτιθέμενους να αποφεύγουν την ανίχνευσή τους κάνοντας χρήση προηγμένων τεχνικών, οι οποίες συγκαλύπτουν τις κακόβουλες ενέργειές τους. Ολοένα και πιο δημοφιλής γίνεται η τακτική, όπου οι εγκληματίες του κυβερνοχώρου επιτίθενται κατ' επανάληψη στα θύματά τους, εκμεταλλευόμενοι ευπάθειες ή κλεμμένα διαπιστευτήρια από προηγούμενες επιθέσεις είτε της ίδιας είτε άλλων ομάδων. Ιδίως παρατηρείται ότι η τυχόν καταβολή λύτρων παρέχει επιπλέον κίνητρο στοχοποίησης των ίδιων προθύμων να πληρώσουν οργανισμών, καθώς η συστηματική περαιτέρω στοχοποίησή τους αποτελεί μια διεθνή τάση.

Επισημαίνεται ότι το συνολικό οικοσύστημα του ransomware έχει ενισχυθεί περαιτέρω ως προς την πολυπλοκότητα, την ανθεκτικότητα και τον βαθμό «επαγγελματοποίησής» του. Ενδεικτικά, καταγράφονται διαρκώς νέες παραλλαγές ransomware που στοχεύουν κρίσιμες υποδομές συνολικά στον ευρωπαϊκό χώρο, γεγονός που καταδεικνύει τη συνεχιζόμενη διαφοροποίηση και εξειδίκευση των απειλών στο τοπίο κυβερνοασφάλειας.

Κακόβουλο Λογισμικό (malware)

Οι επιθέσεις κακόβουλου λογισμικού αντιστοιχούν, σε ευρωπαϊκό επίπεδο, περίπου στο 10%, στο σύνολο των κυβερνοεπιθέσεων. Παράλληλα, οι επιθέσεις που στοχεύουν σε ψηφιακές υποδομές ανέρχονται σε 25%, ενώ εκείνες που πλήττουν τη δημόσια διοίκηση σε ποσοστό 11%. Το κακόβουλο λογισμικό αναδεικνύεται ως μία από τις πλέον κρίσιμες κυβερνοαπειλές, επισημαίνοντας ότι κυριότεροι μηχανισμοί διάδοσής του παραμένουν το phishing και η εκμετάλλευση γνωστών ευπαθειών. Οι επιθέσεις που περιλαμβάνουν malware, ιδίως οικογένειες ransomware και infostealers, προκαλούν τις σοβαρότερες επιχειρησιακές και οικονομικές επιπτώσεις.

Κοινωνική μηχανική (Social Engineering)

Η εκμετάλλευση του ανθρώπινου σφάλματος ή/και η χειραγώγηση των χρηστών για την απόκτηση πρόσβασης σε πληροφορίες ή υπηρεσίες βρίσκονται στον πυρήνα της κοινωνικής μηχανικής. Η επιτυχία της κοινωνικής μηχανικής βασίζεται πρωτίστως στην εκμετάλλευση χαρακτηριστικών του ανθρώπινου παράγοντα.

Η πλέον διαδεδομένη επίθεση αυτού του είδους είναι το «ηλεκτρονικό ψάρεμα» (phishing, μέσω ηλεκτρονικού ταχυδρομείου) ή το "smishing" (μέσω μηνυμάτων κινητού τηλεφώνου). Το phishing[3], συγκεκριμένα, εξακολουθεί να αποτελεί τον κυρίαρχο φορέα διείσδυσης (σε ποσοστό 60% πανευρωπαϊκά) και εξελίσσεται διαρκώς, αξιοποιώντας νέες τεχνικές που εφαρμόζονται σε εκστρατείες μεγάλης κλίμακας.

Μια πρόσφατη εξέλιξη σε αυτό το πλαίσιο είναι το quishing ή phishing μέσω QR κωδικών. Στην περίπτωση αυτή, οι δράστες ενσωματώνουν κακόβουλους QR κωδικούς σε email ή αρχεία, οδηγώντας τα θύματα σε ψεύτικες σελίδες συλλογής διαπιστευτηρίων, φιλοξενούμενες σε νόμιμες cloud πλατφόρμες.

[3] https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf

Η συνολική αξιολόγηση της τάσης δείχνει ότι το phishing παραμένει η πιο κρίσιμη απειλή παρά την τεχνική απλότητά του σε σχέση με πιο σύνθετες επιθέσεις. Άλλες παραλλαγές επιθέσεων κοινωνικής μηχανικής είναι οι τακτικές, μέσω των οποίων εμφανίζονται ψεύτικα σφάλματα κυρίως σε ιστότοπους (τακτική ClickFix[4]), τα οποία ζητούν από τους χρήστες να εκτελέσουν μια «διόρθωση». Οι χρήστες στην προσπάθειά τους να αντιμετωπίσουν το «σφάλμα» κατεβάζουν και μολύνουν το σύστημά τους με κακόβουλο λογισμικό. Πρόκειται για μια τεχνική που σημειώνει σημαντική αύξηση κατά την τρέχουσα περίοδο[5].

Παραβιάσεις Προσωπικών Δεδομένων

Επιθέσεις που αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων. Διακρίνονται σε παραβιάσεις δεδομένων (data breach) και διαρροές δεδομένων (data leakage). Η παραβίαση δεδομένων συνιστά σκόπιμη επίθεση εναντίον ενός συστήματος ή ενός οργανισμού με κύριο στόχο την παράνομη απόκτηση πληροφοριών. Η διαρροή δεδομένων προκύπτει από τεχνικές ευπάθειες, λανθασμένες ρυθμίσεις ή ανθρώπινα σφάλματα και οδηγεί σε ακούσια απώλεια ή έκθεση ευαίσθητων πληροφοριών.

Οι παραβιάσεις αυτές στοχεύουν κυρίως στη δημόσια διοίκηση, στις ψηφιακές υποδομές και υπηρεσίες, καθώς και στον χρηματοπιστωτικό τομέα, συνολικά σε επίπεδο ΕΕ. Σε πολλές περιπτώσεις, τα υποκλαπέντα δεδομένα διακινούνταν σε διαδικτυακά φόρουμ μέσω «μεσιτών αρχικής πρόσβασης» (Initial Access Brokers - IAB), γεγονός που διευκολύνει την περαιτέρω εκμετάλλευσή τους σε εκστρατείες phishing ή άλλες κακόβουλες δραστηριότητες.

Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας (Threats against availability: DISTRIBUTED Denial of Service ATTACKS - DDOS)

Επιθέσεις κατά τις οποίες μεγάλος όγκος διαδικτυακής κίνησης στοχεύει σε μια υπηρεσία, με σκοπό να καταστεί αδύνατο από τα συστήματα να εξυπηρετήσουν νόμιμα αιτήματα. Ουσιαστικά, εκμεταλλεύονται την πεπερασμένη χωρητικότητα συστημάτων και δικτύων, ώστε να καταστήσουν αδύνατη την παροχή υπηρεσιών (απώλεια διαθεσιμότητας).

Οι επιθέσεις DDoS παρουσιάζουν σταθερά αυξητική τάση τα τελευταία χρόνια, ως αποτέλεσμα πολλών και αλληλένδετων παραγόντων. Η ευρεία διαθεσιμότητα υπηρεσιών και εργαλείων τύπου DDoS-for-Hire[6], η ενίσχυση του φαινομένου του χακτιβισμού, καθώς και οι συνεχιζόμενες γεωπολιτικές εντάσεις έχουν συμβάλει καθοριστικά στην αύξηση τόσο της έντασης όσο και της συχνότητας των επιθέσεων αυτών, με το δημόσιο τομέα να αποτελεί τον βασικό στόχο.

Αξιοσημείωτο είναι ότι οι επιθέσεις τύπου DDoS αποτελούν την πολυπληθέστερη κατηγορία κυβερνοεπιθέσων, με την πλειονότητά τους να πραγματοποιείται από χακτιβιστές. Παρότι στην πλειονότητά τους είναι χαμηλής έντασης και ένα πολύ μικρό ποσοστό τους έχει ουσιαστικό

[4] https://www.bleepingcomputer.com/news/security/dprk-hackers-dupe-targets-into-typing-powershell-commands-as-admin/

[5] https://www.bleepingcomputer.com/news/security/clickfix-attack-delivers-infostealers-rats-in-fake-bookingcom-emails/

[6] Το DDoS-for-Hire επιτρέπει την εξαπόλυση επιθέσεων DDoS μεγάλης κλίμακας από χρήστες που δεν έχουν οι ίδιοι τεχνικές δεξιότητες.

επιχειρησιακό αντίκτυπο, ως τακτική χρησιμοποιείται κατά συστηματικό και επαναλαμβανόμενο τρόπο από οργανωμένες ομάδες χακτιβιστών.

Χειραγώγηση πληροφοριών και παρεμβάσεις από Εξωτερικούς Παράγοντες (FOREIGN Information manipulation and interference)

Η χειραγώγηση των πληροφοριών και οι παρεμβάσεις από εξωτερικούς παράγοντες[7] (FIMI) συνιστούν σημαντική απειλή για τη σταθερότητα των δημοκρατικών θεσμών και διαδικασιών στην Ευρωπαϊκή Ένωση συνολικά. Οι καμπάνιες FIMI αξιοποιούν στρατηγικά γεγονότα, όπως εκλογικές διαδικασίες (ευρωπαϊκές ή εθνικές εκλογές και δημοψηφίσματα) για να προωθήσουν αφηγήματα που αποδυναμώνουν την εμπιστοσύνη στους δημοκρατικούς θεσμούς και υπονομεύουν πολιτικές πρωτοβουλίες.

Οι επιθέσεις αυτές χρησιμοποιούν ποικίλες τεχνικές, όπως η δημιουργία ψευδών ειδήσεων, η κατασκευή ερευνών και η παραποίηση δηλώσεων ή εικόνων αξιωματούχων. Επιπλέον, αξιοποιούνται ψευδή έγγραφα και αναρτήσεις που διαδίδονται μέσω ανώνυμων ή μη αναγνωρίσιμων λογαριασμών, ενισχύοντας τη δυσπιστία και την παραπληροφόρηση. Η χρήση Τεχνητής Νοημοσύνης έχει ενισχύσει την αποτελεσματικότητα αυτών των μεθόδων, επιτρέποντας την αυτοματοποίηση της δημιουργίας και της διάδοσης περιεχομένου σε μεγάλη κλίμακα. Ένα χαρακτηριστικό παράδειγμα της στρατηγικής διάδοσης είναι η τεχνική κατά την οποία το ίδιο περιεχόμενο μεταφράζεται και διαμοιράζεται ταυτόχρονα σε πολλαπλές διαδικτυακές πλατφόρμες και λογαριασμούς, με στόχο να ενισχύσει την εμβέλεια και την αξιοπιστία του περιεχομένου.

Η επίδραση των παραπάνω στρατηγικών είναι ευρεία, καθώς περιλαμβάνει την πόλωση της κοινής γνώμης, την υπονόμευση της εμπιστοσύνης στους δημοκρατικούς θεσμούς και τη διαμόρφωση αρνητικών αφηγημάτων σχετικά με αυτούς. Οι επιθέσεις δεν περιορίζονται μόνο σε εκλογικές περιόδους, αλλά εκμεταλλεύονται και άλλες σημαντικές κοινωνικές και πολιτικές εξελίξεις, όπως οικονομικά μέτρα ή ζητήματα ευρύτερου κοινωνικού ενδιαφέροντος, προκειμένου να ενισχύσουν την ατζέντα των στρατηγικών δρώντων και να επηρεάσουν τη δημόσια αντίληψη σε ευρεία κλίμακα.

Επιθέσεις στην Αλυσίδα Εφοδιασμού (Supply Chain Attacks)

Είδος κυβερνοεπίθεσης κατά την οποία οι δράστες στοχεύουν σε έναν οργανισμό, μέσω τρίτων συνεργατών- όπως προμηθευτές, παρόχους λογισμικού ή υπηρεσιών. Το γεγονός ότι η αλυσίδα εφοδιασμού βρίσκεται σε ολοένα και αυξανόμενη εξάρτηση από εξωτερικούς προμηθευτές υπηρεσιών τεχνολογίας και πληροφοριών (IT) συνεπάγεται αφενός οργανωτική πολυπλοκότητα και αφετέρου μεγαλύτερη «επιφάνεια επίθεσης» (attack surface), δηλαδή διεύρυνση των πιθανών σημείων εκμετάλλευσης ενός οργανισμού από έναν επιτιθέμενο.

Οι κυβερνοεπιθέσεις στην αλυσίδα εφοδιασμού βρίσκονται ψηλά στην κατάταξη των απειλών συνολικά στην ΕΕ, γεγονός που οφείλεται αφενός στη δυσκολία ανίχνευσής τους και αφετέρου στην κλίμακα των καταστροφικών και αλυσιδωτών συνεπειών που μπορούν να προκαλέσουν. Σύμφωνα με τον ENISA, οι επιθέσεις στην εφοδιαστική αλυσίδα αυξήθηκαν κατά 20% μέσα σε ένα έτος (2023 με

[7] https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf

2024). Οι περισσότερες των επιθέσεων αυτών στοχεύουν τον κώδικα στο λογισμικό προμηθευτών με αποτέλεσμα να τεθούν σε κίνδυνο οι πελάτες τους[8].

Παράγοντες Απειλών

Οι παράγοντες απειλών στον κυβερνοχώρο αποτελούν αναπόσπαστο στοιχείο του τοπίου των απειλών. Πρόκειται για κακόβουλους δρώντες που χρησιμοποιούν ποικίλες τακτικές και τεχνικές για την επίτευξη του σκοπού τους. Σημαντικό ρόλο στο πεδίο απειλών διαδραματίζουν οι ακόλουθες κατηγορίες:

Κρατικά Υποστηριζόμενοι Δρώντες (State-nexus actors)

Πρόκειται για ομάδες ή δρώντες που εμπλέκονται σε έκνομες ενέργειες στον κυβερνοχώρο και διατηρούν άμεση ή έμμεση σύνδεση με κάποιο κράτος. Δεν πρόκειται απαραίτητα για επίσημους κρατικούς φορείς, αλλά για δρώντες που ενεργούν υπό την καθοδήγηση, την υποστήριξη ή την ανοχή κρατικών δομών. Στο πλαίσιο αυτό, διεξάγουν επιχειρήσεις «κυβερνοκατασκοπείας» (cyber espionage), πραγματοποιούν επιθέσεις σε κρίσιμες υποδομές, εμπλέκονται σε επιχειρήσεις παραπληροφόρησης και στοχεύουν πολιτικούς, οικονομικούς ή ακόμη και στρατιωτικούς στόχους άλλων κρατών.

Πραγματοποιούν προηγμένες, μεγάλης κλίμακας ή στοχευμένες επιχειρήσεις, χωρίς να χρησιμοποιούν κατ' ανάγκη καινοτόμες τεχνικές. Η δράση τους δεν περιορίζεται μόνο σε κρατικούς στόχους, αλλά και σε ιδιωτικούς οργανισμούς, με σκοπό να αποκτήσουν ευαίσθητες πληροφορίες ή ακόμα και οικονομικό όφελος υπέρ της χώρας με την οποία συνδέονται.

Στην κατηγορία των κρατικά υποστηριζόμενων δρώντων κατατάσσονται και οι δρώντες "state-aligned", δηλαδή ομάδες ή οντότητες που, αν και δεν ελέγχονται άμεσα από κρατικούς μηχανισμούς άλλων κρατών, ενεργούν με τρόπο που εξυπηρετεί ή ευθυγραμμίζεται με τα συμφέροντα των τελευταίων. Ιδίως στον ευρωπαϊκό χώρο παρατηρούνται μακροπρόθεσμες εκστρατείες κυβερνοκατασκοπείας με τον δημόσιο τομέα να αποτελεί τον βασικό στόχο τους. Αυτές οι επιθέσεις στοχεύουν επίσης κρίσιμους τομείς και υπηρεσίες ζωτικής σημασίας, όπως οι τηλεπικοινωνίες, τα δίκτυα εφοδιασμού (logistics) και η μεταποίηση, επιδεικνύοντας υψηλό επίπεδο τεχνικής πολυπλοκότητας.

Κυβερνοέγκλημα και «Μισθοφόροι Hackers» (Cybercrime actors and hacker-for-hire actors)

Το κυβερνοέγκλημα λαμβάνει τεράστιες οικονομικές διαστάσεις. Στην τελευταία έκθεση Microsoft Digital Defense Report 2025[9] επισημαίνεται ότι «αν το κυβερνοέγκλημα ήταν χώρα, θα κατατασσόταν ως η τρίτη μεγαλύτερη οικονομία στον κόσμο, με εκτιμώμενο κόστος 9,5 τρισεκατομμυρίων δολαρίων ετησίως έως το 2025». Το έγκλημα στον κυβερνοχώρο πρόκειται για μια «εκβιομηχανοποιημένη» και παγκόσμια απειλή, με εργαλεία που επιτρέπουν ακόμη και σε άτομα με ελάχιστες τεχνικές γνώσεις να συμμετέχουν σε εγκληματικές δραστηριότητες. Ενδεικτικό παράδειγμα της οργάνωσης του διαδικτυακού εγκλήματος αποτελεί το Κυβερνοέγκλημα ως Υπηρεσία (Cybercrime-as-a-Service,

[8] https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

[9] https://news.microsoft.com/en-cee/2025/01/28/governments-face-unprecedented-cyber-threats-ai-emerges-as-the-ultimate-defense-to-cybercrime/

CaaS), όπου οι δράστες παρέχουν εργαλεία και υπηρεσίες προς ενοικίαση ή αγορά σε τρίτους με κακόβουλους σκοπούς, χωρίς να απαιτείται τεχνική γνώση από πλευράς τους.

Πρόκειται για μεμονωμένα φυσικά πρόσωπα ή ομάδες που διαπράττουν έκνομες ενέργειες μέσω του διαδικτύου, με βασικό κίνητρο το οικονομικό όφελος. Οι επιθέσεις τους είναι ευκαιριακές και συνήθως στοχεύουν αδιακρίτως σε δεδομένα ή υποδομές. Προβαίνουν σε απευθείας κλοπή των θυμάτων τους, εκβιασμούς ή σε εκμετάλλευση/αξιοποίηση των υποκλαπέντων πληροφοριών. Οι δράστες του ηλεκτρονικού εγκλήματος χρησιμοποιούν συχνά επιθέσεις κοινωνικής μηχανικής και ποικίλες μεθόδους για να επιτύχουν την πρόσβασή τους στα δίκτυα των οργανισμών – στόχων.

Οι επονομαζόμενοι «μισθοφόροι hackers» (hackers-for-hire) προσφέρουν τις υπηρεσίες τους επ' αμοιβή. Μεταξύ των «υπηρεσιών» τους συγκαταλέγονται η κυβερνοκατασκοπεία (σε βάρος επιχειρήσεων, πολιτικών προσώπων, δημοσιογράφων κ.α.) η παραβίαση email και μέσων κοινωνικής δικτύωσης, οι διαρροές ευαίσθητων δεδομένων ανταγωνιστών, η εγκατάσταση malware ή spyware, καθώς και η διάδοση ψευδών ειδήσεων.

Χακτιβιστές (Hacktivists)

Οι χακτιβιστές δεν διαθέτουν τόσο ισχυρούς πόρους όσο οι άλλοι παράγοντες απειλών, ωστόσο, συχνά τροφοδοτούνται από ισχυρά κίνητρα. Στόχος τους είναι η πρόκληση αναστάτωσης, προκειμένου να προωθήσουν κάποιας μορφής πολιτική ατζέντα. Οι ομάδες των χακτιβιστών είναι πολύ διαφορετικές μεταξύ τους και ποικίλλουν σε μεγάλο βαθμό ως προς τις δεξιότητες και τις ικανότητες. Ενίοτε αξιοποιούνται και από κρατικούς φορείς στο πλαίσιο επιχειρήσεων επιρροής.

Ο «χακτιβισμός» αποτελεί την πιο ενεργή μορφή κυβερνοαπειλής για τα κράτη μέλη της Ε.Ε., παρά τον χαμηλό βαθμό πολυπλοκότητας των επιθέσεων και τον περιορισμένο πραγματικό τους αντίκτυπο σε όρους απτών επιχειρησιακών επιπτώσεων στον οργανισμό-στόχο, γεγονός που καταδεικνύει, κυρίως, τον πληροφοριακό και προπαγανδιστικό χαρακτήρα των εν λόγω ενεργειών. Οι επιθέσεις αυτές συνδέονται χρονικά με διεθνείς ή εθνικές πολιτικές και γεωπολιτικές εξελίξεις, αντανακλώντας τη χρήση του κυβερνοχώρου ως μέσου άσκησης επιρροής και επικοινωνιακής πίεσης. Κύριο στόχο τους αποτελούν οργανισμοί της δημόσιας διοίκησης, ιδίως οι κυβερνητικές ιστοσελίδες, ενώ καταγράφεται αξιοσημείωτη αύξηση της χρήσης botnets.

Σύγκλιση Ομάδων Απειλών (Threat Groups Converging)

Το φαινόμενο αυτό αποτυπώνει τη σταδιακή διάβρωση των ορίων μεταξύ χακτιβισμού, κυβερνοεγκλήματος και κρατικά υποστηριζόμενων δρώντων, καθώς οι διαφορές ανάμεσά τους καθίστανται ολοένα και πιο δυσδιάκριτες. Ομάδες εισβολής που παραδοσιακά διαχωρίζονταν με βάση το επίπεδο τεχνογνωσίας ή τα κίνητρά τους, αρχίζουν πλέον να μοιράζονται κοινά εργαλεία και μεθόδους δράσης.

Ενδεικτικά, παρατηρείται κρατικά υποστηριζόμενες ομάδες να αξιοποιούν χακτιβιστές για να επηρεάσουν, μεταξύ άλλων, τα πολιτικά τεκταινόμενα και να υπηρετήσουν στρατηγικούς στόχους άλλων κρατών. Παράλληλα, τα εργαλεία που χρησιμοποιούνται από χακτιβιστές και τα οικοσυστήματα κυβερνοεγκλήματος διασταυρώνονται ολοένα και περισσότερο, γεγονός που αποτυπώνει την εντεινόμενη διασύνδεση ιδεολογικών και οικονομικών κινήτρων.

Εκ των Έσω Απειλές (Insider Threats)

Οι εκ των έσω απειλές αφορούν σε άτομα που έχουν ή είχαν εξουσιοδοτημένη πρόσβαση ή γνώση πληροφοριών για πόρους ενός οργανισμού και τη χρησιμοποιούν για να βλάψουν τον οργανισμό. Λόγω της φύσης και του επιπέδου πρόσβασης σε συστήματα και πληροφορίες ενός φορέα, καθώς και της μειωμένης χρήσης zero trust αρχιτεκτονικής ασφάλειας σε επίπεδο οργανισμού, οι εκ των έσω απειλές αποτελούν σημαντικό παράγοντα απειλών και έναν από τους πιο δύσκολους στην αναγνώριση και αντιμετώπισή τους.

Παρόλο που οι εκ των έσω απειλές αποτελούν ένα μικρό ποσοστό των αναγνωρισμένων διαύλων αρχικής εισόδου (initial access vectors) συγκριτικά με τις κυρίαρχες μεθόδους, όπως το phishing και η εκμετάλλευση ευπαθειών, παραμένουν στρατηγικής σημασίας λόγω του υψηλού αντικτύπου τους σε θέματα διαρροής δεδομένων και παραβίασης της εμπιστευτικότητας[10].· Ο ανθρώπινος παράγοντας, είτε λόγω κακόβουλης πρόθεσης είτε λόγω αμέλειας, αποτελεί κρίσιμο στοιχείο κινδύνου για την ανθεκτικότητα των οργανισμών, κάτι το οποίο αναγνωρίζεται από περισσότερα ΚΜ της Ένωσης[11].

Κίνητρα

Η κατανόηση των κινήτρων διαφορετικών παραγόντων απειλών είναι καίριας σημασίας για τον σχεδιασμό των κατάλληλων στρατηγικών άμυνας. Στα σημαντικότερα κίνητρα συγκαταλέγονται το οικονομικό όφελος (πραγματοποιείται κυρίως από ομάδες κυβερνοεγκληματιών), η κατασκοπεία (εκτελείται κυρίως από ομάδες που υποστηρίζονται από κράτη), η καταστροφή, ήτοι οποιαδήποτε καταστροφική ενέργεια που θα μπορούσε να έχει μη αναστρέψιμες συνέπειες, καθώς και η ιδεολογική σκοπιμότητα (όπως ο χακτιβισμός). Στην πλειονότητα των περιπτώσεων οι απειλές αποδίδονται σε ένα ή περισσότερα κίνητρα.

Αναδυόμενες Τεχνολογίες και Κρίσιμες Ψηφιακές Υποδομές στην Κυβερνοασφάλεια

Ο ταχύτατα αναπτυσσόμενος ψηφιακός μετασχηματισμός σε όλους τους κοινωνικούς τομείς της σύγχρονης εποχής λαμβάνει χώρα παράλληλα με την ανάδυση νέων τεχνολογιών, όπως είναι η Τεχνητή Νοημοσύνη (artificial intelligence - AI), η Κβαντική Υπολογιστική (quantum computing), το Διαδίκτυο των Πραγμάτων (IoT) και το Blockchain. Πρόκειται για τεχνολογικές καινοτομίες με πρωτοφανείς δυνατότητες, που όμως εισάγουν, παράλληλα, ραγδαίες προκλήσεις στον τομέα της κυβερνοασφάλειας. Οι εν λόγω προκλήσεις καθιστούν απαραίτητη την πλήρη κατανόηση των επιπτώσεών τους για το σχεδιασμό ανθεκτικών συστημάτων και τη διασφάλιση της προστασίας των δεδομένων.

Τεχνητή Νοημοσύνη (artificial intelligence)

Η τεχνητή νοημοσύνη είναι μία τεχνολογία που επιτρέπει σε υπολογιστικά συστήματα να προσομοιώνουν την ανθρώπινη μάθηση, την κατανόηση, την επίλυση προβλημάτων και τη λήψη αποφάσεων, με ποικίλα επίπεδα αυτονομίας. Στη σύγχρονη εποχή, η τεχνητή νοημοσύνη

[10] https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf

[11] Ενδεικτικά, Εθνικό Κέντρο Κυβερνοασφάλειας Ολλανδίας (NCSC) "Managing Insider Threats" (2024) https://english.ncsc.nl/publications/publications/2024/march/25/insiderthreats

αναδιαμορφώνει ριζικά το τοπίο της κυβερνοασφάλειας και έχει διττό ρόλο, καθώς εφαρμόζεται τόσο από τους επιτιθέμενους για κακόβουλη χρήση, όσο και από τους αμυνόμενους ως μέσο πρόληψης και προστασίας.

Επιθετικές χρήσης της τεχνητής νοημοσύνης[12]:

- **Εξελιγμένες επιθέσεις κοινωνικής μηχανικής (social engineering):** οι επιτιθέμενοι χρησιμοποιούν παραγωγική τεχνητή νοημοσύνη (Generative AI) για να δημιουργήσουν ψεύτικες ταυτότητες με δραστηριότητα σε κοινωνικά δίκτυα, καθώς και προσωποποιημένα μηνύματα που μιμούνται με ακρίβεια κάποιο έμπιστο άτομο. Επιπλέον, η τεχνολογία deep-fake μπορεί να δημιουργήσει ιδιαίτερα ρεαλιστικούς μη αληθινούς ήχους και video που μιμούνται πραγματικά πρόσωπα.
- **Δημιουργία προηγμένου κακόβουλου κώδικα:** οι επιτιθέμενοι υλοποιούν τεχνικές μηχανικής μάθησης (machine learning) για να δημιουργήσουν προηγμένο κακόβουλο κώδικα (malware) με νέα χαρακτηριστικά και δυνατότητες, το οποίο δύναται να παρακάμπτει την ανίχνευση από τα παραδοσιακά συστήματα ασφάλειας και να προσαρμόζεται στο περιβάλλον του οργανισμού - στόχου.
- **Ανίχνευση και εκμετάλλευση ευπαθειών:** Μεγάλα Γλωσσικά Μοντέλα (Large Language Models – LLMs) χρησιμοποιούνται κυρίως από κρατικά υποστηριζόμενους δρώντες, για να ανιχνεύουν ευπάθειες και να κατασκευάζουν exploits με αυτοματοποιημένο τρόπο αρκετά ταχύτερα σε σχέση με τις παραδοσιακές μεθόδους, μειώνοντας δραστικά το διαθέσιμο χρόνο των οργανισμών για την εφαρμογή των ενημερώσεων ασφάλειας (security patches).
- **Κλιμακούμενες και αυτόνομες επιθέσεις:** η τεχνητή νοημοσύνη επιτρέπει στους επιτιθέμενους να υλοποιούν ευρείας κλίμακας εκστρατείες με ελάχιστη ανθρώπινη παρέμβαση. Για παράδειγμα, τα botnets που έχουν ενισχυθεί με AI μπορούν να προσαρμόζουν τις στρατηγικές τους και να αλλάζουν τις τακτικές τους αυτόνομα, ανάλογα με το περιβάλλον της επίθεσης και τα αμυντικά μέτρα των οργανισμών.

Αμυντικές χρήσεις της τεχνητής νοημοσύνης[13]:

- **Βελτιωμένη ανίχνευση απειλών:** οι αλγόριθμοι μηχανικής μάθησης μπορούν να επεξεργάζονται και να παρακολουθούν σε πραγματικό χρόνο μεγάλα σύνολα δεδομένων δικτυακής κίνησης, συμπεριφοράς χρηστών και καταγραφών συμβάντων για αποκλίσεις από καθορισμένες τιμές βάσης (anomaly detection), με σκοπό την ανίχνευση ύποπτων ενεργειών, όπως απόπειρες μη εξουσιοδοτημένης πρόσβασης ή εξαγωγής δεδομένων (data exfiltration).
- **Προβλεπτική και προληπτική άμυνα (predictive and proactive defense):** τα συστήματα τεχνητής νοημοσύνης αναλύουν δεδομένα προηγούμενων επιθέσεων και

[12] ENISA Threat Landscape 2025 (October 2025), https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf , CrowdStrike 2025 Threat Hunting Report, https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/

[13] Μεταξύ πολλών άλλων, βλ. Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/ai-risks-and-benefits-in-cybersecurity

τρέχουσες εισροές από threat intelligence με στόχο την ανίχνευση αναδυόμενων μοτίβων επίθεσης. Αυτή η προβλεπτική δυνατότητα ενισχύει την άμυνα των οργανισμών έναντι πιθανών απειλών με προληπτικό τρόπο.

- **Αυτοματοποιημένη απόκριση σε περιστατικά:** τα συστήματα που είναι ενισχυμένα με AI μπορούν αυτόματα να ενεργοποιήσουν ενέργειες αντιμετώπισης απειλών, όπως η δικτυακή απομόνωση παραβιασμένων τερματικών ή το μπλοκάρισμα κακόβουλων IP διευθύνσεων. Αυτή η αυτοματοποίηση εμποδίζει την εξάπλωση των απειλών στο δίκτυο ενός οργανισμού, περιορίζει την επίπτωση και επιταχύνει την ανάκαμψη.
- **Προσαρμοστικά και αυτο-διδασκόμενα συστήματα:** τα συστήματα τεχνητής νοημοσύνης που έχουν εκπαιδευτεί μέσω ενισχυτικής μάθησης (reinforcement learning) μπορούν να προσαρμοστούν δυναμικά σε νέες μορφές επίθεσης, «μαθαίνοντας» από τη συμπεριφορά των αντιπάλων με τον ίδιο τρόπο που οι επιτιθέμενοι εκπαιδεύουν τα επιθετικά τους μοντέλα.

Πέρα από τη χρήση τους είτε για επιθετικούς είτε για αμυντικούς σκοπούς, παρατηρείται ότι τα ίδια τα συστήματα τεχνητής νοημοσύνης αποτελούν πλέον στόχο επιθέσεων μέσω ποικιλίας τεχνικών, όπως prompt injection, data and model poisoning, και supply chain vulnerabilities[14]. Δεδομένων των προκλήσεων και του διττού ρόλου της τεχνητής νοημοσύνης στην κυβερνοασφάλεια, διεθνείς οργανισμοί, η Ε.Ε., καθώς και και κράτη αναπτύσσουν ρυθμιστικά πλαίσια όπως η EU AI Act, το NIST AI Risk Management Framework και το OECD AI Principles. Η αποτελεσματική διαχείριση της τεχνητής νοημοσύνης απαιτεί ισχυρή διακυβέρνηση, ανθρώπινη επίβλεψη, ασφαλείς αλυσίδες εφοδιασμού, καθώς και πλαίσιο διαφάνειας και λογοδοσίας.

Κβαντική Υπολογιστική (quantum computing)

Η κβαντική υπολογιστική αντιπροσωπεύει μια άλλη σημαντική τεχνολογική αλλαγή, με βαθιές επιπτώσεις στην κυβερνοασφάλεια. Σε αντίθεση με τους κλασικούς υπολογιστές, οι οποίοι χρησιμοποιούν bits που αντιπροσωπεύουν είτε το 0 είτε το 1, οι κβαντικοί υπολογιστές χρησιμοποιούν qubits, τα οποία μπορούν να υπάρχουν ταυτόχρονα σε πολλαπλές καταστάσεις μέσω των αρχών της υπέρθεσης και της εμπλοκής. Αυτή η δυνατότητα τους επιτρέπει να λύνουν ορισμένους τύπους προβλημάτων εκθετικά ταχύτερα σε σχέση με τα παραδοσιακά συστήματα.

Στο ευρωπαϊκό πλαίσιο, η Quantum Europe Strategy θέτει το όραμα και τις υψηλού επιπέδου στοχεύσεις της Ένωσης για την ασφαλή και κυρίαρχη ανάπτυξη των κβαντικών τεχνολογιών έως το 2030. Η στρατηγική αυτή επιδιώκει την ενίσχυση της ερευνητικής και βιομηχανικής βάσης της ΕΕ, την οικοδόμηση ενός ολοκληρωμένου οικοσυστήματος καινοτομίας, καθώς και την ανάπτυξη αξιόπιστων ευρωπαϊκών υποδομών κβαντικής υπολογιστικής και επικοινωνιών. Παράλληλα, υπογραμμίζει τον ρόλο των κβαντικών τεχνολογιών ως πυλώνα κυβερνοασφάλειας, μέσω της προώθησης της κβαντικά ασφαλούς επικοινωνίας (EuroQCI) και της μείωσης στρατηγικών εξαρτήσεων από μη ευρωπαϊκούς παρόχους. Η σύνδεση της κβαντικής τεχνολογίας με την ανθεκτικότητα, την οικονομική ασφάλεια και την προστασία κρίσιμων υποδομών καθιστά τη μετάβαση στη μετα-κβαντική κρυπτογραφία ζήτημα στρατηγικής σημασίας για τα κράτη-μέλη, συμπεριλαμβανομένης της Ελλάδας.

[14] OWASP TOP 10 for LLM Applications 2025, https://owasp.org/www-project-top-10-for-large-language-model-applications/

Η σημαντικότερη ανησυχία για την κβαντική υπολογιστική από πλευράς κυβερνοασφάλειας είναι η δυνατότητά της να υπονομεύσει τους μηχανισμούς κρυπτογράφησης που ασφαλίζουν σήμερα σχεδόν κάθε ψηφιακό σύστημα. Ο θεμελιώδης κίνδυνος είναι η παραβίαση της κρυπτογραφίας δημοσίου κλειδιού (break public key encryption), η ασφάλεια του οποίου βασίζεται στην υπολογιστική δυσκολία της παραγοντοποίησης μεγάλων αριθμών ή της επίλυσης διακριτών λογαρίθμων. Οι κβαντικοί αλγόριθμοι, ιδίως ο αλγόριθμος του Shor, θα μπορούσαν θεωρητικά να εκτελέσουν αυτές τις εργασίες πολύ πιο γρήγορα, με συνέπεια την ευθεία παραβίαση των αλγόριθμων RSA, ECC (Elliptic Curve Cryptography) και Diffie-Hellman7. Το γεγονός αυτό θα καταστήσει τις σημερινές μεθόδους κρυπτογράφησης παρωχημένες και θα εκθέσει τα πληροφοριακά συστήματα στους εξής κινδύνους[15][16]:

- **Αποκρυπτογράφηση δεδομένων σε μεταγενέστερο χρόνο ("store now, decrypt later"):** οι επιτιθέμενοι υποκλέπτουν και αποθηκεύουν σήμερα δεδομένα εν αναμονή της ωρίμανσης των τεχνολογιών κβαντικής υπολογιστικής, όπου θα δύνανται να αποκρυπτογραφήσουν τα δεδομένα σε γρήγορο χρόνο. Στο σημείο αυτό δημιουργείται κίνδυνος ιδιαίτερα για ορισμένες κατηγορίες ευαίσθητων δεδομένων που λόγω της φύσης τους τηρούνται εμπιστευτικά για δεκαετίες.
- **Παραβίαση ψηφιακών υπογραφών και επαλήθευσης ταυτότητας:** οι ψηφιακές υπογραφές διασφαλίζουν την ακεραιότητα και την αυθεντικότητα της πληροφορίας. Εάν οι κβαντικοί υπολογιστές μπορούν να εξάγουν τα ιδιωτικά κλειδιά, τότε υπάρχει η δυνατότητα πλαστογράφησης ψηφιακών υπογραφών που θα εμφανίζονται ως νόμιμες. Το γεγονός αυτό θα επιτρέψει σε κακόβουλους δρώντες να υποδύονται κατασκευαστές λογισμικού ή χρήστες χωρίς τη δυνατότητα ανίχνευσης.
- **Παραβίαση ασφαλών επικοινωνιών:** τεχνολογίες όπως το TLS (Transport Layer Security), το HTTPS, τα VPNs και η κρυπτογράφηση των emails βασίζονται στην ανταλλαγή δημοσίων κλειδιών για την εγκαθίδρυση εμπιστοσύνης. Με τη χρήση κβαντικών υπολογιστών, οι επιτιθέμενοι θα μπορούν να αποκρυπτογραφήσουν δικτυακή κίνηση, να υποδύονται συσκευές ή να υποκλέπτουν κωδικούς πρόσβασης κατά τη μεταφορά δεδομένων. Το αποτέλεσμα θα είναι η απώλεια της εμπιστευτικότητας και αυθεντικότητας σε όλα τα παγκόσμια συστήματα επικοινωνιών.
- **Δημιουργία γεωπολιτικής αστάθειας:** τα πρώτα κράτη ή οργανισμοί που θα αναπτύξουν δυνατότητες κβαντικής υπολογιστικής θα αποκτήσουν δυσανάλογο πλεονέκτημα όσον αφορά στη διαχείριση πληροφοριών και στην άμυνα, καθώς κρυπτογραφημένα οικονομικά, διπλωματικά ή ακόμη και στρατιωτικού ενδιαφέροντος δεδομένα άλλων κρατών ή κρίσιμων υποδομών θα είναι εκτεθειμένα. Η εν λόγω ανισορροπία δύναται να επηρεάσει έως και τη δυναμική της παγκόσμιας ισχύος.

[15] European Commission, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (2025), https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[16] Palo Alto Networks, 8 Quantum Computing Cybersecurity Risks, https://www.paloaltonetworks.com/cyberpedia/what-is-quantum-computings-threat-to-cybersecurity

Στο πλαίσιο αυτό, ερευνητές και υπηρεσίες κυβερνοασφάλειας εργάζονται πάνω στη μετα-κβαντική κρυπτογραφία (post-quantum cryptography), δηλαδή σε κρυπτογραφικούς αλγόριθμους που θα είναι ανθεκτικοί στις κβαντικές επιθέσεις. Οργανισμοί όπως το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) έχουν ήδη εκκινήσει προγράμματα για την τυποποίηση τέτοιων αλγορίθμων[17].

Παρατηρούμε ότι και στην περίπτωση της κβαντικής υπολογιστικής, όπως αντίστοιχα στην τεχνητή νοημοσύνη, έχουμε μία αναδυόμενη τεχνολογία με πρωτοφανείς δυνατότητες, αλλά ταυτόχρονα με διττό ρόλο, καθώς μπορεί να χρησιμοποιηθεί και για νόμιμους και για κακόβουλους σκοπούς. Η προετοιμασία για τη μετάβαση στη μετα-κβαντική κρυπτογραφία θα απαιτήσει παγκόσμιο συντονισμό, έγκαιρη υιοθέτηση μετα-κβαντικών προτύπων και ευαισθητοποίηση τόσο μεταξύ των υπευθύνων χάραξης δημόσιων πολιτικών όσο και της βιομηχανίας.

Διαδίκτυο των Πραγμάτων (Internet of Things – IoT)

Το Διαδίκτυο των Πραγμάτων περιγράφει ένα δίκτυο φυσικών αντικειμένων ("things") που είναι ενσωματωμένα σε αισθητήρες, λογισμικό και άλλες τεχνολογίες, με σκοπό τη σύνδεση και ανταλλαγή δεδομένων με άλλες συσκευές και συστήματα στο Διαδίκτυο. Τα εν λόγω αντικείμενα περιλαμβάνουν κοινές οικιακές συσκευές έως και εξειδικευμένα βιομηχανικά συστήματα. Από τα έξυπνα σπίτια και τις φορητές συσκευές έως τους βιομηχανικούς αισθητήρες και τα αυτόνομα οχήματα, οι τεχνολογίες IoT καθίστανται αναπόσπαστο κομμάτι της καθημερινής ζωής και των σύγχρονων υποδομών και εκτιμάται ότι μέχρι το τέλος της δεκαετίας θα υπάρχουν παγκοσμίως δεκάδες δισεκατομμύρια συνδεδεμένες συσκευές.

Ενώ οι τεχνολογίες IoT βελτιώνουν την αποτελεσματικότητα, την ευκολία και τη λήψη αποφάσεων που βασίζονται σε δεδομένα, από την άλλη επεκτείνουν δραματικά την επιφάνεια των κυβερνοεπιθέσεων (attack surface). Οι σημαντικότερες ευπάθειες που παρατηρούνται στις IoT συσκευές είναι οι ακόλουθες[18]:

- **Αδύναμοι μηχανισμοί αυθεντικοποίησης:** Πολλές συσκευές IoT διαθέτουν προεπιλεγμένους (default) κωδικούς πρόσβασης, γεγονός που καθιστά εύκολη την παραβίασή τους από εισβολείς. Σε κάποιες περιπτώσεις, μάλιστα, οι κωδικοί πρόσβασης είναι ενσωματωμένοι (hard-coded) στον πηγαίο κώδικα της εφαρμογής. Η αδύναμη αυθεντικοποίηση ενέχει τον κίνδυνο της εύκολης παραβίασης της συσκευής και της ενσωμάτωσής της σε ένα ευρύ δίκτυο botnet, μέσω του οποίου οι επιτιθέμενοι μπορούν να εξαπολύσουν μεγάλης κλίμακας επιθέσεις κατανεμημένης άρνησης παροχής υπηρεσιών (distributed denial-of-service attacks).
- **Έλλειψη τακτικών ενημερώσεων λογισμικού:** σε αντίθεση με τα παραδοσιακά υπολογιστικά συστήματα. Πολλές συσκευές IoT δεν μπορούν εύκολα να λαμβάνουν ενημερώσεις και σε κάποιες περιπτώσεις οι κατασκευαστές σταματούν την υποστήριξη λίγο μετά την κυκλοφορία τους. Αυτό έχει σαν αποτέλεσμα την ύπαρξη

[17] https://csrc.nist.gov/projects/post-quantum-cryptography

[18] OWASP, IoT Top 10, https://owasp.org/www-project-internet-of-things/

πληθώρας ευπαθειών και τον συνακόλουθο κίνδυνο παραβίασης των εν λόγω συσκευών λόγω του ξεπερασμένου (outdated) λογισμικού και υλικολογισμικού τους (firmware).

- **Μετάδοση δεδομένων χωρίς κρυπτογράφηση:** πολλές συσκευές IoT αποστέλλουν ευαίσθητα δεδομένα σε μη κρυπτογραφημένη μορφή, καθιστώντας εύκολη την υποκλοπή τους μέσω ποικιλίας μεθόδων, όπως είναι π.χ. οι επιθέσεις ενδιάμεσου (man-in-the-middle attacks). Στα δεδομένα μπορούν να περιλαμβάνονται τα πάντα, από μετρήσεις αισθητήρων, σήματα εντολών, καθώς και δεδομένα χρήστη που μεταδίδονται μεταξύ συσκευών και κεντρικών συστημάτων.
- **Μη ασφαλείς δικτυακές υπηρεσίες:** σε πολλές συσκευές IoT περιλαμβάνονται μη απαραίτητες ή ανασφαλείς δικτυακές υπηρεσίες που εκτελούνται στην ίδια τη συσκευή, ειδικά εκείνες που είναι εκτεθειμένες στο Διαδίκτυο, οι οποίες θέτουν σε κίνδυνο την εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα ή τη διαθεσιμότητα των πληροφοριών ή επιτρέπουν τη μη εξουσιοδοτημένη εξ αποστάσεως πρόσβαση.

Επιπλέον, η σύγκλιση των συσκευών IoT και IIoT (industrial internet-of-things) με κρίσιμες υποδομές, όπως συστήματα υγειονομικής περίθαλψης, ενεργειακά δίκτυα και δίκτυα μεταφορών, αυξάνει τους κινδύνους. Μια κυβερνοεπίθεση σε συνδεδεμένες ιατρικές συσκευές ή βιομηχανικά συστήματα ελέγχου (industrial control systems) θα μπορούσε να έχει απειλητικές συνέπειες για την ανθρώπινη ζωή. Η πρόκληση έγκειται στην εξισορρόπηση της λειτουργικότητας, του κόστους και της ασφάλειας στο σχεδιασμό και στην ανάπτυξη συστημάτων IoT. Οι λύσεις περιλαμβάνουν την επιβολή αρχών ασφάλειας από το σχεδιασμό (security by design), την υιοθέτηση ισχυρής διαχείρισης ταυτότητας συσκευών και την προώθηση παγκόσμιων προτύπων για την κυβερνοασφάλεια του IoT.

Τεχνολογίες Blockchain και έξυπνα συμβόλαια (smart contracts)

Το blockchain είναι ένα είδος τεχνολογίας κατανεμημένου καθολικού (distributed ledger technology) που έχει σχεδιαστεί για να καταγράφει συναλλαγές σε ένα δίκτυο υπολογιστών, οι οποίες θα είναι ανθεκτικές στην παραβίαση. Σε αντίθεση με τις παραδοσιακές βάσεις δεδομένων, όπου η εγκαθίδρυση εμπιστοσύνης στηρίζεται στην ύπαρξη μίας κεντρικής αρχής, το blockchain λειτουργεί σε ένα αποκεντρωμένο και κατανεμημένο περιβάλλον, στο οποίο τα δεδομένα αποθηκεύονται σε “blocks” που συνδέονται μεταξύ τους χρονολογικά σε μία «αλυσίδα» (chain).

Θεμελιακό στοιχείο των σύγχρονων συστημάτων blockchain αποτελούν τα «έξυπνα συμβόλαια» (smart contracts). Πρόκειται για υπολογιστικά προγράμματα που εκτελούνται αυτόματα (self-executing) όταν πληρούνται προκαθορισμένοι όροι και προϋποθέσεις και λειτουργούν ως ψηφιακά συμβόλαια που αποθηκεύονται στο δίκτυο του blockchain.

Το blockchain υλοποιεί μία σειρά προηγμένων κρυπτογραφικών μηχανισμών, όπως είναι η κρυπτογραφία δημοσίου κλειδιού, οι συναρτήσεις κατακερματισμού (hashing) και οι ψηφιακές υπογραφές, οι οποίες διασφαλίζουν την αυθεντικότητα και τη μη-αποποίηση (non-repudiation) των συναλλαγών. Λόγω του γεγονότος ότι κάθε block περιλαμβάνει το hash του προηγούμενου block, το blockchain επιτυγχάνει την έννοια του αμετάβλητου (immutability): η αλλοίωση ενός block θα απαιτούσε την τροποποίηση όλων των επακόλουθων blocks, το οποίο είναι υπολογιστικά ανέφικτο σε μεγάλα δίκτυα. Σαν αποτέλεσμα, η τεχνολογία blockchain μπορεί να χρησιμοποιηθεί για την ασφαλή

καταγραφή κάθε είδους συναλλαγών (κρυπτονομίσματα, μεταβιβάσεις κινητών και ακινήτων, αγοραπωλησίες ενέργειας, επαλήθευση πνευματικών δικαιωμάτων, ιχνηλάτηση κίνησης προϊόντων κ.α.), μειώνοντας το συναλλακτικό κόστος και καταπολεμώντας τη γραφειοκρατία. Ενώ η αποκεντρωμένη φύση του blockchain αφαιρεί συγκεκριμένους κινδύνους (π.χ. επιθέσεις σε κεντρικούς διακομιστές), ταυτόχρονα εισάγει νέους[19]:

- **Επιθέσεις «51%» (51% attacks):** λαμβάνουν χώρα όταν οι επιτιθέμενοι αποκτούν τον έλεγχο περισσότερου του μισού της υπολογιστικής δύναμης (computing power) ενός δικτύου blockchain, επιτρέποντας την τροποποίηση του ιστορικού των συναλλαγών και τη διενέργεια διπλών δαπανών (double spending). Περισσότερο ευπαθή στις εν λόγω επιθέσεις είναι τα μικρότερα δίκτυα blockchain, λόγω χαμηλότερης υπολογιστικής δύναμης.
- **Sybil attacks:** στην περίπτωση αυτή, οι επιτιθέμενοι δημιουργούν πολλαπλές ψευδείς ταυτότητες, με αποτέλεσμα να αποκτούν δυσανάλογη επιρροή στο peer-to-peer δίκτυο του blockchain, με σκοπό τη χειραγώγησή του.
- **Ευπάθειες έξυπνων συμβολαίων:** πρόκειται για ευπάθειες στον κώδικα των έξυπνων συμβολαίων, όπως επιθέσεις επανεισόδου (reentrancy attacks), υπερχείλιση / υποχείλιση ακεραίων (integer overflow / underflow), τρωτότητες στον έλεγχο πρόσβασης, επιθέσεις άρνησης παροχής υπηρεσίας και λογικά λάθη (business logic vulnerabilities).
- **Κρυπτογραφικές αδυναμίες:** η ασφάλεια του blockchain βασίζεται στην ισχυρή κρυπτογραφία. Οι ευπάθειες στο συγκεκριμένο πεδίο πηγάζουν από ξεπερασμένους αλγόριθμούς κατακερματισμού, από λάθη στην υλοποίηση παραγωγής τυχαίων αριθμών, καθώς και από λάθη στη δημιουργία κρυπτογραφικών κλειδιών.

Η τεχνολογία του blockchain παρουσιάζει νομοθετικές και κανονιστικές προκλήσεις λόγω της αποκεντρωμένης φύσης της. Ένα σημείο-κλειδί είναι η δικαιοδοσία (jurisdiction): επειδή τα δίκτυα blockchain εκτείνονται σε πολλές χώρες, αναφύονται ζητήματα σχετικά με το εφαρμοστέο δίκαιο σε κάθε χωριστή περίπτωση, όπως σε συναλλαγές, δεδομένα ή ακόμη και σε δικαστικές διαφορές. Επίσης, ένα πρόσθετο ζήτημα είναι η προστασία των δεδομένων προσωπικού χαρακτήρα: η αμετάβλητη φύση του blockchain πρέπει να συμμορφώνεται ιδίως με τον ΓΚΠΔ, ο οποίος παρέχει στα φυσικά πρόσωπα – χρήστες το δικαίωμα διόρθωσης ή διαγραφής των προσωπικών δεδομένων που τα αφορούν. Η διασφάλιση της συμμόρφωσης με την ταυτόχρονη τήρηση της ακεραιότητας του blockchain παραμένει ένα πολύπλοκο πρόβλημα.

Τεχνολογίες Νέφους (Cloud Computing) και Big Data

Η αποθήκευση και επεξεργασία δεδομένων στο υπολογιστικό νέφος (Cloud Computing) αποτελεί πλέον δομικό στοιχείο της λειτουργίας επιχειρήσεων και οργανισμών. Τα μοντέλα cloud (IaaS, PaaS, SaaS) προσφέρουν κλιμάκωση, ευελιξία και σημαντικές οικονομίες κλίμακας, αλλά ταυτόχρονα εισάγουν νέους κινδύνους και εξαρτήσεις από τρίτους παρόχους.

[19] OWASP Smart Contract Top 10, https://owasp.org/www-project-smart-contract-top-10/

Κρίσιμες προκλήσεις για την κυβερνοασφάλεια στον χώρο του cloud περιλαμβάνουν:

- τον κίνδυνο παραβίασης της ιδιωτικότητας και διαρροής δεδομένων,
- την εσφαλμένη παραμετροποίηση υπηρεσιών και υποδομών,
- την ασαφή κατανόηση ή παρερμηνεία του μοντέλου κοινής ευθύνης (shared responsibility model),
- την συγκέντρωση κρίσιμων δεδομένων και υπηρεσιών σε περιορισμένο αριθμό παρόχων μεγάλης κλίμακας (hyperscalers), με συνακόλουθες επιπτώσεις στην ανθεκτικότητα, την εξάρτηση και την τεχνολογική κυριαρχία.

Αντίστοιχα, τα Big Data δημιουργούν ανάγκη προστασίας τόσο των ίδιων των δεδομένων όσο και της διαδικασίας συλλογής τους, η οποία μπορεί να είναι αδιαφανής ή καταχρηστική. Η αξιοποίηση μεγάλων δεδομένων για σκοπούς ανάλυσης, επιχειρηματικής ευφυΐας ή πρόβλεψης συμπεριφορών πρέπει να συμμορφώνεται με τις αρχές της προστασίας δεδομένων προσωπικού χαρακτήρα, της ελαχιστοποίησης δεδομένων και της λογοδοσίας.

Η ενίσχυση της ασφάλειας στο cloud και στα Big Data προϋποθέτει:

- σαφή προσδιορισμό ρόλων και ευθυνών μεταξύ παρόχου και πελάτη,
- υιοθέτηση ισχυρών πρακτικών διαχείρισης ταυτοτήτων και προσβάσεων (IAM),
- κρυπτογράφηση δεδομένων σε μεταφορά και αποθήκευση,
- τακτικούς ελέγχους συμμόρφωσης και αξιολόγηση κινδύνων στην εφοδιαστική αλυσίδα υπηρεσιών cloud.

Υποθαλάσσια καλώδια τηλεπικοινωνιών ως κρίσιμη υποδομή

Τα υποθαλάσσια καλώδια τηλεπικοινωνιών, όπως και το σύνολο της βασικής υποδομής κορμού του διαδικτύου (backbone infrastrucure), συνιστούν κρίσιμη πρόκληση για την παγκόσμια ασφάλεια, καθώς αποτελούν τη ραχοκοκαλιά της ψηφιακής επικοινωνίας. Η διασύνδεση κρατών, οικονομιών και κοινωνιών εξαρτάται σχεδόν αποκλειστικά από αυτά, δεδομένου ότι μεταφέρουν τη συντριπτική πλειονότητα της παγκόσμιας διαδικτυακής κίνησης. Οποιαδήποτε παρακολούθηση, βλάβη ή διακοπή τους μπορεί να επιφέρει ανυπολόγιστες γεωπολιτικές και οικονομικές συνέπειες.

Παρά τη σημαντική ανάπτυξη των χερσαίων δικτύων, η Ευρωπαϊκή Ένωση παραμένει εξαιρετικά εξαρτημένη από τα υποθαλάσσια καλώδια, ενώ την τελευταία δεκαετία το μερίδιο των ευρωπαϊκών τηλεπικοινωνιακών παρόχων έχει μειωθεί, με τις εταιρείες τεχνολογίας μεγάλης κλίμακας (hyperscalers) να ενισχύουν σταθερά τον έλεγχό τους. Η κατάσταση αυτή καθιστά επιτακτική την ανάγκη ανάπτυξης ανθεκτικών, ασφαλών και τεχνολογικά αυτόνομων υποθαλάσσιων υποδομών, ικανών να διασφαλίσουν την οικονομική και στρατηγική κυριαρχία της Ένωσης στο ψηφιακό πεδίο.

Ενίσχυση της Ασφάλειας Αναδυόμενων Τεχνολογιών και Κρίσιμων Υποδομών Συνδεσιμότητας

Η ταχεία εξέλιξη των αναδυόμενων τεχνολογιών και η αυξανόμενη εξάρτηση της οικονομίας και της κοινωνίας από κρίσιμες ψηφιακές υποδομές καθιστούν επιτακτική την ανάγκη για μια συνεκτική στρατηγική προσέγγιση που θα ενισχύει την τεχνολογική κυριαρχία και την ψηφιακή ασφάλεια της χώρας. Στο επίπεδο της Ευρωπαϊκής Ένωσης, η Στρατηγική Κυβερνοασφάλειας για την Ψηφιακή

Δεκαετία [20] θέτει το πλαίσιο για ένα ασφαλές, ανθεκτικό και τεχνολογικά αυτόνομο ψηφιακό οικοσύστημα έως το 2030, δίνοντας έμφαση:

- στη μείωση της εξάρτησης από τρίτες χώρες σε κρίσιμες τεχνολογίες και υποδομές,
- στην προώθηση της υπεύθυνης, ηθικής και ασφαλούς χρήσης της τεχνολογίας,
- στη διασφάλιση ανθεκτικών, ασφαλών και διαλειτουργικών υποδομών συνδεσιμότητας, cloud και δεδομένων,
- στην προστασία της ψηφιακής ανεξαρτησίας και της στρατηγικής αυτονομίας της Ένωσης.

Οι αναδυόμενες τεχνολογίες (όπως η Τεχνητή Νοημοσύνη, η Κβαντική Υπολογιστική, το IoT/IIoT και το Blockchain) και οι κρίσιμες ψηφιακές υποδομές (όπως τα δίκτυα 5G, οι υπηρεσίες υπολογιστικού νέφους και τα υποθαλάσσια καλώδια) αναμορφώνουν δραστικά το τοπίο της κυβερνοασφάλειας. Η «οπλοποίηση» της τεχνολογικής προόδου, η διεύρυνση της επιφάνειας επίθεσης και η ταχύτητα με την οποία εξελίσσονται οι απειλές δημιουργούν νέες προκλήσεις, αλλά και ευκαιρίες για ενίσχυση της εθνικής και ευρωπαϊκής ανθεκτικότητας.

Σε αυτό το πλαίσιο, απαιτείται μια ολιστική, προληπτική και προσαρμοστική στρατηγική κυβερνοασφάλειας, η οποία:

- ενσωματώνει με ασφάλεια τις αναδυόμενες τεχνολογίες στις δημόσιες και ιδιωτικές υποδομές,
- ενισχύει την εγχώρια ικανότητα καινοτομίας και την ανάπτυξη ψηφιακών δεξιοτήτων,
- υιοθετεί σύγχρονα κανονιστικά και θεσμικά εργαλεία,
- στηρίζεται στη διεθνή και ευρωπαϊκή συνεργασία,
- ενδυναμώνει την ανθεκτικότητα κρίσιμων ψηφιακών υποδομών και αλυσίδων εφοδιασμού,
- προωθεί την ασφάλεια, την ιδιωτικότητα και την προστασία θεμελιωδών δικαιωμάτων στον ψηφιακό χώρο.

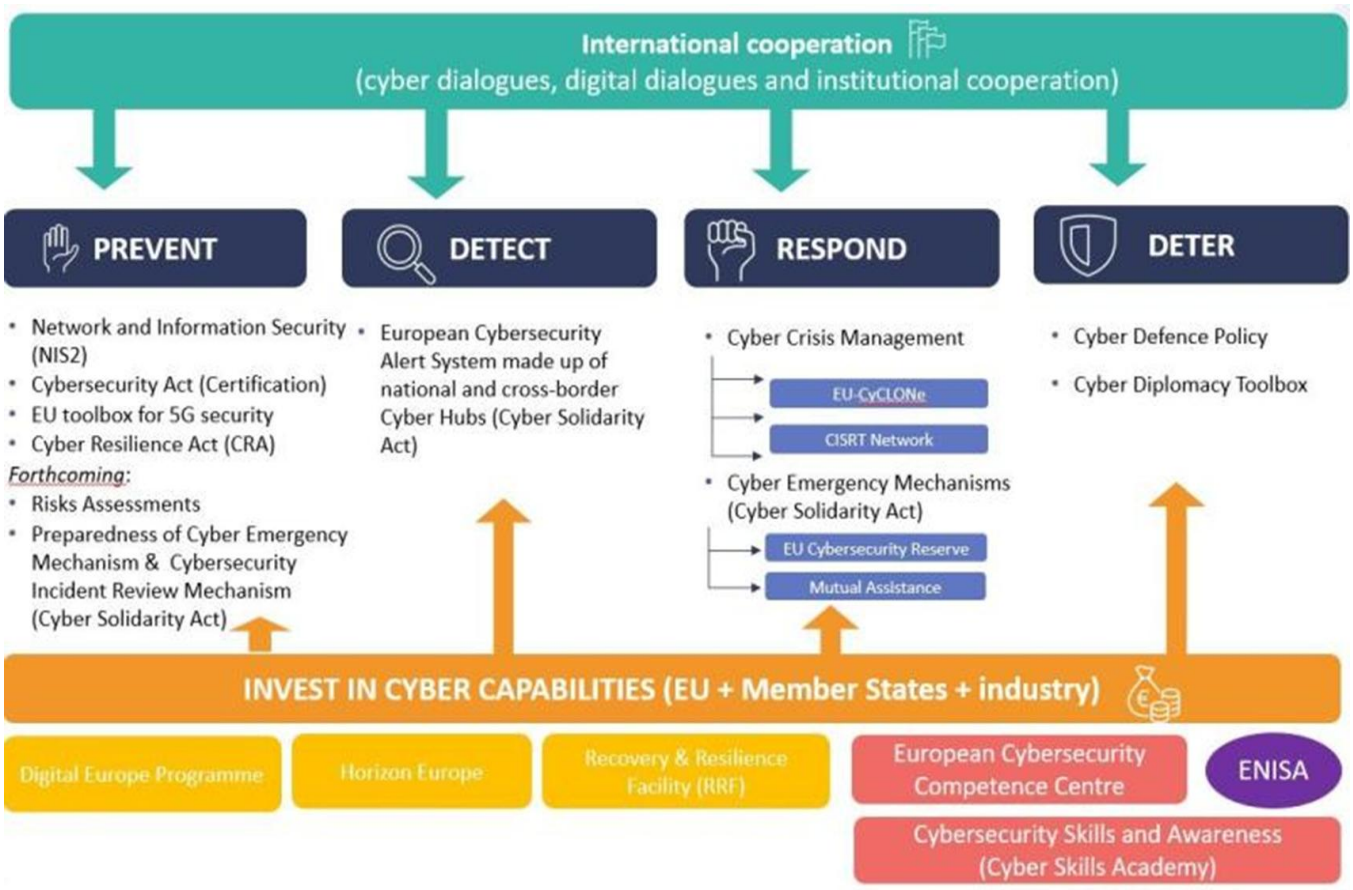
Με μια τέτοια στρατηγική αντίληψη, οι τεχνολογικές προκλήσεις μπορούν να μετατραπούν σε καταλύτες για ένα ασφαλές, αξιόπιστο και ανταγωνιστικό ψηφιακό περιβάλλον, ενισχύοντας την εθνική και ευρωπαϊκή ασφάλεια και συμβάλλοντας στην επίτευξη των στόχων της Ψηφιακής Δεκαετίας.

1.Β Εξελίξεις στο Κανονιστικό Επίπεδο

Ενωσιακό και εθνικό δίκαιο κυβερνοασφάλειας

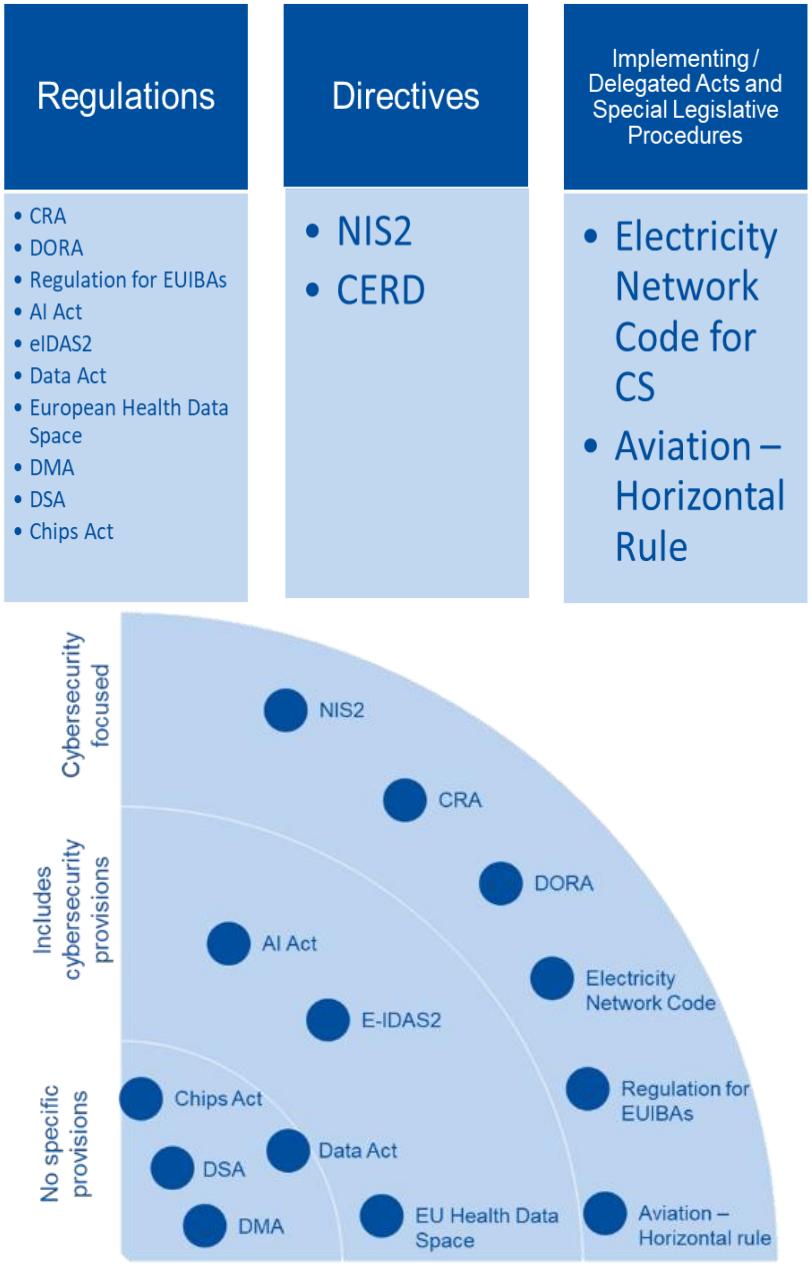
Η κυβερνοασφάλεια έχει αναδειχθεί σε δημόσια πολιτική αυξημένης προτεραιότητας για την Ευρωπαϊκή Ένωση. Η ΕΕ διαμορφώνει ένα συνεκτικό ρυθμιστικό και επιχειρησιακό πλαίσιο που στοχεύει σε κοινό υψηλό επίπεδο κυβερνοανθεκτικότητας στα κράτη-μέλη, καλύπτοντας τους πυλώνες της πρόληψης, της ανίχνευσης, της απόκρισης και της αποτροπής, με παράλληλη ενίσχυση των αρμόδιων ευρωπαϊκών φορέων και αξιοποίηση χρηματοδοτικών εργαλείων.

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018



Εικόνα 3: Ολοκληρωμένη Προσέγγιση της ΕΕ για την ενίσχυση της κυβερνοασφάλειας[21]

[21] Πηγή https://digital-strategy.ec.europa.eu/en/policies/cybersecurity



Εικόνα 4: Το βασικό ενωσιακό δίκαιο κυβερνοασφάλειας (πηγή: ENISA)

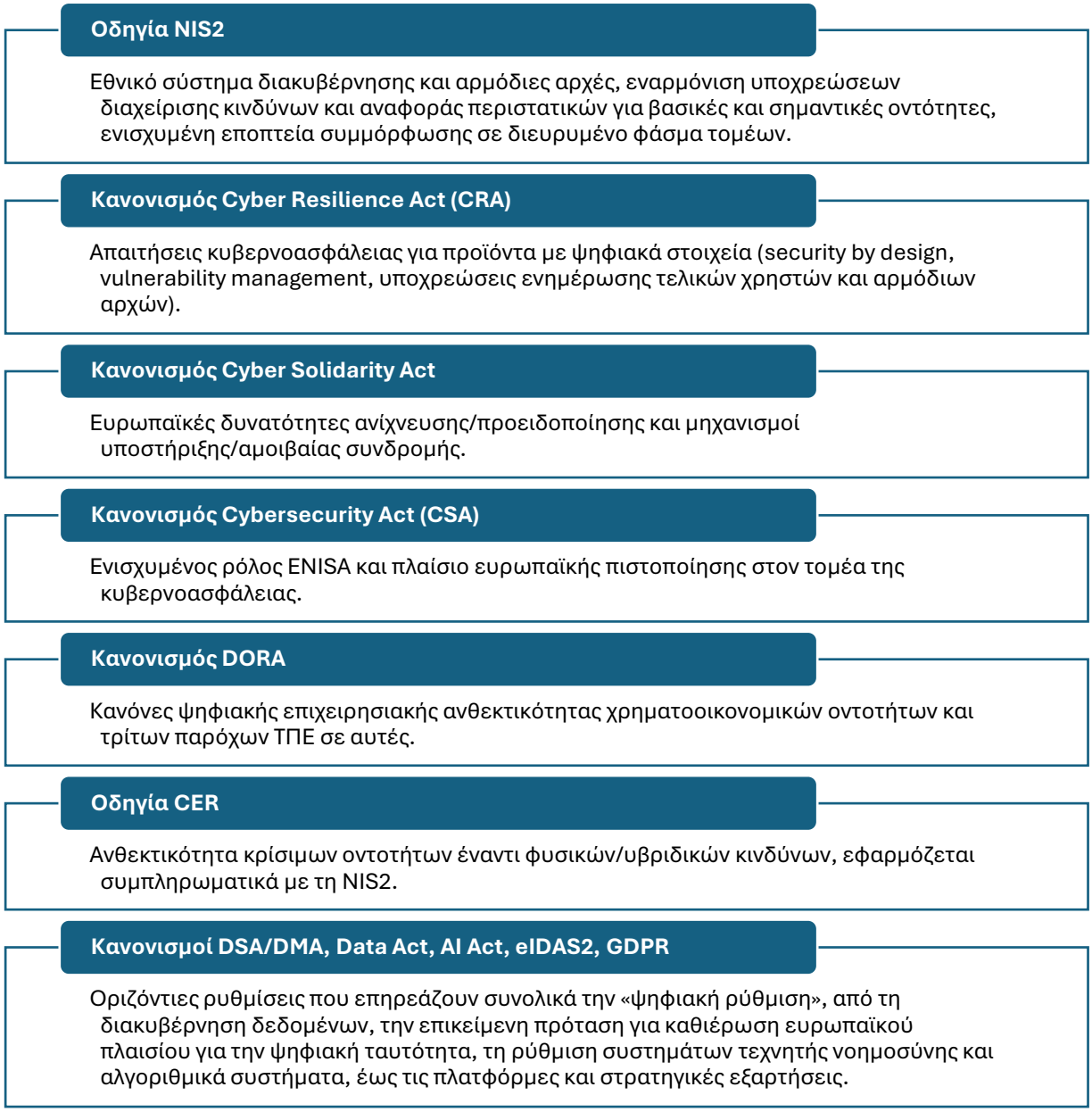
Βασικό χαρακτηριστικό του ενωσιακού πλαισίου είναι η εκτεταμένη θέσπιση παραγώγου ενωσιακού δικαίου, ιδίως Κανονισμών (άμεσης εφαρμογής). Το συνολικό οικοσύστημα κανόνων επεκτείνεται πέραν της «παραδοσιακής» έννοιας της κυβερνοασφάλειας, καλύπτοντας προϊόντα με ψηφιακά στοιχεία, ψηφιακές πλατφόρμες, δεδομένα, τεχνητή νοημοσύνη και ψηφιακή ταυτότητα.

Περαιτέρω, θεμελιώδη πυλώνα στο ανωτέρω οικοσύστημα συνιστά η Οδηγία NIS2, η οποία ως κεντρικό νομοθέτημα εναρμόνισης που επηρεάζει το σύστημα διακυβέρνησης, την εποπτεία και τις υποχρεώσεις διαχείρισης κινδύνων και αναφοράς περιστατικών εκ μέρους των βασικών και σημαντικών οντοτήτων, θέτει υποχρεώσεις λήψης μέτρων και αναφοράς περιστατικών σε ένα ευρύ

φάσμα επιχειρήσεων και οργανισμών που δραστηριοποιούνται σε δεκάδες τομείς, που εκτείνονται από τους παραδοσιακούς κρίσιμους τομείς (όπως τράπεζες, ενέργεια, υγεία) έως ένα ευρύ φάσμα της οικονομικής και κοινωνικής δραστηριότητας (όπως, το σύνολο της εφοδιαστικής αλυσίδας παραγωγής τροφίμων έως υπηρεσίες ταχυμεταφορών και τον κατασκευαστικό κλάδο).

Για την Εθνική Στρατηγική 2026–2030, οι βασικές συνέπειες του ενωσιακού κανονιστικού πλαισίου συνοψίζονται στα εξής:

- Ενίσχυση διακυβέρνησης και εποπτείας: σαφείς αρμοδιότητες, αυστηρότερη συμμόρφωση και κυρώσεις (ιδίως NIS2/DORA).
- Ασφάλεια αλυσίδας εφοδιασμού και προϊόντων: υποχρεώσεις “security by design” και διαχείριση τρωτότητας σε όλο τον κύκλο ζωής (CRA).
- Ευρωπαϊκή επιχειρησιακή ετοιμότητα και αλληλεγγύη: μηχανισμοί έγκαιρης προειδοποίησης, συντονισμού και υποστήριξης σε συμβάντα μεγάλης κλίμακας και δημιουργία Ευρωπαϊκού Αποθεματικού Κυβερνοασφάλειας (Cyber Solidarity Act).
- Πιστοποίηση και εμπιστοσύνη στην ενιαία αγορά: ενιαίο ευρωπαϊκό πλαίσιο πιστοποίησης και ρόλος των εθνικών αρχών και ενίσχυση των αρμοδιοτήτων του ENISA (Cybersecurity Act/ENISA).
- Σύγκλιση κυβερνοασφάλειας–προστασίας δεδομένων και ψηφιακής ρύθμισης: ανάγκη συνεκτικής εφαρμογής GDPR/Data Act/eIDAS2/DSA/DMA/AI Act σε επίπεδο οργανισμών και δημόσιων πολιτικών.



Εικόνα 5: Βασικό Κανονιστικό Ενωσιακό Πλαίσιο

Η υλοποίηση των στόχων που θέτει το ανωτέρω ενωσιακό πλαίσιο, καθώς και των πρόσφατων εθνικών ρυθμίσεων προσαρμογής σε αυτό, αποτελούν το ελάχιστο δεσμευτικό ρυθμιστικό πλαίσιο, εντός του οποίου κινείται η χώρα για την επίτευξη των εθνικών στόχων κυβερνοασφάλειας. Για την πληρεστερη εφαρμογή του ενωσιακού δικαίου, ψηφίζονται αντίστοιχες εθνικές ρυθμίσεις, με βασικότερη εθνική νομοθεσία το ν. 5160/2024, με τον οποίο μεταφέρθηκε στην ελληνική νομοθεσία η Οδηγία NIS2, θέτοντας το βασικό πλαίσιο διακυβέρνησης της δημόσιας πολιτικής κυβερνοασφάλειας στη χώρα μας.

2. Μεθοδολογία Ανάπτυξης της Στρατηγικής

Εργαλεία και διαδικασίες για τη διαμόρφωση της ΕΣΚ 2026–2030 και του Σχεδίου Δράσης

Στο πλαίσιο της διαμόρφωσης της νέας Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026–2030 και του αντίστοιχου Σχεδίου Δράσης, η αξιοποίηση στοχευμένων εργαλείων και οργανωμένων πρωτοβουλιών διαβούλευσης παρήγαγε ουσιαστικά αποτελέσματα και συνέβαλε καθοριστικά στον καθορισμό των στρατηγικών προτεραιοτήτων και στον σχεδιασμό συγκεκριμένων παρεμβάσεων.

Συνοπτικά, παρουσιάζονται κατωτέρω τα βασικά εργαλεία και τα αποτελέσματα των διαβουλεύσεων που υποστήριξαν τη διαδικασία αυτή:

Πιλοτική εφαρμογή του NCAF v2.0

Το Πλαίσιο Αξιολόγησης Εθνικών Ικανοτήτων - National Capabilities Assessment Framework (NCAF) του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), αποτελεί βασικό εργαλείο αυτοαξιολόγησης για τα κράτη μέλη της ΕΕ, επιτρέποντας τους να μετρήσουν το επίπεδο ωριμότητας των εθνικών τους ικανοτήτων στον τομέα της κυβερνοασφάλειας και να προσαρμόσουν ανάλογα τις εθνικές πολιτικές τους.

Σε συνέχεια της αναθεώρησης της Οδηγίας NIS, ο ENISA προχώρησε στην αναθεώρηση του NCAF διασφαλίζοντας ότι τα κράτη μέλη διαθέτουν ένα σύγχρονο πλαίσιο για την αξιολόγηση και τη συνεχή βελτίωση των εθνικών τους ικανοτήτων.

Συμβολή του NCAF v2.0 στην αναθεώρηση της εθνικής στρατηγικής

Η πιλοτική εφαρμογή του NCAF v2.0 συνέβαλε ουσιαστικά στη διαμόρφωση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026–2030, υποστηρίζοντας την αναλυτική τεκμηρίωση και τον στρατηγικό σχεδιασμό μέσω των ακόλουθων βασικών συνεισφορών:

- Παρείχε ένα δομημένο πλαίσιο που διευκόλυνε την ευθυγράμμιση των εθνικών προτεραιοτήτων με τις στρατηγικές κατευθύνσεις και τις κανονιστικές απαιτήσεις της Ευρωπαϊκής Ένωσης.
- Προσέφερε μια συστηματική δεξαμενή ιδεών για την ανάπτυξη νέων παρεμβάσεων και δράσεων.
- Υποστήριξε την ενσωμάτωση μιας προσέγγισης βασισμένης σε επίπεδα ωριμότητας στον κύκλο κατάρτισης της στρατηγικής, επιτρέποντας έναν περισσότερο ρεαλιστικό σχεδιασμό και μια πιο εξειδικευμένη και μετρήσιμη παρακολούθηση της υλοποίησης για την περίοδο 2026–2030.

10 Βασικά Συμπεράσματα από την Εφαρμογή του Pilot NCAF v2.0		
1	Ενισχυμένη ευθυγράμμιση με NIS2 και το ευρωπαϊκό πλαίσιο	Το αναθεωρημένο NCAF υποστηρίζει την πλήρη ενσωμάτωση των απαιτήσεων NIS2, διευκολύνοντας τον σχεδιασμό πολιτικών σύμφωνα με τις ευρωπαϊκές κατευθύνσεις.
2	Σαφής και ολοκληρωμένη δομή στρατηγικού σχεδιασμού	Τα clusters και οι στόχοι του NCAF παρείχαν ένα συνεκτικό πλαίσιο για την αναδιάρθρωση των αξόνων της εθνικής στρατηγικής.
3	Ακριβέστερη αποτύπωση εθνικού επιπέδου ωριμότητας	Το μοντέλο επιπέδων ωριμότητας επέτρεψε συγκεκριμένη και ρεαλιστική αξιολόγηση της υφιστάμενης κατάστασης στις θεματικές περιοχές του εργαλείου.
4	Ανάδειξη ασυμμετριών μεταξύ στρατηγικής και εφαρμογής	Η διάκριση μεταξύ “maturity” και “coverage” αποκάλυψε τομείς όπου οι πολιτικές υπάρχουν αλλά δεν εφαρμόζονται ομοιόμορφα.
5	Ανάγκη ενίσχυσης της διακυβέρνησης και του οριζόντιου συντονισμού	Η αξιολόγηση ανέδειξε απαιτήσεις για πιο συνεκτικούς μηχανισμούς συνεργασίας και καλύτερη διασύνδεση μεταξύ φορέων.
6	Εντοπισμός ρυθμιστικών κενών και αναγκών επικαιροποίησης	Το NCAF κατέδειξε περιοχές όπου απαιτούνται επικαιροποιήσεις ή συμπληρωματικές ρυθμιστικές παρεμβάσεις.
7	Ανάδειξη επιχειρησιακών ελλείψεων σε ορισμένους τομείς	Εντοπίστηκαν ανάγκες βελτίωσης σε διαδικασίες, υποδομές και ικανότητες που σχετίζονται με την αποτελεσματική απόκριση σε περιστατικά.
8	Επιβεβαίωση των αναγκών σε δεξιότητες και ενίσχυση ανθρώπινου δυναμικού	Η αξιολόγηση υπογράμμισε την κρίσιμη σημασία της ενίσχυσης των ικανοτήτων, της εκπαίδευσης και της εξειδίκευσης.
9	Μετάβαση σε τεκμηριωμένη χάραξη πολιτικής	Το NCAF ενίσχυσε τον προσανατολισμό σε evidence-based policymaking, συμβάλλοντας σε στοχευμένες αποφάσεις και αποδοτική κατανομή πόρων.
10	Δημιουργία σταθερής βάσης για συνεχή παρακολούθηση και βελτίωση	Η εφαρμογή του NCAF καθιερώνει ένα επαναλαμβανόμενο και συστηματικό εργαλείο αξιολόγησης, ενσωματωμένο στον ετήσιο κύκλο εθνικού σχεδιασμού και παρακολούθησης.

Δείκτης Κυβερνοασφάλειας της ΕΕ

Εκτός από την πιλοτική εφαρμογή του NCAF v2.0 για την αναθεωρημένη Εθνική Στρατηγική Κυβερνοασφάλειας 2026–2030, αξιοποιήθηκαν επίσης τα αποτελέσματα του Δείκτη Κυβερνοασφάλειας 2024 (EU Cybersecurity Index – EU-CSI). Ο EU-CSI αποτελεί εργαλείο αποτύπωσης του επιπέδου ετοιμότητας και ωριμότητας των κρατών μελών και της Ευρωπαϊκής Ένωσης στον τομέα της κυβερνοασφάλειας και χρησιμεύει ως βάση για την ποσοτική και ποιοτική αξιολόγηση των εθνικών ικανοτήτων και πόρων, σύμφωνα με το άρθρο 18 της Οδηγίας NIS2. Ο δείκτης αναπτύσσεται και υλοποιείται από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (ENISA), σε συνεργασία με τα κράτη μέλη μέσω του Δικτύου National Liaison Officers (NLO).

Η αποτύπωση της εθνικής επίδοσης στον ENISA Cybersecurity Index 2024, αναδεικνύει σημαντικές διαρθρωτικές προκλήσεις που η νέα Εθνική Στρατηγική καλείται να αντιμετωπίσει: υστέρηση στη διαμόρφωση και εφαρμογή ολοκληρωμένων πολιτικών κυβερνοασφάλειας, χαμηλό επίπεδο ωρίμανσης στα εθνικά συστήματα κατάρτισης, ευαισθητοποίησης και ενίσχυσης δεξιοτήτων, καθώς και κενά στη συνεργασία και τον συντονισμό σε εθνικό επίπεδο. Παράλληλα, επισημαίνονται θέματα προετοιμασίας για την αντιμετώπιση κυβερνοεπιθέσεων, ελλείψεις σε μηχανισμούς εποπτείας για φορείς κρίσιμων τομέων και περιορισμένη ενσωμάτωση της κυβερνοασφάλειας στην εκπαίδευση και τις επιχειρησιακές διαδικασίες των οργανισμών. Οι αδυναμίες αυτές, ιδίως στους τομείς χάραξης πολιτικής, ανάπτυξης δεξιοτήτων και επιχειρησιακού συντονισμού, καθιστούν τον δείκτη βασικό εργαλείο για τον αναπροσανατολισμό προτεραιοτήτων και τη στοχευμένη ενίσχυση της εθνικής κυβερνοανθεκτικότητας.

Τα πεδία αυτά δεν συνιστούν αδυναμίες με τη στενή έννοια του όρου. Αντιθέτως, αποτελούν τομείς πολιτικής και επιχειρησιακής ικανότητας όπου απαιτείται συστηματική και στοχευμένη βελτίωση, προκειμένου η Ελλάδα να επιτύχει υψηλότερο επίπεδο κυβερνοασφάλειας σε εθνική κλίμακα.

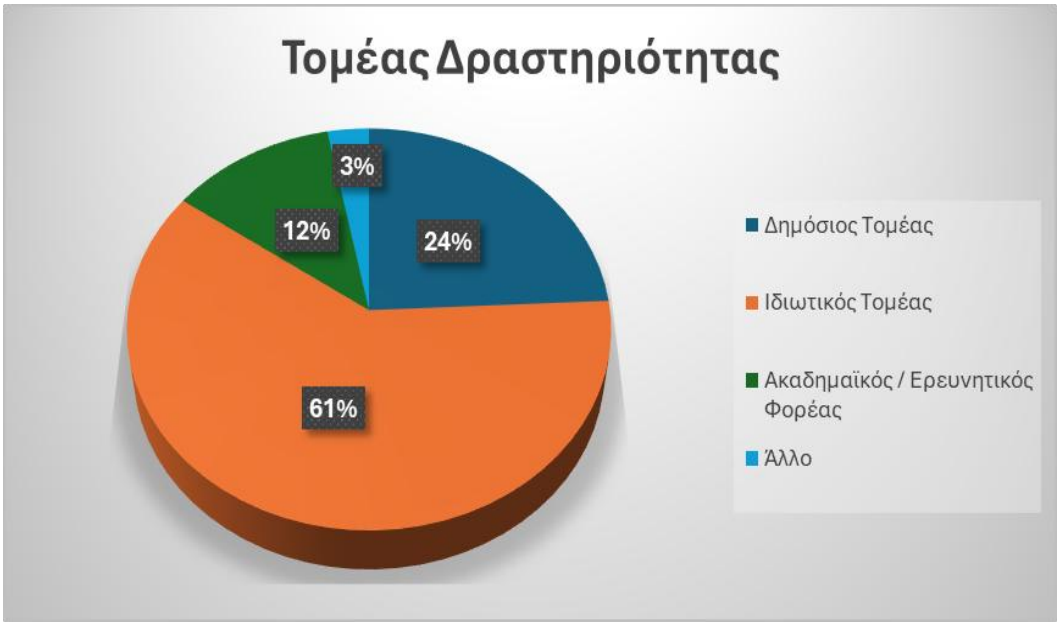
Ερωτηματολόγιο Δημόσιας Διαβούλευσης

Μια διαδικασία, η οποία επίσης συνέβαλε στη διαμόρφωση της Εθνικής Στρατηγικής υπήρξε η Δημόσια Διαβούλευση που διενεργήθηκε από την Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ) επί θεματικών ενοτήτων της νέας ΕΣΚ 2026-2030 για το διάστημα από 10 Οκτωβρίου 2025 έως και 10 Νοεμβρίου 2025. Επισημαίνοντας τη σημασία της διαβούλευσης ως έναν ουσιαστικό και αναγκαίο μηχανισμό, ο οποίος προάγει τη συμμετοχικότητα και καθιστά τους συμμετέχοντες κοινωνούς των παραγόμενων πολιτικών, η ΕΑΚ κάλεσε όλους τους φορείς και πολίτες να συνεισφέρουν με συγκεκριμένες προτάσεις, απαντώντας σε σχετικά ερωτήματα κατανεμημένα σε 5 θεματικές περιοχές:

1. Στρατηγικές Κατευθύνσεις και Διακυβέρνηση
2. Νομοθεσία, Ρυθμιστικά Μέτρα και Συμμόρφωση
3. Τεχνολογικές Προκλήσεις και Καινοτομία
4. Δεξιότητες, Εκπαίδευση και Ανθρώπινο Δυναμικό
5. Συνεργασίες, Οικοσύστημα και Διεθνής Διάσταση

Η εφαρμοζόμενη διαδικασία επέτρεψε τη συμμετοχή φορέων τόσο από το δημόσιο όσο και από τον ιδιωτικό τομέα, καθώς και από την ακαδημαϊκή/ερευνητική κοινότητα (Γράφημα 1) με τους κλάδους δραστηριότητας να καλύπτουν ένα ευρύ φάσμα του εγχώριου οικοσυστήματος κυβερνοασφάλειας.

Ενδεικτικά στη δημόσια διαβούλευση συμμετείχαν: δημόσιοι φορείς κεντρικής διοίκησης/αποκεντρωμένες διοικήσεις, δήμοι, δικαστικές/αστυνομικές αρχές, τεχνολογικές εταιρείες, πανεπιστήμια/ερευνητικά κέντρα, εταιρείες από τον κλάδο των τηλεπικοινωνίων, μεταφορών, ενέργειας και υγείας. Πέραν των άλλων, το γεγονός αυτό διασφαλίζει τη συμμετοχή και δέσμευση του εθνικού οικοσυστήματος κυβερνοασφάλειας στην υλοποίηση των εθνικών στρατηγικών στόχων, ως προϋπόθεση για την εφαρμογή μιας ολιστικής προσέγγισης στη διακυβέρνηση της δημόσιας πολιτικής κυβερνοασφάλειας (whole of government and whole of society approach).



Εικόνα 6: Τομείς Δραστηριότητας στη Δημόσια Διαβούλευση ΕΣΚ 2026-2030

Βασικοί Άξονες Προτάσεων Δημόσιας Διαβούλευσης

1. Δημιουργία ενιαίου, ολοκληρωμένου συστήματος διακυβέρνησης κυβερνοασφάλειας

Οι συμμετέχοντες ζητούν ξεκάθαρους ρόλους, λιγότερη πολυδιάσπαση και ισχυρό κεντρικό συντονισμό μεταξύ όλων των δημόσιων φορέων.

2. Ενίσχυση της Εθνικής Αρχής Κυβερνοασφάλειας με διακριτό ρόλο, τεχνικές υποδομές και εξειδικευμένο ανθρώπινο δυναμικό

Η Αρχή πρέπει να έχει επιχειρησιακή αυτονομία, σύγχρονες υποδομές και επαρκή στελέχωση.

3. Εθνικό πρόγραμμα ενίσχυσης ΜΜΕ με κλιμακωτή υποστήριξη, επιδοτήσεις και εργαλεία ωριμότητας

Περιλαμβάνει risk-based υποστήριξη, maturity models, πρόσβαση σε εκπαιδεύσεις και επιχορήγηση cyber insurance.

4. Συστηματική ανάπτυξη δεξιοτήτων και πιστοποιημένων προγραμμάτων εκπαίδευσης για όλο το οικοσύστημα

Εμφανίζεται καθολικά ως ανάγκη – από στελέχη δημόσιου τομέα έως ΜΜΕ και κρίσιμες υποδομές.

5. Θεσμοθέτηση και υιοθέτηση ενιαίων πλαισίων διαχείρισης κινδύνου και ελάχιστων απαιτήσεων κυβερνοασφάλειας

Ιδιαίτερα για κρίσιμες υποδομές, δημόσιους φορείς και παρόχους υπηρεσιών.

6. Δημιουργία εθνικής υποδομής Threat Intelligence & Early Warning

Με διαλειτουργικότητα, συνεργασία με το EL-SOC/G-SOC και συμμετοχή σε ευρωπαϊκά δίκτυα.

7. Σημαντική ενίσχυση υποδομών και συστημάτων κυβερνοασφάλειας σε δημόσιους φορείς και κρίσιμες υποδομές

Αναβάθμιση legacy συστημάτων, δικτύων, διαδικασιών και ευπαθειών σε όλο τον δημόσιο τομέα.

8. Ενίσχυση διεθνούς και ευρωπαϊκής συνεργασίας

Συμμετοχή σε pilots, testbeds, research projects, ανταλλαγή πληροφοριών και ενεργή εμπλοκή σε διεθνείς οργανισμούς.

9. Εκστρατείες ευαισθητοποίησης και καλλιέργεια εθνικής κουλτούρας κυβερνοασφάλειας

Ευρεία εκπαίδευση πολιτών, μαθητών, επιχειρήσεων και δημοσίων υπαλλήλων.

10. Δημιουργία πρακτικών εργαλείων και οδηγών εφαρμογής για φορείς και οργανισμούς

Πρότυπα, templates, οδηγοί συμμόρφωσης, checklists και frameworks για εύκολη υλοποίηση της στρατηγικής στην πράξη.

Συμμετοχή βασικών εμπλεκόμενων φορέων στο Σχέδιο Δράσης

Σε συνέχεια της ολοκλήρωσης της Δημόσιας Διαβούλευσης για τη νέα Εθνική Στρατηγική Κυβερνοασφάλειας (ΕΣΚ) 2026–2030, ζητήθηκε η συνδρομή των βασικών εμπλεκόμενων φορέων στην υλοποίηση της ΕΣΚ για τον σχολιασμό των προτεινόμενων δράσεων του Σχεδίου Δράσης, καθώς και για την υποβολή νέων προτάσεων ανά τομέα αρμοδιότητας. Η ενεργός συμμετοχή τους κρίθηκε καθοριστική για τη διαμόρφωση ενός ολοκληρωμένου και εφαρμόσιμου στρατηγικού πλαισίου.

Στο πλαίσιο αυτό, στόχος του Σχεδίου Δράσης είναι η αποτύπωση συγκεκριμένων πρωτοβουλιών και δραστηριοτήτων που οι συναρμόδιοι φορείς προγραμματίζουν να υλοποιήσουν στο πλαίσιο των θεσμικών τους αρμοδιοτήτων, τόσο σε εθνικό όσο και σε τομεακό επίπεδο. Οι προτεινόμενες δράσεις αφορούν πολιτικές, ρυθμιστικές και επιχειρησιακές παρεμβάσεις στους τομείς ευθύνης κάθε φορέα.

Η κοινή αυτή διαδικασία συμβάλλει στη διαμόρφωση κοινής αντίληψης σχετικά με τον πρακτικό τρόπο υλοποίησης της ΕΣΚ και ενισχύει τη συνοχή και την αποτελεσματικότητα των επιμέρους παρεμβάσεων, προάγοντας παράλληλα μια ενιαία προσέγγιση στη διακυβέρνηση της κυβερνοασφάλειας σε εθνικό επίπεδο.

3. Βασικοί Εμπλεκόμενοι Φορείς

Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ)

Η Εθνική Αρχή Κυβερνοασφάλειας εποπτεύεται από τον Υπουργό Ψηφιακής Διακυβέρνησης και αποτελεί την ενιαία και λειτουργική δομή, που αναλαμβάνει το συντονισμό για την υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας, στο πλαίσιο των εθνικών αναγκών και των ενωσιακών δεσμεύσεων της χώρας. Βασική αποστολή της ΕΑΚ αποτελεί η αποτελεσματική πρόληψη και διαχείριση κυβερνοεπιθέσεων, καθώς και η ανάπτυξη του οικοσυστήματος κυβερνοασφάλειας στην Ελλάδα. Είναι επιφορτισμένη με τη συνολική διαχείριση της εθνικής στρατηγικής κυβερνοασφάλειας αποτελώντας τον κεντρικό εθνικό φορέα (lead agency) για τη διαμόρφωση και αποτελεσματική υλοποίηση της εθνικής πολιτικής και της διακυβέρνησης της κυβερνοασφάλειας, ως μιας διακριτής και εν πολλοίς οριζόντιας δημόσιας πολιτικής, η οποία διατρέχει πληθώρα άλλων δημόσιων πολιτικών.

Η ΕΑΚ αναπτύσσει επαρκή δράση στο σύνολο των βασικών πυλώνων που χαρακτηρίζουν την κυβερνοασφάλεια, ήτοι:

- Στρατηγική διοίκηση και διακυβέρνηση, η οποία καλύπτει όλο τον «κύκλο ζωής» της εθνικής στρατηγικής κυβερνοασφάλειας, ενισχύοντας στον πυρήνα του το μοντέλο διακυβέρνησης και διασφαλίζοντας τον αναγκαίο συντονισμό για την αναγνώριση και το μετριασμό των κινδύνων στον κυβερνοχώρο σε εθνικό επίπεδο.
- Επιχειρησιακές λειτουργίες, οι οποίες διασφαλίζουν την αποτελεσματική διαχείριση περιστατικών μεγάλης κλίμακας και κρίσεων στον κυβερνοχώρο, μέσω συγκεκριμένων δράσεων που ενισχύουν το επίπεδο κυβερνοασφάλειας σε όλα τα επίπεδα και τους τομείς της οικονομικής και κοινωνικής ζωής, στη δημόσια διοίκηση, καθώς και εν γένει στο σύνολο της ελληνικής κοινωνίας.

- Τεχνικές λειτουργίες, οι οποίες διασφαλίζουν τη συμπερίληψη των νέων τεχνολογιών και εργαλείων, που απαιτούνται για την επίτευξη των εθνικών στρατηγικών στόχων.
- Πυλώνας εποπτικών καθηκόντων, καθώς και ρύθμισης στον τομέα της κυβερνοασφάλειας, προκειμένου να διασφαλίζεται η κανονιστική συμμόρφωση των οργανισμών και πρωτίστως των κρίσιμων υποδομών της χώρας προς τις απαιτήσεις του ευρωπαϊκού και εθνικού νομοθετικού πλαισίου στον νευραλγικό τομέα της κυβερνοασφάλειας.

Ο ρόλος της ΕΑΚ στο εθνικό οικοσύστημα κυβερνοασφάλειας, είναι πολυδιάστατος και προσδιορίζεται από την εθνική και ενωσιακή νομοθεσία. Επιτελεί τις εξής κυρίως λειτουργίες:

- Της αρμόδιας εθνικής αρχής υπεύθυνης για την κυβερνοασφάλεια, της αρμόδιας εθνικής αρχής εποπτείας και ελέγχου, του ενιαίου σημείου επαφής της Ελλάδας και της εθνικής αρχής διαχείρισης κρίσεων στον κυβερνοχώρο σύμφωνα με την Οδηγία NIS2.
- Είναι το Εθνικό Κέντρο Συντονισμού και η Εθνική Αρχή Πιστοποίησης στον τομέα της Κυβερνοασφάλειας σύμφωνα με τον Κανονισμό 2019/881/ΕΕ (CSA).
- Είναι το αρμόδιο εθνικό CSIRT για το σύνολο των τομέων του ν. 5160/2024, καθώς και το συντονιστικό CSIRT, όπου λειτουργεί σε τομεακό επίπεδο άλλο αρμόδιο CSIRT.
- Είναι αρμόδιος φορέας για την έκδοση ή εισήγηση του συνόλου της νομοθεσίας και των συναφών ρυθμίσεων στον τομέα της κυβερνοασφάλειας.
- Είναι αρμόδια για τη λειτουργία του Ενοποιημένου Κέντρου Αναφοράς Κυβερνοασφάλειας (Ενοποιημένο Security Operation Center - SOC), το οποίο ως σκοπό έχει την ανάπτυξη, υποστήριξη και ενδυνάμωση των ικανοτήτων σε εθνικό επίπεδο για την έγκαιρη ανίχνευση και αντιμετώπιση κυβερνοαπειλών σε όλη την Επικράτεια, αποτελώντας ταυτόχρονα το κεντρικό σημείο του Εθνικού Δικτύου SOC.

Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό CERT[22] (Ε.Υ.Π.)

Σύμφωνα με τον ν. 5160/2024 (Α' 195) ειδικά για τους Φορείς κεντρικής κυβέρνησης, ΟΤΑ Α' και Β' βαθμού ως αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (CSIRT) ορίζεται η Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT) της Διεύθυνσης Κυβερνοχώρου της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.), ασκώντας όλες τις σχετικές αρμοδιότητες, με την Εθνική Αρχή Κυβερνοασφάλειας να επιτελεί συντονιστικό ρόλο.

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό CERT είναι αρμόδια για την αντιμετώπιση και την προστασία κυρίως του Δημόσιου τομέα και των κρίσιμων υποδομών, όπως ορίζεται στην παρ. 8 του άρθρου 4 του ν. 3649/2008 (Α΄ 39). Για την εκπλήρωση της αποστολής της, ασκεί τις αρμοδιότητες της Εθνικής Αρχής Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και μεριμνά για την πρόληψη και τη στατική και ενεργητική αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής, σύμφωνα με σχετικές διατάξεις του π.δ. 325/2003 (Α΄ 273). Ακολούθως, με το π.δ. 17/2024 (Α'47)

[22] Βλ. https://www.nis.gr/downloads/national-cert/RFC2350-GR.pdf (προσβάσιμο στις 30-06-2025)

κατοχυρώθηκε η αρμοδιότητα της Διεύθυνσης Κυβερνοχώρου της ΕΥΠ ως Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT).

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - Εθνικό CERT συνεργάζεται με άλλα CSIRT, υπηρεσίες του Δημόσιου τομέα, καθώς και εθνικούς και διεθνείς φορείς, αρμόδιους για θέματα Κυβερνοασφάλειας. Επιπρόσθετα, η ΕΥΠ αποτελεί Τεχνικής Φύσεως Αρχή Ασφαλείας Πληροφοριών (INFOSEC), Εθνική Αρχή «CRYPTO», Εθνική Αρχή «TEMPEST» και μετέχει στην Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας του ν. 5002/2022 (Α' 228).

Επιπλέον, η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT) συνεργάζεται στενά με τις συναρμόδιες εθνικές αρχές και φορείς, ανάλογα με τη φύση και τη σοβαρότητα ενός περιστατικού κυβερνοασφάλειας. Ειδικότερα, συνεργάζεται:

- με την Κυβέρνηση, την Εθνική Αρχή Κυβερνοασφάλειας, καθώς και λοιπές αρμόδιες υπηρεσίες για ζητήματα εθνικής σημασίας, σχετικά με την ασφάλεια κυβερνητικών ή κρίσιμων υποδομών,
- με τη Διεύθυνση Δίωξης Κυβερνοεγκλήματος της Ελληνικής Αστυνομίας για περιπτώσεις ύποπτης εγκληματικής δραστηριότητας,
- με το αρμόδιο CSIRT του ΓΕΕΘΑ.

Πέραν της επιχειρησιακής ανταπόκρισης, το Εθνικό CERT διαδραματίζει σημαντικό ρόλο στην πρόληψη και ευαισθητοποίηση της κοινότητας κυβερνοασφάλειας. Αποτελεί τον αρμόδιο φορέα λειτουργίας του κυβερνητικού SOC (Security Operations Center) το οποίο εντάσσεται στο Εθνικό Δίκτυο SOC και εκδίδει προειδοποιήσεις, ανακοινώσεις και τεχνικές οδηγίες για αναδυόμενες απειλές στον τομέα αρμοδιότητάς του, προτείνει μέτρα πρόληψης και βέλτιστες πρακτικές, αξιολογεί τρωτότητες σε πληροφοριακά συστήματα και διεξάγει αντίστοιχες δράσεις εκπαίδευσης. Εκπρόσωπος της Διεύθυνσης Κυβερνοχώρου μετέχει, επίσης, στην Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας του ν. 5002/2022 (Α' 228).

Διεύθυνση Κυβερνοάμυνας (ΔΙΚΥΒ) του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ)

Η Διεύθυνση Κυβερνοάμυνας (ΔΙΚΥΒ) του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ) είναι αρμόδια για την ενίσχυση της Κυβερνοασφάλειας και προστασίας των Ενόπλων Δυνάμεων.

Με το ν. 5110/2024 (Α' 75) συστήνεται Κοινό Σώμα Πληροφορικής, με αποστολή, μεταξύ άλλων, την παροχή υποστήριξης στις μονάδες των Ενόπλων Δυνάμεων σε θέματα πληροφορικής, την αποτροπή κυβερνοαπειλών στον τομέα της Εθνικής Άμυνας, την ενίσχυση της κυβερνοασφάλειας, τον εντοπισμό και αντιμετώπιση κυβερνοεπιθέσεων, την ανάπτυξη, διαχείριση και ασφάλεια των τοπικών δικτύων πληροφορικής, καθώς και την έρευνα, ανάπτυξη και αξιοποίηση αναδυόμενων και ανατρεπτικών τεχνολογιών συμπεριλαμβανομένων των κβαντικών, της τεχνητής νοημοσύνης, των μεγάλων δεδομένων, της ρομποτικής, τεχνικές εξόρυξης δεδομένων (data-mining) και τα αυτόνομα συστήματα.

Σύμφωνα με το ν. 5160/2024, η αρμόδια για θέματα κυβερνοάμυνας οργανική μονάδα του Γενικού Επιτελείου Εθνικής Άμυνας ορίζεται ως ομάδα απόκρισης για συμβάντα που αφορούν στην ασφάλεια υπολογιστών (CSIRT) και υποστηρίζει μεταβατικά την CSIRT της Εθνικής Αρχής Κυβερνοασφάλειας.

Εκπρόσωπος της ΔΙΚΥΒ μετέχει, επίσης, στην Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας του ν. 5002/2022 (Α' 228).

Διεύθυνση Δίωξης Κυβερνοεγκλήματος (ΕΛ.ΑΣ.)

Η Διεύθυνση Δίωξης Κυβερνοεγκλήματος (Δι.Δι.Κ.), με έδρα την Αττική, καθώς και η Υποδιεύθυνση Δίωξης Κυβερνοεγκλήματος Βορείου Ελλάδας (Υ.Δι.Κ.Β.Ε.), με έδρα τη Θεσσαλονίκη, λειτουργούν σύμφωνα με τις διατάξεις του ν. 5187/2025 (Α΄ 48). Η Δι.Δι.Κ. αποτελεί τον βασικό επιχειρησιακό μηχανισμό της Ελληνικής Αστυνομίας για την αντιμετώπιση των εγκλημάτων που τελούνται στον κυβερνοχώρο.

Η αποστολή της Δι.Δι.Κ. περιλαμβάνει τη διερεύνηση, ανακάλυψη και εξιχνίαση αμιγώς υποθέσεων κυβερνοεγκλήματος, για τις οποίες απαιτείται εξειδικευμένη τεχνική ή ψηφιακή έρευνα. Η Δι.Δι.Κ. χαρακτηρίζεται ως επιχειρησιακή κεντρική υπηρεσία (Ειδική Υπηρεσία Ασφάλειας), η οποία εποπτεύεται, συντονίζεται και ελέγχεται απευθείας από τον Αρχηγό της Ελληνικής Αστυνομίας.

Για την αποτελεσματική εκπλήρωση της αποστολής της, η Δι.Δι.Κ. συνεργάζεται με λοιπές αρμόδιες υπηρεσίες της Ελληνικής Αστυνομίας, με άλλες αρμόδιες αρχές και φορείς της χώρας, καθώς και με αντίστοιχες υπηρεσίες, οργανισμούς και φορείς άλλων κρατών και κρατών-μελών της Ευρωπαϊκής Ένωσης, στο πλαίσιο των ισχυουσών διατάξεων και των σχετικών διεθνών συμφωνιών και συμβάσεων. Παράλληλα, η Διεύθυνση συμμετέχει στην Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας του ν. 5002/2022 (Α' 228), συμβάλλοντας στον εθνικό σχεδιασμό και στον συντονισμό δράσεων για την ενίσχυση της κυβερνοασφάλειας στη χώρα.

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) αποτελεί ανεξάρτητη διοικητική αρχή με συνταγματικά κατοχυρωμένο ρόλο και αποστολή την προστασία των πολιτών από την αθέμιτη ή παράνομη επεξεργασία προσωπικών δεδομένων.
Βασικός της σκοπός είναι η διασφάλιση του σεβασμού της ιδιωτικής ζωής και των θεμελιωδών δικαιωμάτων των φυσικών προσώπων, καθώς και η προώθηση της ασφαλούς και ορθής χρήσης των δεδομένων προσωπικού χαρακτήρα, στο πλαίσιο της ψηφιακής οικονομίας και κοινωνίας.

Η Αρχή παρακολουθεί και εποπτεύει την εφαρμογή του ευρωπαϊκού και εθνικού πλαισίου για την προστασία των δεδομένων, όπως του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), συνεργαζόμενη με τις αντίστοιχες αρχές των κρατών μελών και τα θεσμικά όργανα της Ευρωπαϊκής Ένωσης, προκειμένου να διασφαλίζεται η συνεπής και ενιαία εφαρμογή των κανόνων σε ευρωπαϊκό επίπεδο.

Παράλληλα, η Αρχή:

- Ενισχύει την ενημέρωση και την ευαισθητοποίηση πολιτών, οργανισμών και επιχειρήσεων σχετικά με τα δικαιώματα και τις υποχρεώσεις που απορρέουν από το ισχύον πλαίσιο προστασίας δεδομένων.
- Παρέχει κατευθύνσεις και γνωμοδοτήσεις προς τη δημόσια διοίκηση και άλλους φορείς για ζητήματα που σχετίζονται με την προστασία προσωπικών δεδομένων.

- Εξετάζει καταγγελίες πολιτών και διενεργεί ελέγχους για την τήρηση της νομοθεσίας.
- Συμβάλλει στη διαμόρφωση πολιτικών και καλών πρακτικών για την ενίσχυση της εμπιστοσύνης στην ψηφιακή διακυβέρνηση.

Μέσα από τις αρμοδιότητες και τις δράσεις της, η ΑΠΔΠΧ αποτελεί κρίσιμο θεσμό για την προστασία της ιδιωτικότητας, την ενίσχυση της λογοδοσίας και τη διασφάλιση της εμπιστοσύνης πολιτών και οργανισμών στη χρήση των ψηφιακών τεχνολογιών.

Μεταξύ της ΑΠΔΠΧ και της ΕΑΚ έχει υπογραφεί Μνημόνιο Συνεργασίας[23], με αντικείμενο την από κοινού δέσμευση για συνεκτική και συντονισμένη δράση, προς όφελος α) της ενίσχυσης της εμπιστοσύνης των πολιτών στις ψηφιακές υπηρεσίες, β) της ασφαλούς λειτουργίας κρίσιμων ψηφιακών υποδομών της χώρας, γ) της προστασίας των δικαιωμάτων των πολιτών και δ) της ενίσχυσης της ψηφιακής ασφάλειας και της καινοτομίας. Στο πλαίσιο αυτό εδραιώνεται η συνεργασία των δύο Αρχών σε θέματα κοινού ενδιαφέροντος, τη διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων και κυβερνοεπιθέσεων με συντονισμένο τρόπο, καθώς και τη διατύπωση κοινών συστάσεων και κατευθυντήριων γραμμών για φορείς του δημόσιου και ιδιωτικού τομέα.

Για την επίτευξη των σκοπών του Μνημονίου Συνεργασίας λειτουργεί ειδική επιτροπή, αποτελούμενη από ανώτερα στελέχη των δύο αρχών, τα οποία επωμίζονται να λειτουργούν συντονισμένα παρακολουθώντας την πρόοδο της συνεργασίας.

Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)[24] είναι Ανεξάρτητη Αρχή με διοικητική και οικονομική αυτοτέλεια. Αποτελεί την Εθνική Ρυθμιστική Αρχή σε θέματα παροχής υπηρεσιών/δικτύων ηλεκτρονικών επικοινωνιών, καθώς και ταχυδρομικών υπηρεσιών και άλλων συναφών υπηρεσιών. Επίσης, έχει τον ρόλο του Εθνικού Συντονιστή Ψηφιακών Υπηρεσιών.

Η ΕΕΤΤ ρυθμίζει, εποπτεύει και ελέγχει α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται ιδίως οι επιχειρήσεις/πάροχοι σταθερής ή/και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και Διαδικτύου, β) τη χρήση του φάσματος ραδιοσυχνοτήτων, έχοντας, μεταξύ άλλων, αρμοδιότητα για τη χορήγηση, την ανάκληση ή τον περιορισμό των δικαιωμάτων χρήσης ραδιοσυχνοτήτων και την αδειοδότηση κατασκευών κεραιών, καθώς και για θέματα που αφορούν στις προϋποθέσεις διάθεσης στην αγορά και χρήσης συσκευών ραδιοεξοπλισμού και γ) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι επιχειρήσεις παροχής ταχυδρομικών υπηρεσιών ασκώντας αρμοδιότητες επιτροπής ανταγωνισμού και διαθέτοντας όλες τις εξουσίες και τα δικαιώματα ελέγχου της, κατά την εφαρμογή της εθνικής και ενωσιακής νομοθεσίας του ελεύθερου ανταγωνισμού στις παραπάνω αγορές.

[23] Βλ.https://lawnet.gr/law-news/ellada/mnimonio-synergasias-metaxy-tis-archis-prostasias-dedomenon-kai-tis-ethnikis-archis-kyvernoasfaleias/ https://cyber.gov.gr/ypografi-mnimonioy-synergasias-metaxy-tis-archis-prostasias-dedomenon-kai-tis-ethnikis-archis-kyvernoasfaleias/ (προσβάσιμο στις 30-06-2025)

[24] Βλ. https://www.eett.gr/eett/schetika-me-tin-eett/poia-einai-i-eett/ (προσβάσιμο στις 30-06-2025)

Υπό αυτό το πρίσμα, εξασφαλίζει την ομαλή λειτουργία των αγορών, αντιμετωπίζοντας αποτελεσματικά τους κινδύνους στρέβλωσης του ανταγωνισμού και προασπίζοντας τα δικαιώματα των χρηστών.

Έχοντας τον ρόλο του Εθνικού Συντονιστή Ψηφιακών Υπηρεσιών, εφαρμόζει την Πράξη για τις Ψηφιακές Υπηρεσίες (DSA) στην Ελλάδα και εποπτεύει την ορθή εφαρμογή της. Επίσης, διασφαλίζει τον συντονισμό σε εθνικό επίπεδο και συμβάλλει στην αποτελεσματική και συνεπή εφαρμογή της Πράξης σε ευρωπαϊκό επίπεδο.

Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.)

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών[25] έχει ως σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών.

Με το άρθρο 1 του ν. 3115/2003 συστάθηκε, κατά την παράγραφο 2 του άρθρου 19 Συντ., η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) με σκοπούς α) την προστασία του απορρήτου των επιστολών και β) της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και γ) της ασφάλειας των δικτύων και πληροφοριών. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο.

Η ΑΔΑΕ είναι Ανεξάρτητη Αρχή που απολαύει διοικητικής αυτοτέλειας και οι αποφάσεις της κοινοποιούνται με μέριμνά της στον Υπουργό Δικαιοσύνης, ενώ στο τέλος κάθε έτους υποβάλλει Έκθεση πεπραγμένων στον Πρόεδρο της Βουλής, στον Υπουργό Δικαιοσύνης και στους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή και στο Ευρωπαϊκό Κοινοβούλιο. Η ΑΔΑΕ υπόκειται σε κοινοβουλευτικό έλεγχο κατά τον τρόπο και τη διαδικασία που κάθε φορά προβλέπεται από τον Κανονισμό της Βουλής.

Πέραν της συνταγματικής της αποστολής αναφορικά με τη διασφάλιση του απορρήτου των επικοινωνιών, η ΑΔΑΕ, σύμφωνα με το άρθρο 29 παρ.4 του ν. 5160/2024, ορίστηκε ως τομεακό σημείο επαφής και συνεργασίας σε εθνικό επίπεδο (NSFP) με την Εθνική Αρχή Κυβερνοασφάλειας, αναφορικά με τους παρόχους δημόσιων δικτύων ηλεκτρονικών επικοινωνιών ή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών. Επίσης, σύμφωνα με το άρθρο 29 παρ.1 του ν. 5160/2024, η ΑΔΑΕ δύναται να θεσπίζει κανονιστικό πλαίσιο σχετικά με τα ενισχυμένα μέτρα κυβερνοασφάλειας στον τομέα των ηλεκτρονικών επικοινωνιών.

Στο ανωτέρω πλαίσιο του ρόλου της, η ΑΔΑΕ είναι επιφορτισμένη με την κατάρτιση του γενικότερου κανονιστικού πλαισίου στα θέματα των αρμοδιοτήτων της (ενδεικτικά αναφέρεται ο Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών, Απόφ. 304/2025, ΦΕΚ 4268/Β/7.8.2025), στα οποία συμπεριλαμβάνεται, επιπροσθέτως, ο έλεγχος της τήρησης των όρων και της διαδικασίας στην περίπτωση άρσης του απορρήτου των επικοινωνιών και η εξασφάλιση της μέγιστης δυνατής διαθεσιμότητας και της αδιάλειπτης πρόσβασης σε υπηρεσίες έκτακτης ανάγκης, σε

[25] Βλ. https://adae.gov.gr/adae/sxetika-me-tin-adae (προσβάσιμο στις 30-06-2025)

περιπτώσεις καταστροφικής βλάβης του δικτύου και σε περιπτώσεις ανωτέρας βίας. Επίσης, η ΑΔΑΕ πραγματοποιεί τακτικούς και έκτακτους ελέγχους στους εποπτευόμενους φορείς, εξετάζει καταγγελίες και περιστατικά ασφαλείας, διενεργεί ακροάσεις των εποπτευόμενων φορέων και επιβάλει κυρώσεις, όπου απαιτείται.

Ρυθμιστική Αρχή Αποβλήτων Ενέργειας και Υδάτων (Ρ.Α.Α.Ε.Υ.)

Η Ρυθμιστική Αρχή Αποβλήτων Ενέργειας και Υδάτων (ΡΑΑΕΥ)[26] ιδρύθηκε ως ανεξάρτητη ρυθμιστική αρχή, η οποία συστήθηκε με το ν. 2773/1999 (Α΄ 286), στο πλαίσιο εναρμόνισης με την Οδηγία 96/92/ΕΚ σχετικά με τους κοινούς κανόνες για την εσωτερική αγορά ηλεκτρικής ενέργειας και μετέπειτα με τις Οδηγίες 2003/54/ΕΚ και 2003/55/ΕΚ, οι οποίες αφορούν τον ηλεκτρισμό και το φυσικό αέριο, με κύρια αρμοδιότητά της να εποπτεύει την εγχώρια αγορά ενέργειας, σε όλους τους τομείς ευθύνης της. Μεταξύ άλλων, λαμβάνει μέτρα και εισηγείται τη λήψη μέτρων προς τους αρμόδιους φορείς της Πολιτείας και για την επίτευξη του στόχου της απελευθέρωσης των αγορών ηλεκτρικής ενέργειας και φυσικού αερίου. Η ΡΑΑΕΥ διαθέτει αυτοτελή νομική προσωπικότητα, καθώς και διοικητική και οικονομική αυτοτέλεια, υπόκειται δε μόνο σε κοινοβουλευτικό και σε δικαστικό έλεγχο (ν. 4001/2011, Α΄ 179).

Ο ρόλος της ΡΑΑΕΥ ως εθνικής ρυθμιστικής αρχής ενέργειας αναβαθμίστηκε από το 2011 (ν. 4001/2011, Α' 179), με την επαύξηση και ενίσχυση των αποφασιστικών αρμοδιοτήτων της σχετικά με τη ρύθμιση των αγορών ηλεκτρικής ενέργειας και φυσικού αερίου, αποτελώντας την εθνική ρυθμιστική αρχή σε θέματα ηλεκτρικής ενέργειας και φυσικού αερίου, σύμφωνα με το ενωσιακό δίκαιο.

Η Αρχή μετονομάστηκε σε Ρυθμιστική Αρχή Αποβλήτων, Ενέργειας και Υδάτων (ΡΑΑΕΥ) με τον ν. 5037/2023 και το αντικείμενό της διευρύνθηκε, περιλαμβάνοντας αρμοδιότητες επί των υπηρεσιών Ύδατος και της διαχείρισης Αστικών Αποβλήτων.

Οι κυριότερες αρμοδιότητες της ΡΑΑΕΥ, σύμφωνα με το νομοθετικό πλαίσιο που διέπει τη λειτουργία της, αφορούν τους κλάδους α) της Ενέργειας, β) των Αποβλήτων, και γ) των Υδάτων. Διαδραματίζει σημαντικό ρόλο και για την κυβερνοασφάλεια των τομέων αυτών, καθώς αποτελεί την υπεύθυνη ρυθμιστική αρχή για την εκτέλεση καθηκόντων που προβλέπονται στον κατ' εξουσιοδότηση Κανονισμό (ΕΕ) 2024/1366 της Επιτροπής αναφορικά με τη θέσπιση κώδικα δικτύου σχετικά με ειδικούς τομεακούς κανόνες για τις πτυχές της κυβερνοασφάλειας στις διασυνοριακές ροές ηλεκτρικής ενέργειας.

Αρχή Πολιτικής Αεροπορίας (Α.Π.Α.)

Η Α.Π.Α. συστάθηκε με τον ν. 4757/2020 (Α΄ 240), έχει ως αρμοδιότητες α) την εισήγηση ως προς τη χάραξη εθνικής στρατηγικής αερομεταφορών, β) τη ρύθμιση και θέσπιση των κανονισμών που εντάσσονται στις αρμοδιότητές της, γ) την άσκηση εποπτείας στη λειτουργία της πολιτικής αεροπορίας, δ) την εφαρμογή του εθνικού και ενωσιακού δικαίου και των οικείων διεθνών συμβάσεων[27].

[26] Βλ. https://www.raaey.gr/energeia/sxetika-me-ti-rae/ (προσβάσιμο στις 30-06-2025)

[27] Βλ. https://hcaa.gov.gr/el/armodiotites (προσβάσιμο στις 30-06-2025)

Αποστολή της Α.Π.Α. είναι η εκτέλεση των καθηκόντων πιστοποίησης, εποπτείας και επιβολής στον τομέα των αερομεταφορών, της αεροναυτιλίας και των αερολιμένων, η εφαρμογή της εθνικής και ενωσιακής νομοθεσίας, καθώς και των διεθνών συμβάσεων στον οικείο τομέα[28].

Με τις διατάξεις της με αριθμ. ΑΠΑ/31639/17.11.2023 (Β' 6692) απόφασης του Εκτελεστικού Συμβουλίου της Α.Π.Α., προβλέφθηκε η σύσταση και λειτουργία Τμήματος Ασφάλειας Κυβερνοχώρου Πολιτικής Αεροπορίας (HCAA/Cyber).

Η Α.Π.Α., κατόπιν υπογραφής σχετικής Κοινής Υπουργικής Απόφασης (ΚΥΑ 1879/2025, Β΄ 3543) μεταξύ του Υπουργού Ψηφιακής Διακυβέρνησης και του Διοικητή της Α.Π.Α., ορίζεται (δια του Τμήματος HCAA/Cyber) ως Τομεακό Σημείο Επαφής και Συνεργασίας σε εθνικό επίπεδο (National Sectorial Focal Point, NSFP) με την Εθνική Αρχή Κυβερνοασφάλειας, με στόχο, μεταξύ άλλων, την ενίσχυση της επιχειρησιακής ετοιμότητας και του συντονισμού στον τομέα των εναέριων μεταφορών, κατά την εφαρμογή του ευρωπαϊκού και εθνικού κανονιστικού πλαισίου για την κυβερνοασφάλεια, όπως το τελευταίο διαμορφώθηκε από τη μεταφορά και την ενσωμάτωση στην εθνική έννομη τάξη της ευρωπαϊκής Οδηγίας NIS2 με τον ν. 5160/2024 (Α΄ 195)[29].

Με τον τρόπο αυτό, διασφαλίζεται η απρόσκοπτη συνεργασία της Εθνικής Αρχής Κυβερνοασφάλειας και της Αρχής Πολιτικής Αεροπορίας για α) την εφαρμογή του νομικού πλαισίου Κυβερνοασφάλειας, β) την απρόσκοπτη ροή πληροφοριών, γ) την ταχεία επικοινωνία και τη συνεργασία των αρμόδιων φορέων με αντικείμενα την αντιμετώπιση κυβερνοαπειλών ή περιστατικών κυβερνοασφάλειας που αφορούν τον οικείο τομέα και δ) την υλοποίηση δράσεων που αποσκοπούν στην υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας.

Επιτροπή Συντονισμού για Θέματα Κυβερνοασφάλειας

Η Επιτροπή Συντονισμού για θέματα Κυβερνοασφάλειας, αποτελεί συλλογικό όργανο με «...αποστολή τον προγραμματισμό, την παρακολούθηση, τον συντονισμό ενεργειών, τις παρεμβάσεις σε ζητήματα που άπτονται της κυβερνοασφάλειας από το αρχικό στάδιο της πρόληψης μέχρι το στάδιο της αποτελεσματικής αντιμετώπισης περιστατικών κυβερνοεπιθέσεων και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο...» (α. 21 του ν.5002/2022, Α΄ 218).

Η Επιτροπή λειτουργεί στην Προεδρία της Κυβέρνησης και υπό την προεδρία του Γενικού Γραμματέα Εθνικής Ασφάλειας της Προεδρίας της Κυβέρνησης. Αποτελεί συντονιστικό όργανο μεταξύ: α) της Εθνικής Αρχής Κυβερνοασφάλειας, β) της Διεύθυνσης Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας, γ) της Διεύθυνσης Κυβερνοχώρου της Ε.Υ.Π. ως ομάδας αντιμετώπισης ηλεκτρονικών επιθέσεων (Εθνικό CERT) και δ) της Ελληνικής Αστυνομίας.

Σε αυτήν μετέχουν εκπρόσωποι α) των παραπάνω φορέων, β) του αρμόδιου για την εποπτεία της ΕΥΠ μέλους της Κυβέρνησης. Κατά περίπτωση, δύναται να καλούνται στις συνεδριάσεις της δημόσιοι

[28] Βλ. https://hcaa.gov.gr/el/apostoli (προσβάσιμο στις 30-06-2025)

[29] Βλ. https://cyber.gov.gr/i-archi-politikis-aeroporias-oristike-os-tomeako-simeio-epafis-kai-synergasias-gia-tis-enaeries-metafores-me-tin-ethniki-archi-kyvernoasfaleias/ (προσβάσιμο στις 30-06-2025)

λειτουργοί και υπάλληλοι, πάσης φύσεως στελέχη που απασχολούνται στο δημόσιο και ιδιώτες εμπειρογνώμονες, χωρίς δικαίωμα ψήφου.

Στις αρμοδιότητες της Επιτροπής περιλαμβάνονται, μεταξύ άλλων, η έγκριση του εθνικού σχεδίου αντιμετώπισης περιστατικών μεγάλης κλίμακας και κρίσεων στον κυβερνοχώρο, η παροχή κατευθύνσεων σε περίπτωση εξαιρετικού συμβάντος που ενέχει στρατηγικό κίνδυνο, καθώς και η εισήγηση προς το Κυβερνητικό Συμβούλιο Εθνικής Ασφάλειας οποιουδήποτε θέματος εμπίπτει στο πεδίο της κυβερνοασφάλειας, ενώ δύναται να λαμβάνει περιοδικές συγκεντρωτικές αναφορές από την ΕΑΚ για την πρόοδο υλοποίησης της Εθνικής Στρατηγικής.

Γενική Γραμματεία Προστασίας Κρίσιμων Οντοτήτων (Γ.Γ.Π.Κ.Ο.) – Υπουργείο Προστασίας του Πολίτη

Σύμφωνα με τον ν. 5236/2025 (Α΄ 175) η Γενική Γραμματεία Προστασίας Κρίσιμων Οντοτήτων (ΓΓΠΚΟ) του Υπουργείου Προστασίας του Πολίτη ορίζεται ως αρμόδια εθνική αρχή και ενιαίο σημείο επαφής με σκοπό την ενίσχυση της ανθεκτικότητας και της φυσικής ασφάλειας των κρίσιμων οντοτήτων, εξαιρουμένης δηλαδή της κυβερνοασφάλειας αυτών. Παράλληλα, διαμορφώνει την Εθνική Στρατηγική για την Ενίσχυση της Ανθεκτικότητας των Κρίσιμων Οντοτήτων, η οποία επικαιροποιείται τουλάχιστον ανά τετραετία. Η Στρατηγική καθορίζει τους στρατηγικούς στόχους και τα μέτρα πολιτικής για την επίτευξη και τη διατήρηση υψηλού επιπέδου ανθεκτικότητας των κρίσιμων οντοτήτων, ως παρόχων βασικών υπηρεσιών που διαδραματίζουν θεμελιώδη ρόλο στη διατήρηση ζωτικών κοινωνικών λειτουργιών και οικονομικών δραστηριοτήτων, έναντι ανθρωπογενών ή φυσικών κινδύνων και απειλών.

Η Γ.Γ.Π.Κ.Ο. του Υπουργείου Προστασίας του Πολίτη προσδιορίζει, τις κρίσιμες οντότητες για τους τομείς και τους υποτομείς που περιλαμβάνονται στο πεδίο εφαρμογής του ν. 5236/2025 (Α’ 175) ενώ προβλέπεται η στενή συνεργασία με την Εθνική Αρχή Κυβερνοασφάλειας σε μια σειρά κρίσιμων θεμάτων, δεδομένου ότι η φυσική ασφάλεια και κυβερνοασφάλεια των κρίσιμων οντοτήτων αποτελούν διακριτά μεν πεδία δραστηριότητας πλην όμως τελούν σε στενή σχέση μεταξύ τους.

Η Γ.Γ.Π.Κ.Ο: α) υποστηρίζει τις κρίσιμες οντότητες στο πεδίο της ενίσχυσης της ανθεκτικότητάς τους, β) συνεργάζεται και ανταλλάσσει πληροφορίες και ορθές πρακτικές με τις κρίσιμες οντότητες των τομέων ευθύνης της και γ) διευκολύνει την οικειοθελή ανταλλαγή πληροφοριών μεταξύ κρίσιμων οντοτήτων σχετικά με ζητήματα φυσικής ασφάλειας, σύμφωνα με την ενωσιακή και την εθνική νομοθεσία.

Επιπλέον, η Γ.Γ.Π.Κ.Ο. για την επίτευξη της αποστολής της διαβουλεύεται και συνεργάζεται με τις αρμόδιες αρχές των λοιπών κρατών μελών της Ευρωπαϊκής Ένωσης.

Τράπεζα της Ελλάδος (ΤτΕ)[30]

Η Τράπεζα της Ελλάδος, η κεντρική τράπεζα της χώρας, αποτελεί ανεξάρτητη αρχή που ασκεί δημόσιο λειτούργημα μεριμνώντας για τη σταθερότητα των τιμών και την εύρυθμη λειτουργία του χρηματοπιστωτικού συστήματος (τραπεζών, ασφαλιστικών εταιριών κ.ά.). Αποτελεί αναπόσπαστο

30 https://www.bankofgreece.gr/

μέλος του Ευρωσυστήματος και συμμετέχει με τις υπόλοιπες εθνικές κεντρικές τράπεζες της Ευρωζώνης και την Ευρωπαϊκή Κεντρική Τράπεζα στη χάραξη της ενιαίας νομισματικής πολιτικής επί του κοινού νομίσματος. Ειδικότερα, στις αρμοδιότητες της ΤτΕ[31] περιλαμβάνεται και η εποπτεία των πιστωτικών ιδρυμάτων που δραστηριοποιούνται στη χώρα, η οποία διεξάγεται σε συνεργασία με την Ευρωπαϊκή Κεντρική Τράπεζα στο πλαίσιο του Ενιαίου Εποπτικού Μηχανισμού και αποσκοπεί στη σταθερότητα και την εύρυθμη λειτουργία του χρηματοπιστωτικού συστήματος. Για το σκοπό αυτό, διεξάγει συνεχή εποπτεία καθώς και επιτόπιες επιθεωρήσεις σε περιοδική ή έκτακτη βάση στα εποπτευόμενα ιδρύματα.

Η Ευρωπαϊκή Ένωση προχώρησε στην έκδοση του Κανονισμού (ΕΕ) 2022/2554 για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα (DORA)[32], με εφαρμογή από 17 Ιανουαρίου 2025. Στοχεύει στο να διασφαλίσει ότι, οι χρηματοοικονομικές οντότητες της ΕΕ που βρίσκονται στο εύρος του Κανονισμού, διαθέτουν ισχυρή ψηφιακή επιχειρησιακή ανθεκτικότητα, ώστε να μπορούν να προλαμβάνουν, να αντιμετωπίζουν και να ανακάμπτουν από περιστατικά Τεχνολογίας, Πληροφορικής και Επικοινωνίας (ΤΠΕ). Επιπλέον, θεσπίζει ενιαίο πλαίσιο κανόνων για τη διαχείριση κινδύνων ΤΠΕ και ενισχύει την εποπτεία κρίσιμων τρίτων παρόχων υπηρεσιών ΤΠΕ.

Η Τράπεζα της Ελλάδος έχει την αρμοδιότητα να εποπτεύει τις χρηματοοικονομικές οντότητες που βρίσκονται στο εύρος του Κανονισμού για τη συμμόρφωση με το ως άνω κανονιστικό πλαίσιο. Σε συνέχεια του ν. 5193/2025, έχει οριστεί ως αρμόδια εποπτική αρχή για την εφαρμογή του DORA στην Ελλάδα, στα πιστωτικά ιδρύματα (σε συνεργασία με τον Ενιαίο Εποπτικό Μηχανισμό), ιδρύματα πληρωμών, ιδρύματα ηλεκτρονικού χρήματος, παρόχους υπηρεσιών πληροφοριών λογαριασμού (AISPs), παρόχους υπηρεσιών κρυπτοστοιχείων (MiCA) και εκδότες ψηφιακών μαρκών, ταμεία επαγγελματικής ασφάλισης, (αντ)ασφαλιστικές επιχειρήσεις, (αντ)ασφαλιστικούς διαμεσολαβητές και στο Ταμείο Παρακαταθηκών και Δανείων.

Η συνεργασία της Τράπεζας της Ελλάδος με εθνικές και διεθνείς αρχές με ανάλογες αρμοδιότητες, ενισχύει την ανταλλαγή πληροφόρησης για την αποτελεσματικότερη κυβερνοανθεκτικότητα του ελληνικού χρηματοπιστωτικού τομέα, προστατεύοντας τις κρίσιμες υποδομές και δεδομένα και συμβάλλοντας στη συνολική σταθερότητα του τραπεζικού συστήματος στην Ελλάδα και στην Ευρώπη. Τέλος, για την εκπλήρωση των υπολοίπων ρόλων[33] της, η Τράπεζα μεριμνά για την «ψηφιακή ανθεκτικότητά» της με τη λήψη συγκεκριμένων τεχνολογικών μέτρων και την εφαρμογή των σχετικών πολιτικών ασφάλειας.

Βασικές και σημαντικές οντότητες

Πρόκειται για τα νομικά πρόσωπα, επιχειρήσεις και οργανισμούς του δημόσιου και ιδιωτικού τομέα, που υπάγονται στο πεδίο εφαρμογής του ν. 5160/2024. Κατηγοριοποιούνται σε «βασικές» και

[31] https://www.bankofgreece.gr/trapeza/rolos-kai-armodiotites

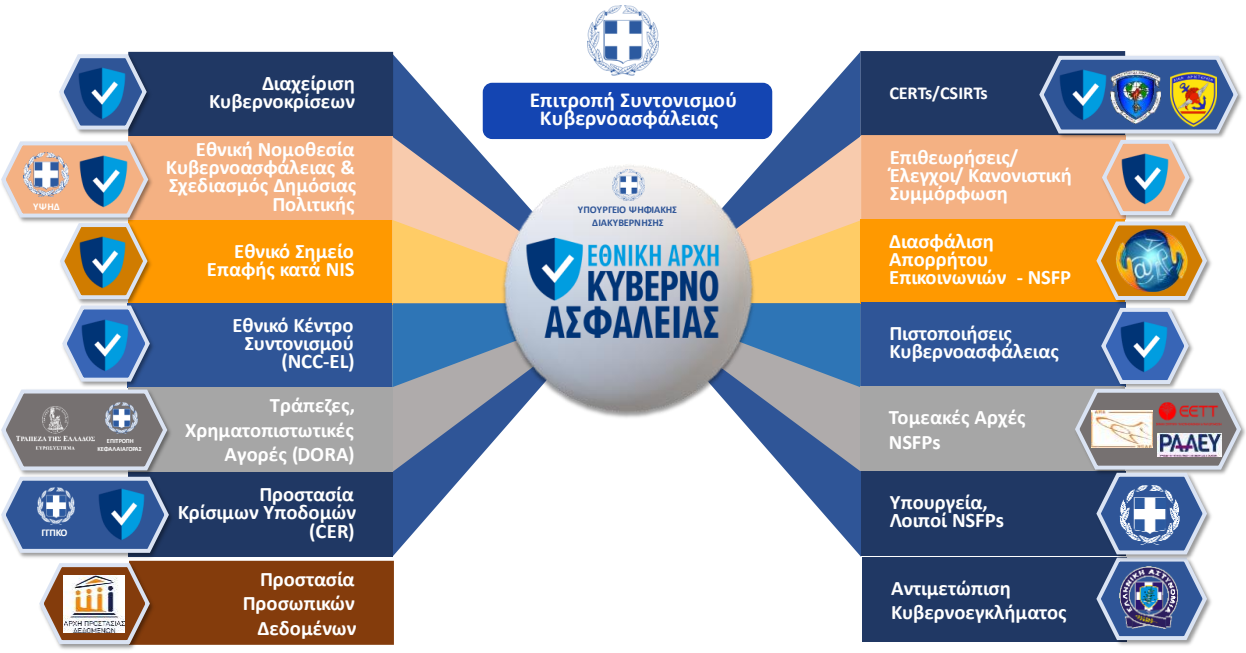
[32] Κανονισμός (ΕΕ) 2022/2554 σχετικά με την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοοικονομικού τομέα

[33] Όπως η επίβλεψη των συστημάτων πληρωμών και διακανονισμού, η έκδοση τραπεζογραμματίων, η πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, η διαχείριση των διαθεσίμων της χώρας, η συναλλαγών για λογαριασμό του Ελληνικού Δημοσίου, κ.α. Βλ. https://www.bankofgreece.gr/trapeza/rolos-kai-armodiotites

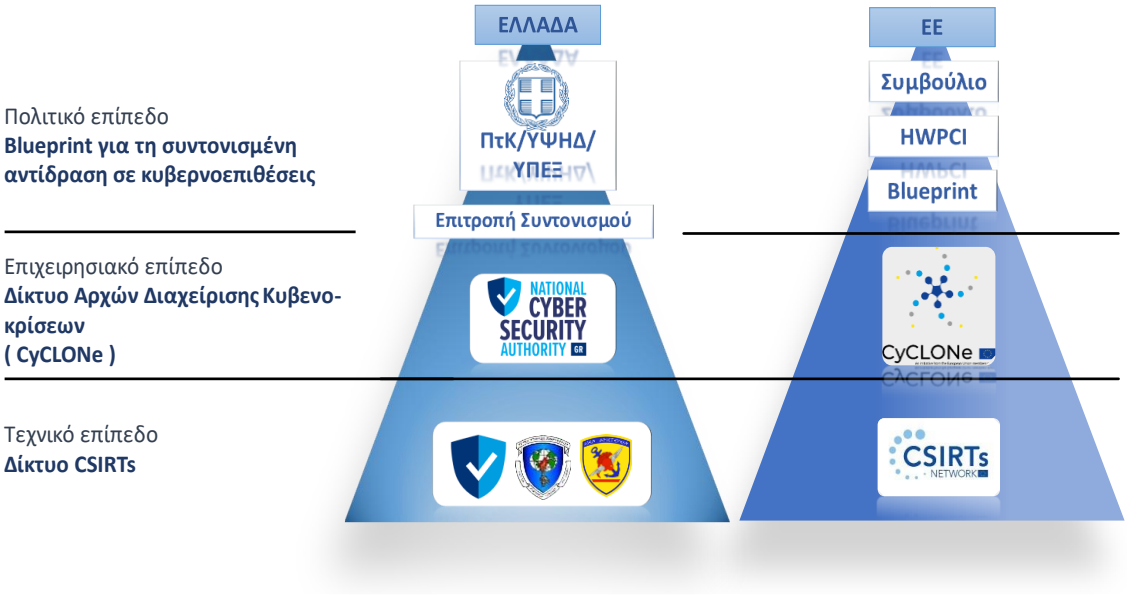
«σημαντικές» οντότητες, ανάλογα με τον τομέα δραστηριότητας και το μέγεθός τους, κατά κανόνα, από μεσαίες επιχειρήσεις και άνω, έχοντας τις αντίστοιχες έννομες υποχρεώσεις. Για τις βασικές και σημαντικές οντότητες η διαχείριση του ρίσκου στον κυβερνοχώρο και η προστασία των ψηφιακών υποδομών τους δεν αποτελεί απλά προϋπόθεση της εύρυθμης λειτουργίας τους, της οικονομικής τους βιωσιμότητας και ενίσχυσης της ανθεκτικότητάς τους. Λόγω της σημασίας τους για την ομαλή κοινωνική και οικονομική ζωή της χώρας, αποτελεί νομική τους υποχρέωση η λήψη μέτρων κυβερνοασφάλειας, τηρώντας κατάλληλη τεκμηρίωση, η διαχείριση των περιστατικών κυβερνοασφάλειας που αντιμετωπίζουν και η αναφορά των περιστατικών αυτών στο αρμόδιο CSIRT, ενώ υπάγονται σε ισχυρό πλαίσιο εποπτείας από την ΕΑΚ.

Σχηματική απεικόνιση εθνικού μοντέλου διακυβέρνησης κυβερνοασφάλειας

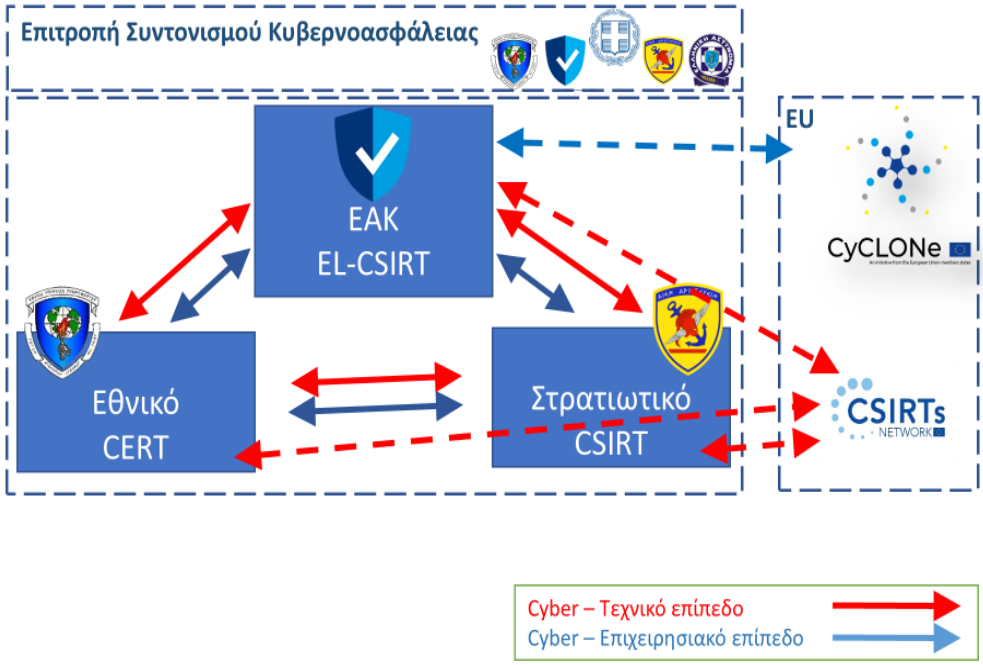
Οι αρμόδιοι φορείς και οι ρόλοι τους στη διακυβέρνηση της δημόσιας πολιτικής κυβερνοασφάλειας, καθώς και για τη διαχείριση κρίσεων και σημαντικών περιστατικών κυβερνοασφάλειας απεικονίζονται ως εξής:



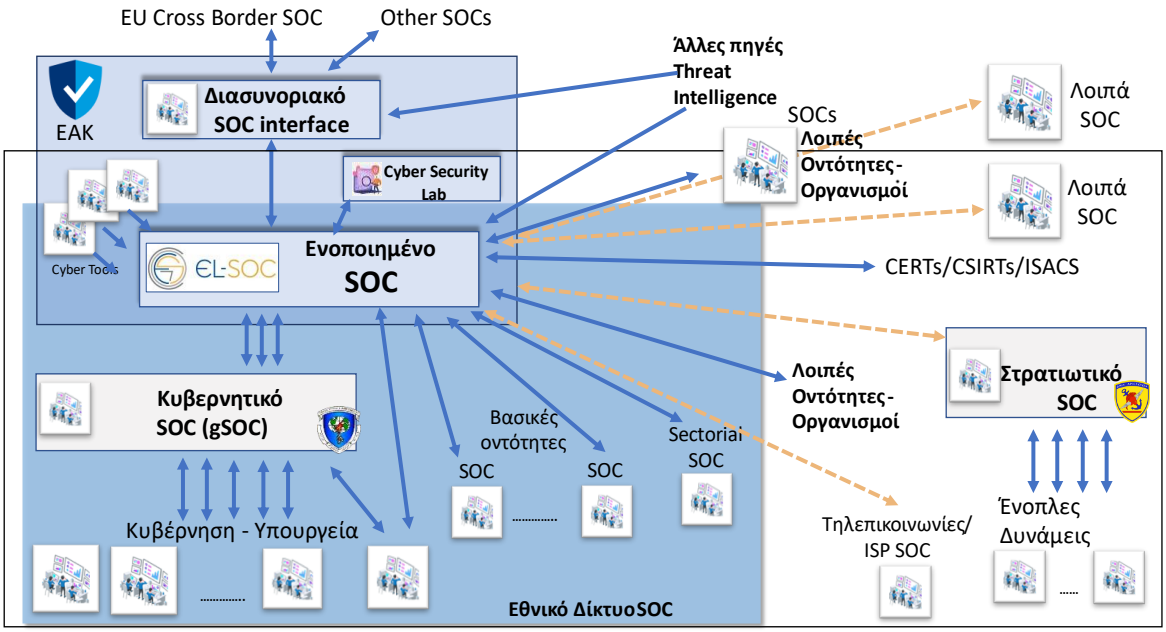
Εικόνα 7: Διακυβέρνηση δημόσιας πολιτικής Κυβερνοασφάλειας



Εικόνα 8: Απόκριση σε σημαντικά περιστατικά και κρίσεις κυβερνοασφάλειας

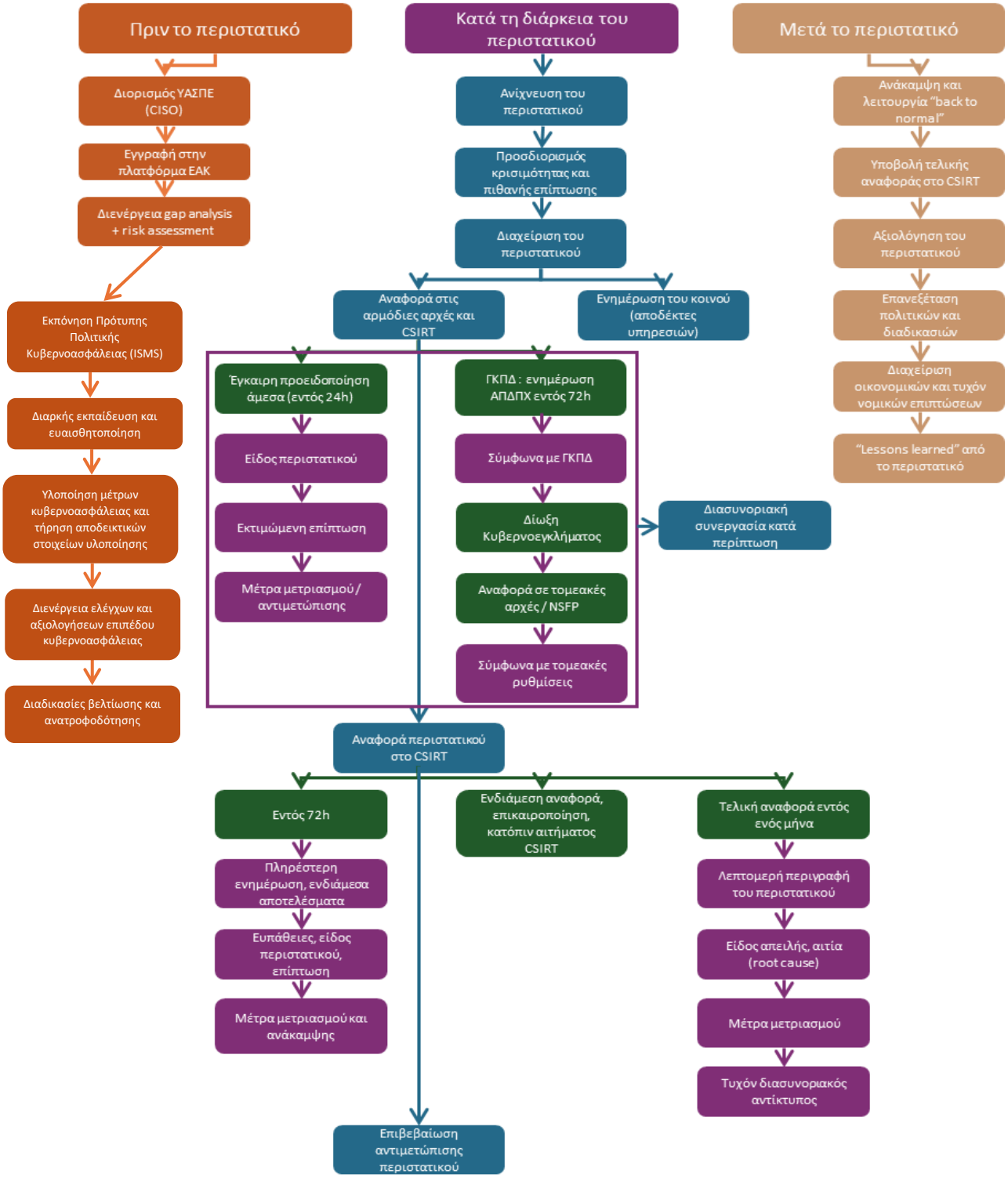


Εικόνα 9: Εθνικός Μηχανισμός Διαχείρισης Περιστατικών και Κρίσεων



Εικόνα 10: Ενοποιημένο SOC ΕΑΚ & Εθνικό Δίκτυο SOC

Δεδομένου ότι την ευθύνη για την κυβερνοασφάλεια κάθε κρίσιμου οργανισμού (βασικές και σημαντικές οντότητες) έχει κατά κύριο λόγο η ανώτατη διοίκησή του, οι υποχρεώσεις αυτές συνοψίζονται διαγραμματικά ως εξής:



Εικόνα 11: Ρόλος και υποχρεώσεις βασικών και σημαντικών οντοτήτων

4. Κρίσιμοι Παράγοντες Επιτυχίας για την Υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026-2030.

4.Α. Συμπεράσματα από την Ανάλυση Περιβάλλοντος και Κρίσιμοι Παράγοντες Επιτυχίας

Η εκπόνηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026–2030 βασίστηκε στη συνδυαστική αξιολόγηση του εσωτερικού και εξωτερικού περιβάλλοντος του εθνικού οικοσυστήματος κυβερνοασφάλειας, μέσω της διενέργειας SWOT (Strengths, Weaknesses, Opportunities and Threats) και PESTL-sec (Political, Economic, Social, Technological, Legal & Security).

Η σύνθεση των αποτελεσμάτων αυτής της ανάλυσης ανέδειξε ότι η πρόκληση για την Ελλάδα δεν έγκειται αποκλειστικά στην αναγνώριση και αντιμετώπιση των κυβερνοαπειλών, αλλά πρωτίστως στην ικανότητα του κράτους και του ευρύτερου οικοσυστήματος να υλοποιήσουν με συνέπεια, ταχύτητα και ανθεκτικότητα μια σύνθετη δημόσια πολιτική οριζόντιου χαρακτήρα.

Τα ευρήματα καταδεικνύουν ότι η χώρα διαθέτει ενισχυμένο θεσμικό πλαίσιο, αυξανόμενη ευρωπαϊκή ενσωμάτωση, σημαντικές δυνατότητες χρηματοδότησης και ένα αναπτυσσόμενο οικοσύστημα συνεργασίας, στοιχεία τα οποία συνιστούν ισχυρή βάση για την εφαρμογή της Στρατηγικής.

Παράλληλα, εντοπίζονται διαρθρωτικές αδυναμίες που αφορούν την οργανωσιακή ωρίμανση, τη διαθεσιμότητα εξειδικευμένων ανθρώπινων πόρων, τον κατακερματισμό δομών και διαδικασιών, καθώς και περιορισμούς στην ταχύτητα υλοποίησης λόγω διοικητικών και δημοσιονομικών παραμέτρων. Οι αδυναμίες αυτές επιτείνονται από ένα εξαιρετικά απαιτητικό εξωτερικό περιβάλλον, το οποίο χαρακτηρίζεται από ραγδαία τεχνολογική η αυξανόμενη γεωπολιτική αστάθεια, εντεινόμενη δραστηριότητα κρατικών και μη κρατικών κακόβουλων δρώντων και συνεχή διεύρυνση της επιφάνειας επίθεσης.

Η στρατηγική σύνθεση των παραπάνω συμπερασμάτων οδήγησε στον προσδιορισμό ιεραρχημένων Κρίσιμων Παραγόντων Επιτυχίας, οι οποίοι αποτελούν αναγκαίες και μη διαπραγματεύσιμες προϋποθέσεις για την αποτελεσματική υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026–2030. Οι παράγοντες αυτοί δεν συνιστούν απλές κατευθύνσεις πολιτικής, αλλά κρίσιμες συνθήκες οι οποίες, εάν δεν πληρωθούν, αυξάνουν σημαντικά τον κίνδυνο αστοχίας κατά την εφαρμογή της Στρατηγικής.

Εικόνα 12: Συνοπτική Απεικόνιση Ανάλυσης SWOT

4.Β. Προϋποθέσεις Επιτυχίας της ΕΣΚ 2026 – 2030 (Critical Success Factors)

1. Σταθερό, συνεκτικό και προσαρμοστικό ρυθμιστικό πλαίσιο

- Η αποτελεσματική εφαρμογή της Στρατηγικής προϋποθέτει ένα ρυθμιστικό πλαίσιο σαφές, εφαρμόσιμο και ικανό να προσαρμόζεται έγκαιρα στις τεχνολογικές και γεωπολιτικές εξελίξεις, διασφαλίζοντας την ασφάλεια δικαίου και τη συμμόρφωση των εμπλεκομένων φορέων, αλλά και την ικανότητα καθοδήγησης της ανθρώπινης συμπεριφοράς.

2. Ικανότητα υλοποίησης και επιχειρησιακή ωριμότητα του εθνικού συστήματος διακυβέρνησης

- Η επιτυχία της Στρατηγικής εξαρτάται από τη σαφή κατανομή ρόλων ανάμεσα στους εμπλεκόμενους φορείς, την ύπαρξη ώριμων διαδικασιών συντονισμού και τη διαρκή επιχειρησιακή ετοιμότητα των αρμόδιων φορέων.

3. Επάρκεια, προσέλκυση και διατήρηση εξειδικευμένων ανθρώπινων πόρων

- Η υλοποίηση της Στρατηγικής προϋποθέτει επαρκές και εξειδικευμένο ανθρώπινο δυναμικό σε συνθήκες δομικού ανταγωνισμού με τον ιδιωτικό τομέα, όπου ο δημόσιος τομέας βρίσκεται εξ ορισμού σε μειονεκτική θέση. Η αντιμετώπιση του περιορισμού αυτού απαιτεί συνδυασμό θεσμικών και οργανωσιακών, καθώς και συνεχή επένδυση στην εκπαίδευση και αναβάθμιση δεξιοτήτων.

4. Προβλέψιμη, επαρκής και στρατηγικά ευθυγραμμισμένη χρηματοδότηση

- Η υλοποίηση των στόχων της Στρατηγικής απαιτεί μια εργοκεντρική προσέγγιση και σταθερή χρηματοδότηση, άμεσα συνδεδεμένη με τις στρατηγικές προτεραιότητες και το Σχέδιο Δράσης, καθώς και τον σχεδιασμό κινήτρων για διενέργεια επενδύσεων κυβερνοασφάλειας από τις οντότητες.

5. Τεχνολογική ετοιμότητα και επένδυση σε ανθεκτικές και διαλειτουργικές υποδομές

- Η αντιμετώπιση του εξελισσόμενου τοπίου απειλών προϋποθέτει συνεχή τεχνολογική αναβάθμιση και υιοθέτηση αρχών ασφάλειας εξ αρχής (security-by-design).

6. Θεσμική αξιοποίηση συνεργασιών και συμπράξεων δημόσιου και ιδιωτικού τομέα

- Η συστηματική αξιοποίηση συνεργασιών με τον ιδιωτικό τομέα, την ακαδημαϊκή κοινότητα και διεθνείς εταίρους ενισχύει την επιχειρησιακή ικανότητα και τη μεταφορά τεχνογνωσίας.

7. Συγκρότηση και ενεργοποίηση μιας συνεκτικής εθνικής κοινότητας κυβερνοασφάλειας

- Η επιτυχία της Στρατηγικής προϋποθέτει ενεργή συνεργασία και ανταλλαγή πληροφοριών μεταξύ όλων των εμπλεκομένων φορέων, ενισχύοντας την εθνική ανθεκτικότητα και την κοινή επίγνωση της κατάστασης.

4.Γ. Ανατροφοδότηση και Παρακολούθηση Υλοποίησης του Σχεδίου Δράσης

Σύστημα διαχείρισης, παρακολούθησης και αξιολόγησης της πορείας υλοποίησης της Εθνικής Στρατηγικής

Ο αποτελεσματικός στρατηγικός σχεδιασμός για την επίτευξη του βέλτιστου επιπέδου ασφάλειας των πληροφοριών στην Ελλάδα, σε συνεργασία με τους βασικούς εμπλεκόμενους φορείς, αποτελεί εθνική προτεραιότητα για τη διασφάλιση ενός υψηλού επιπέδου κυβερνοασφάλειας στη χώρα. Η διαμόρφωση, παρακολούθηση, αξιολόγηση και ανατροφοδότηση της Εθνικής Στρατηγικής από την ΕΑΚ απαιτεί τη διαχείριση όλων των σταδίων του «στρατηγικού κύκλου ζωής» (strategic lifecycle) σε ευθυγράμμιση με τις διεθνείς και ευρωπαϊκές καλές πρακτικές . Δεδομένου ότι πρόκειται για ένα έργο εθνικής εμβέλειας, το οποίο υλοποιείται σε βάθος χρόνου, από περισσότερους εμπλεκόμενους η διαρκής ανατροφοδότηση πρέπει να καταλήγει σε προσαρμογές, ανάλογα με τεκμηριωμένα αποτελέσματα και τις αναδυόμενες προκλήσεις.

Με στόχο την αποτελεσματικότερη υλοποίηση των στρατηγικών προτεραιοτήτων, διαμορφώνεται ένα κατάλληλο πλαίσιο υλοποίησης, υποστηριζόμενο από τα κατάλληλα εργαλεία, το οποίο επιτρέπει:

- Τον καλύτερο χρονοπρογραμματισμό και συντονισμό των δραστηριοτήτων.
- Τη βελτιστοποίηση της αξιοποίησης των διαθέσιμων πόρων.
- Την αποτελεσματικότερη αποτύπωση και αξιολόγηση της πορείας εφαρμογής με βάση κατάλληλα εργαλεία διαχείρισης και δείκτες μέτρησης.
- Την έγκαιρη και τεκμηριωμένη λήψη απόφασης για την ανατροφοδότηση της Εθνικής Στρατηγικής.

Βασικά χαρακτηριστικά του πλαισίου για την αποτελεσματική υλοποίηση και παρακολούθηση της πορείας εφαρμογής

Η υλοποίηση των στρατηγικών στόχων της Εθνικής Στρατηγικής Κυβερνοασφάλειας παρακολουθείται από την Εθνική Αρχή Κυβερνοασφάλειας, με σκοπό την αξιολόγηση και την ανατροφοδότηση της Στρατηγικής. Η διαδικασία αυτή υποστηρίζεται από ένα ολοκληρωμένο σύστημα παρακολούθησης και αξιολόγησης της προόδου εφαρμογής μέσω:

- της ανάπτυξης κατάλληλων δεικτών μέτρησης (KPIs),
- της έκδοσης περιοδικών εκθέσεων (quarterly reporting) και
- της έκδοσης ετήσιας έκθεσης δράσεων και αποτελεσμάτων.

Υπό το πρίσμα αυτό, ορίζεται ο υπεύθυνος φορέας για την υλοποίηση κάθε εμβληματικής δράσης και οι φορείς που συμμετέχουν στην υλοποίησή της, στο πλαίσιο των αρμοδιοτήτων, της αποστολής τους και την κρισιμότητα του ρόλου τους. Για κάθε δράση καταρτίζεται Υπόμνημα (Concept Note), με βάση πρότυπο υπόδειγμα, στο οποίο περιλαμβάνονται συνοπτικά οι αναγκαίες πληροφορίες για τον σκοπό, την περιγραφή, τα παραδοτέα καθώς και ενδεικτικό χρονοπρογραμματισμό υλοποίησής της. Κάθε φορέας παρέχει πληροφορίες για την πορεία υλοποίησης της δράσης στην οποία εμπλέκεται, στο πλαίσιο του ολοκληρωμένου μηχανισμού συγκέντρωσης, διαχείρισης και ανάλυσης δεδομένων, ο οποίος υποστηρίζεται από ψηφιακά εργαλεία και περιλαμβάνει το σύνολο των αναγκαίων σταδίων, από τη συλλογή των στοιχείων για την πορεία υλοποίησης των δράσεων, μέχρι τη σύνταξη ετήσιων εκθέσεων και την ανατροφοδότηση του εθνικού στρατηγικού σχεδιασμού.

Εικόνα 13: Στάδια συγκέντρωσης και ανάλυσης δεδομένων για την αξιολόγηση της πορείας υλοποίησης της ΕΣΚ 2026-2030

Η εισαγωγή των στοιχείων στις φόρμες παρακολούθησης και αξιολόγησης από τους Συντονιστές πραγματοποιείται μέσω κατάλληλης πλατφόρμας, με στόχο τη βελτιστοποίηση των διαδικασιών αξιολόγησης, αναφοράς, συνολικής διοίκησης των δράσεων και παρακολούθησης της προόδου υλοποίησης.

Με τον ανωτέρω μηχανισμό παρέχεται σε πραγματικό χρόνο πληροφόρηση για την πορεία υλοποίησης της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026 – 2030, προκύπτουν τα δυνατά σημεία αλλά και οι τυχόν αδυναμίες και προκλήσεις στην εφαρμογή των δράσεων, με σκοπό την αποτελεσματικότερη και έγκαιρη αντιμετώπισή τους.

5. Προσδιορισμός των Αρχών και του Οράματος της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026–2030

5.Α. Κατευθυντήριες Αρχές για τον Σχεδιασμό και την Υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας

Το Όραμα, οι στρατηγικοί και ειδικοί στόχοι της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026–2030, διαμορφώνονται βάσει ενός συνόλου θεμελιωδών κατευθυντηρίων αρχών που καθοδηγούν τον εθνικό σχεδιασμό πολιτικής στον τομέα της κυβερνοασφάλειας. Οι αρχές αυτές καθοδηγούν την ανάπτυξη του Σχεδίου Δράσης και διαμορφώνουν το πλαίσιο υλοποίησής του. Συγκεκριμένα:

Προσέγγιση της Κοινωνίας ('Whole of Society Approach')

Ο σχεδιασμός και η εφαρμογή της στρατηγικής θεμελιώνονται στη συνεργασία και τη συνυπευθυνότητα όλων των εμπλεκόμενων φορέων: δημόσιων οργανισμών, ιδιωτικού τομέα, ακαδημαϊκής και ερευνητικής κοινότητας, κοινωνίας των πολιτών και των ίδιων των πολιτών. Η αρχή αυτή ενσωματώνεται μέσω δομημένων μηχανισμών διακυβέρνησης που εξασφαλίζουν συνεχή συνεργασία, συντονισμό και διάχυση πληροφορίας.

Εφαρμογή Συστήματος Διακυβέρνησης για την Εφαρμογή της Στρατηγικής

Η στρατηγική υποστηρίζεται από ενιαίο σύστημα διακυβέρνησης που παρακολουθεί την πρόοδο υλοποίησης, συλλέγει ανατροφοδότηση, διασφαλίζει την ευθυγράμμιση των εμπλεκόμενων φορέων και επιτρέπει την προσαρμογή των δράσεων στις ανάγκες της κοινωνίας και της οικονομίας. Η οργανωμένη αυτή δομή ενισχύει την αποτελεσματική εφαρμογή της "whole-of-society" προσέγγισης.

Τεκμηριωμένη, 'Risk-based' και 'Evidence-driven' Πολιτική

Οι προτεραιότητες καθορίζονται μέσω ανάλυσης κινδύνων, αποτίμησης απειλών και αξιοποίησης μετρήσιμων δεδομένων σχετικά με την ωριμότητα κυβερνοασφάλειας που παρουσιάζουν οι διάφοροι τομείς. Ο σχεδιασμός λαμβάνει υπόψη τη δυναμική του περιβάλλοντος απειλών και τις ανάγκες των κρίσιμων λειτουργιών της χώρας.

Εναρμόνιση με το Ευρωπαϊκό και Διεθνές Πλαίσιο

Η στρατηγική ευθυγραμμίζεται με το ενωσιακό θεσμικό και στρατηγικό πλαίσιο κυβερνοασφάλειας και υιοθετεί καθιερωμένες διεθνείς και ευρωπαϊκές αρχές, πρότυπα και βέλτιστες πρακτικές. Η εναρμόνιση αυτή ενισχύει τη διαλειτουργικότητα, την αξιοπιστία και τη συνολική ανθεκτικότητα του εθνικού οικοσυστήματος κυβερνοασφάλειας.

Συμμετοχικός Σχεδιασμός και Δημόσια Διαβούλευση

Οι απόψεις της κοινωνίας ενσωματώνονται μέσα από τη διαδικασία δημόσιας διαβούλευσης, διασφαλίζοντας ότι οι προτεραιότητες της στρατηγικής αντικατοπτρίζουν τις ανάγκες των πολιτών και των χρηστών ψηφιακών υπηρεσιών.

Άμεση Συμβολή των Βασικών Εμπλεκόμενων Φορέων

Οι φορείς της Δημόσιας Διοίκησης συμβάλουν ενεργά στον σχεδιασμό, στην αποτύπωση αναγκών και στον εντοπισμό εμβληματικών δραστηριοτήτων, διασφαλίζοντας ότι το Σχέδιο Δράσης αντανακλά πραγματικές και κοινά αποδεκτές επιχειρησιακές και στρατηγικές προτεραιότητες.

Επικέντρωση σε Υψηλής Προτεραιότητας Εμβληματικές Δραστηριότητες

Το Σχέδιο Δράσης περιλαμβάνει αποκλειστικά τις εμβληματικές δραστηριότητες που, οι οποίες αποτελούν κρίσιμες εθνικές προτεραιότητες στον τομέα της κυβερνοασφάλειας. Παράλληλα, πλήθος συμπληρωματικών δράσεων μπορούν να υλοποιούνται εντός του πλαισίου του Σχεδίου Δράσης, υπό την προϋπόθεση ότι συμβάλλουν στους στρατηγικούς και ειδικούς στόχους της Στρατηγικής.

Ευελιξία και Προσαρμοστικότητα

Η Εθνική Στρατηγική Κυβερνοασφάλειας είναι ζωντανό και δυναμικό στρατηγικό κείμενο, το οποίο αποσκοπεί στην καθοδήγηση των ενεργειών όλων των εμπλεκομένων για την επίτευξη των στόχων σε βάθος χρόνου. Το Σχέδιο Δράσης επανεξετάζεται περιοδικά και επικαιροποιείται συστηματικά ιδίως βάσει:

- του διαρκώς εξελισσόμενου τοπίου απειλών
- των τεχνολογικών εξελίξεων
- του κανονιστικού πλαισίου
- των μεταβαλλόμενων αναγκών της κοινωνίας και της οικονομίας σε εθνικό επίπεδο
- των στρατηγικών επιλογών της χώρας σε τομείς όπως η εθνική άμυνα, η πολιτική προστασία, η οικονομική ανάπτυξη και η προστασία των θεμελιωδών δικαιωμάτων.

Υιοθέτηση Αρχών Αποτελεσματικότητας, Διαφάνειας και Λογοδοσίας

Ο σχεδιασμός και η υλοποίηση των δράσεων βασίζονται σε σαφώς καθορισμένα ορόσημα, μετρήσιμα αποτελέσματα, διαφανείς διαδικασίες λήψης αποφάσεων και μηχανισμούς λογοδοσίας για την πρόοδο και τα επιτεύγματα της στρατηγικής.

5.Β. Διατύπωση του Στρατηγικού Οράματος της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026 - 2030

> «Εγκαθίδρυση μιας ασφαλούς, ανθεκτικής και αξιόπιστης ψηφιακής κοινωνίας, όπου οι Πολίτες, η Δημόσια Διοίκηση και οι Επιχειρήσεις, προστατεύονται αποτελεσματικά από τις κυβερνοαπειλές, ενισχύοντας την εμπιστοσύνη, τη συνεργασία και την καινοτομία στον κυβερνοχώρο. Βασική επιδίωξη είναι η επίτευξη εθνικού επιπέδου κυβερνοανθεκτικότητας, αντίστοιχο με τα πλέον ώριμα ευρωπαϊκά κράτη, επενδύοντας στη συνεχή ενδυνάμωση των ικανοτήτων, στην προστασία των θεμελιωδών δικαιωμάτων και στη βιώσιμη ανάπτυξη του εθνικού οικοσυστήματος κυβερνοασφάλειας.».

Ανάλυση των Δομικών Στοιχείων του Οράματος

Το Όραμα της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026–2030 διαμορφώνεται γύρω από πέντε κεντρικούς άξονες, οι οποίοι αποτυπώνουν τις υψηλού επιπέδου φιλοδοξίες της χώρας για την ερχόμενη πενταετία, καθώς και τη δέσμευσή της να ευθυγραμμίσει το συνολικό επίπεδο την κυβερνοανθεκτικότητάς της με τα πλέον ώριμα οικοσυστήματα κυβερνοασφάλειας των κρατών μελών της Ευρωπαϊκής Ένωσης.

1. Διαμόρφωση ενός αποτελεσματικού συστήματος διακυβέρνησης της κυβερνοασφάλειας

Το όραμα στηρίζεται στην καθιέρωση ενός συνεκτικού, συμπεριληπτικού και αποτελεσματικού συστήματος διακυβέρνησης της κυβερνοασφάλειας, το οποίο καλύπτει το σύνολο της δημόσιας διοίκησης και επεκτείνεται στο σύνολο της Κοινωνίας.

Η προσέγγιση “whole-of-society” αποτελεί θεμέλιο της στρατηγικής, με έμφαση:

- στον σαφή επιμερισμό ρόλων, αρμοδιοτήτων και ευθυνών,
- στη λειτουργική διασύνδεση των εμπλεκόμενων φορέων, ξεπερνώντας τη λειτουργία «σιλό»,
- στη δημιουργία μηχανισμών χάραξης, εφαρμογής και παρακολούθησης πολιτικής που εξασφαλίζουν διαφάνεια, συνέπεια και συνεχή ανατροφοδότηση.
- Το σύστημα διακυβέρνησης αποτελεί βασικό παράγοντα για τη διατηρήσιμη εφαρμογή του οράματος και ως εκ τούτου ενσωματώνεται σε όλες τις θεματικές προτεραιότητες της στρατηγικής.

2. Ενίσχυση της επιχειρησιακής ικανότητας, με έμφαση στα πεδία της πρόληψης, ετοιμότητας και απόκρισης

Κεντρικό στοιχείο του οράματος είναι η θεμελίωση μιας ανθεκτικής και αποτελεσματικής εθνικής επιχειρησιακής αρχιτεκτονικής κυβερνοασφάλειας.

Αυτή περιλαμβάνει ιδίως:

- Την αναβάθμιση των δυνατοτήτων ανίχνευσης και απόκρισης σε περιστατικά.
- Τη βελτίωση των μηχανισμών διαχείρισης κινδύνων σε δημόσιο και ιδιωτικό τομέα.
- Την ενίσχυση των κρίσιμων υποδομών έναντι εξελισσόμενων απειλών.

- Την ανάπτυξη εθνικών υπηρεσιών και υποδομών που υποστηρίζουν την πρόληψη, ετοιμότητα και ανάκαμψη από επιθέσεις.

Η αυξημένη επιχειρησιακή ικανότητα αποτελεί το πρακτικό σκέλος της κυβερνοανθεκτικότητας και συνδέεται άμεσα με την ικανότητα της χώρας να προστατεύει τη λειτουργικότητα του κοινωνικού και οικονομικού της ιστού.

3. Οριζόντια ανάπτυξη δεξιοτήτων, γνώσεων και κουλτούρας κυβερνοασφάλειας

Το όραμα προβλέπει ένα περιβάλλον όπου πολίτες, επαγγελματίες και οργανισμοί διαθέτουν το αναγκαίο επίπεδο δεξιοτήτων, επίγνωσης και ευαισθητοποίησης, ώστε να λειτουργούν με ασφάλεια στον κυβερνοχώρο.

Η υλοποίηση του οράματος προϋποθέτει:

- ένα συνεκτικό πλαίσιο εκπαίδευσης και κατάρτισης,
- την ενίσχυση της ψηφιακής υπευθυνότητας των χρηστών,
- την προσέλκυση, ανάπτυξη και διατήρηση ανθρώπινου δυναμικού υψηλής εξειδίκευσης,
- την εδραίωση κουλτούρας πρόληψης, λογοδοσίας και ασφάλειας “by-design”.

Η καλλιέργεια ενός ώριμου κοινωνικού και επαγγελματικού οικοσυστήματος αποτελεί προϋπόθεση για τη μακροπρόθεσμη επιτυχία της στρατηγικής.

4. Προώθηση επενδύσεων, καινοτομίας και των συνεργασιών ως μοχλών κυβερνοανθεκτικότητας

Το όραμα αναγνωρίζει την ανάγκη για ένα ισχυρό, ανταγωνιστικό και καινοτόμο οικοσύστημα κυβερνοασφάλειας που συνδέει:

- την έρευνα και τεχνολογική ανάπτυξη,
- την επιχειρηματικότητα,
- τη συνεργασία δημόσιου και ιδιωτικού τομέα,
- την αξιοποίηση εθνικών και ευρωπαϊκών μηχανισμών χρηματοδότησης.

Η χώρα στοχεύει να λειτουργήσει ως ενεργός κόμβος κυβερνοασφάλειας και να ενισχύσει τη συμμετοχή της στα ευρωπαϊκά δίκτυα και στα σχήματα συνεργασίας ευρωπαϊκών και διεθνών οργανισμών.

5. Επίτευξη υψηλών επιπέδων κυβερνοανθεκτικότητας, συγκρίσιμων με τα πλέον ώριμα κράτη-μέλη της ΕΕ

Η φιλοδοξία της Στρατηγικής δεν περιορίζεται στη συμμόρφωση με το ενωσιακό πλαίσιο, αλλά επεκτείνεται στη σταδιακή σύγκλιση, σε ορίζοντα πενταετίας, με τα πιο προηγμένα οικοσυστήματα κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης, όπως αποτυπώνεται σε ευρωπαϊκούς και διεθνείς δείκτες ωριμότητας.

Η επίτευξη αυτού του στόχου βασίζεται:

- στη συστηματική παρακολούθηση της προόδου υλοποίησης του Action Plan,
- στην αξιολόγηση της ωριμότητας μέσω τυποποιημένων μεθοδολογιών όπως το National Capabilities Assessment Framework και δεικτών όπως ο Cybersecuriy Index του ENISA,

- στην προσαρμογή της στρατηγικής βάσει της δυναμικής εξέλιξης του πεδίου απειλών και των τεχνολογικών εξελίξεων,
- στη συνεχή βελτίωση πολιτικών, διαδικασιών και θεσμικών ρυθμίσεων.

Το στοιχείο αυτό του οράματος λειτουργεί ως δείκτης κατεύθυνσης και ως μέτρο επιτυχίας της στρατηγικής στο σύνολό της.

Τέσσερις (4) Στρατηγικοί Στόχοι ΕΣΚ 2026 - 2030

Σε ένα πρώτο επίπεδο, αξιοποιούνται τα αποτελέσματα της ανάλυσης των στρατηγικών προτεραιοτήτων, ώστε να διαμορφωθούν τέσσερις (4) εμβληματικοί στόχοι ανάπτυξης του στρατηγικού σχεδιασμού,

Στρατηγικός Στόχος 1: Ανάπτυξη Ικανοτήτων & Ευαισθητοποίηση	•Ενίσχυση Δεξιοτήτων •Ευαισθητοποίηση της Κοινωνίας •Ετοιμότητα & Απόκριση
Στρατηγικός Στόχος 2: Ενίσχυση Εθνικής, Ευρωπαϊκής και Διεθνούς Συνεργασίας	•Πρόληψη & Αντιμετώπιση Κυβερνοεγκλήματος •Ανταλλαγή Πληροφοριών •Διακρατική Συνεργασία
Στρατηγικός Στόχος 3: Ένα Σύστημα Διακυβέρνησης της Κυβερνοασφάλειας	•Διαχείριση Κρίσεων •Ψηφιακή Εμπιστοσύνη •Αξιολόγηση Κινδύνων
Στρατηγικός Στόχος 4: Ενίσχυση Κανονιστικής Συμμόρφωσης & Αναβάθμιση Πολιτικών	•Κυβερνοασφάλεια και προστασία της ιδιωτικότητας από το σχεδιασμό •Ασφάλεια Εφοδιαστικής Αλυσίδας •Διαχείριση Κινδύνων & Συμμόρφωση

19 Ειδικοί Στόχοι

Για κάθε έναν από τους ανωτέρω στρατηγικούς στόχους αναπτύσσονται ειδικοί στόχοι, οι οποίοι αποσκοπούν στην εξειδίκευση και καλύτερη διαχείριση του στρατηγικού πλαισίου (cascade effect). Εν συνεχεία, οι ειδικοί στόχοι εξειδικεύονται σε εμβληματικές δραστηριότητες, οι οποίες καλύπτουν όλο το φάσμα της αναγνώρισης, πρόληψης και προστασίας, αποτροπής και ανάκαμψης από κυβερνοεπιθέσεις.

Στρατηγικοί Στόχοι ΕΣΚ 2026 - 2030	Ειδικοί Στόχοι
1. Ανάπτυξη Ικανοτήτων και Ευαισθητοποίηση	1.Α. Ενίσχυση της Κυβερνοανθεκτικότητας και της Κυβερνο-Υγιεινής του Ιδιωτικού Τομέα και των Μικρομεσαίων Επιχειρήσεων
	1.Β. Γεφύρωση του Χάσματος Δεξιοτήτων στην Κυβερνοασφάλεια
	1.Γ. Προώθηση των Επενδύσεων και της Καινοτομίας
	1.Δ. Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας
2. Ενίσχυση της Εθνικής, Ευρωπαϊκής και Διεθνούς Συνεργασίας	2.Α. Ενίσχυση των Μηχανισμών Πρόληψης και Αντιμετώπισης του Κυβερνοεγκλήματος
	2.Β. Ενίσχυση της Ευρωπαϊκής και Διεθνούς Συνεργασίας
	2.Γ. Θέσπιση Αξιόπιστων Μηχανισμών Ανταλλαγής Πληροφοριών
	2.Δ. Θέσπιση Διαδικασιών Αμοιβαίας Συνδρομής
3. Ένα Σύστημα Διακυβέρνησης της Κυβερνοασφάλειας για το Σύνολο της Κοινωνίας	3.Α. Ανάπτυξη Πλαισίων Διαχείρισης Κρίσεων Κυβερνοασφάλειας
	3.Β. Ασφαλής Ψηφιακή Ταυτότητα και Εμπιστοσύνη στις Δημόσιες Ψηφιακές Υπηρεσίες
	3.Γ. Θέσπιση Εθνικού Πλαισίου Εκτίμησης Κινδύνων Κυβερνοασφάλειας
	3.Δ. Ενίσχυση της Εθνικής Διακυβέρνησης Κυβερνοασφάλειας
	3.Ε. Θέσπιση Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας
	3.ΣΤ. Ενίσχυση Μηχανισμών Αναφοράς Περιστατικών Κυβερνοασφάλειας

4. Ενίσχυση της Κανονιστικής Συμμόρφωσης & Αναβάθμιση Πολιτικών & Μέτρων Κυβερνοασφάλειας	4.Α. Διασφάλιση της Ισορροπίας μεταξύ Κυβερνοασφάλειας και Προστασίας της Ιδιωτικότητας
	4.Β. Ενίσχυση της Κυβερνοασφάλειας της Εφοδιαστικής Αλυσίδας
	4.Γ. Προστασία και Ενίσχυση της Ανθεκτικότητας των Κρίσιμων Τομέων
	4.Δ. Θέσπιση Εθνικής Πολιτικής Συντονισμένης Γνωστοποίησης Ευπαθειών (CVD Policy)
	4.Ε: Προώθηση της Ενεργητικής Προστασίας στον Κυβερνοχώρο

6. Χρηματοδότηση Έργων και Δράσεων Κυβερνοασφάλειας

Για την επιτυχή υλοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026–2030 και του Σχεδίου Δράσης, είναι κρίσιμη η διαθεσιμότητα ευρωπαϊκών και εθνικών χρηματοδοτικών εργαλείων, τα οποία μπορούν να υποστηρίξουν τις εμβληματικές δραστηριότητες και τις συμπληρωματικές πρωτοβουλίες που θα αναπτυχθούν για την εφαρμογή του. Παράλληλα, η χρηματοδότηση έργων κυβερνοασφάλειας από φορείς του δημόσιου και του ιδιωτικού τομέα —ανεξάρτητα από το κατά πόσο εντάσσονται στο πλαίσιο της Στρατηγικής— συμβάλλει ουσιαστικά στην ενίσχυση των εθνικών ικανοτήτων και στη διαμόρφωση ενός πιο ανθεκτικού οικοσυστήματος. Η αποτελεσματικότητα της Στρατηγικής εξαρτάται σε μεγάλο βαθμό από τη συνολική διαθεσιμότητα και διοχέτευση πόρων σε υποδομές, ανθρώπινο δυναμικό, έρευνα, καινοτομία και υπηρεσίες ασφάλειας, δημιουργώντας συνέργειες που ενισχύουν την ψηφιακή ανθεκτικότητα της χώρας. Οι πηγές χρηματοδότησης διακρίνονται σε τρεις κύριες κατηγορίες: (i) χρηματοδοτήσεις από τον ευρωπαϊκό προϋπολογισμό, (ii) χρηματοδοτήσεις από τον κρατικό προϋπολογισμό, και (iii) χρηματοδοτήσεις και επενδύσεις από τη βιομηχανία και τον ιδιωτικό τομέα εν γένει (βασικές και σημαντικές οντότητες).

6.Α. Ευρωπαϊκές πηγές χρηματοδότησης

Digital Europe Programme

Το Πρόγραμμα Ψηφιακή Ευρώπη (Digital Europe Programme) αποτελεί το βασικό χρηματοδοτικό εργαλείο της Ευρωπαϊκής Ένωσης για την προώθηση και υιοθέτηση προηγμένων ψηφιακών τεχνολογιών από επιχειρήσεις, πολίτες και δημόσιους οργανισμούς, με ιδιαίτερη έμφαση στην κυβερνοασφάλεια, την τεχνητή νοημοσύνη, τις ψηφιακές δεξιότητες και τις υποδομές υψηλών επιδόσεων. Στο ίδιο πλαίσιο, το ECCC Digital Europe Cybersecurity Work Programme 2025–2027[34], ενισχύει τη στοχευμένη ευρωπαϊκή επένδυση στην κυβερνοασφάλεια, παρέχοντας χρηματοδοτικά εργαλεία για την υποστήριξη υλοποίησης των ευρωπαϊκών στόχων κυβερνοασφάλειας.

Το πλαίσιο αυτό δημιουργεί σημαντικές ευκαιρίες για την Ελλάδα, για την αναβάθμιση εθνικών υποδομών και την υποστήριξη κρίσιμων τομέων και επιχειρήσεων.

[34] https://cybersecurity-centre.europa.eu/document/download/a35f7be2-4464-43d3-a40f-6ec942036f48_en?filename=Amendment2cleanDEPcybersecurityWP2025-2027.pdf

Οι χρηματοδοτικές δράσεις οργανώνονται σε τρεις κατηγορίες:

1. Τεχνολογική αναβάθμιση και καινοτομία στην κυβερνοασφάλεια

Η κατηγορία αυτή επικεντρώνεται στην υιοθέτηση και εφαρμογή προηγμένων τεχνολογιών ασφάλειας. Περιλαμβάνει:

- αξιοποίηση παραγωγικής τεχνητής νοημοσύνης (generative AI),
- ενίσχυση της ασφάλειας συστημάτων AI και χρήση AI για την αντιμετώπιση κυβερνοαπειλών,
- μετάβαση σε τεχνολογίες **Post-Quantum Encryption** για δημόσια διοίκηση και κρίσιμες υποδομές,
- ενίσχυση εθνικών και διασυνοριακών **Cyber Hubs** για τη βελτίωση των επιχειρησιακών δυνατοτήτων κυβερνοάμυνας.

2. Εφαρμογή του Cyber Solidarity Act & ενίσχυση ευρωπαϊκών μηχανισμών ανίχνευσης–απόκρισης

- ανάπτυξη και ενίσχυση **Cyber Hubs** και **Cross-Border Cyber Hubs**,
- ενσωμάτωση στο **European Cybersecurity Alert System** για έγκαιρη ανίχνευση απειλών,
- συντονισμένες δοκιμές, ασκήσεις και δράσεις ετοιμότητας για τομείς υψηλής κρισιμότητας,
- ενεργοποίηση του **Cybersecurity Emergency Mechanism**,
- ενίσχυση πρωτοβουλιών **αμοιβαίας συνδρομής μεταξύ κρατών μελών**,
- επενδύσεις σε περιφερειακούς κόμβους προστασίας υποθαλάσσιων καλωδίων και σε συστήματα ασφάλειας κρίσιμων υποθαλάσσιων υποδομών.

3. Ενίσχυση ανθεκτικότητας & εφαρμογή ενωσιακών κανονιστικών πλαισίων

Περιλαμβάνει:

- υποστήριξη της εφαρμογής των **NIS2**, **Cybersecurity Act** και **Cyber Resilience Act**,
- ενίσχυση ΜΜΕ, νεοφυών επιχειρήσεων και βιομηχανικών φορέων για τη συμμόρφωση στις απαιτήσεις ασφάλειας,
- δράσεις για την κυβερνοασφάλεια του **τομέα της υγείας**, με έμφαση στην προστασία νοσοκομείων και παρόχων υγείας,
- πρωτοβουλίες για την ανάπτυξη και θωράκιση υποδομών προστασίας υποθαλάσσιων συστημάτων και εθνικών κρίσιμων υποδομών.

Ορίζοντας Ευρώπη (Horizon Europe)

Το πρόγραμμα Ορίζοντας Ευρώπη αποτελεί βασικό χρηματοδοτικό μηχανισμό της Ευρωπαϊκής Ένωσης για την έρευνα και την καινοτομία στον τομέα της κυβερνοασφάλειας. Στο πλαίσιο της Ομάδας 3 «Ασφάλεια των πολιτών για την κοινωνία»[35] (Cluster 3 "Civil Security for Society"), το Πρόγραμμα υποστηρίζει δράσεις που ενισχύουν την ανθεκτικότητα κρίσιμων υποδομών, την ανάπτυξη προηγμένων τεχνολογιών ασφάλειας, καθώς και την έρευνα σε τομείς όπως η κυβερνοάμυνα, η προστασία συστημάτων και η ασφάλεια δεδομένων.

Το Στρατηγικό Πλάνο (Strategic Plan) 2025–2027[36] του Ορίζοντα Ευρώπη συνεχίζει να δίνει προτεραιότητα στην κυβερνοασφάλεια, προωθώντας στοχευμένες επενδύσεις και διευρύνοντας τις δυνατότητες συμμετοχής της Ελλάδας σε ερευνητικά και καινοτομικά έργα υψηλής στρατηγικής αξίας.

Κατά την περίοδο εφαρμογής της Στρατηγικής (2026–2030), αναμένεται να συνεχίσει να υποστηρίζει ερευνητικές δράσεις στο πλαίσιο του Cluster 3 – "Civil Security for Society". Για τον νέο κύκλο 2026–2027, η Ευρωπαϊκή Επιτροπή έχει δημοσιοποιήσει προσχέδια θεματικών προτεραιοτήτων του Cluster 3, όπου περιλαμβάνονται δράσεις για έρευνα, δοκιμή και ανάπτυξη προηγμένων λύσεων κυβερνοασφάλειας, κρυπτογραφίας, τεχνητής νοημοσύνης ασφαλείας και προστασίας κρίσιμων ψηφιακών υποδομών.

ΕΣΠΑ 2021 - 2027

Το ΕΣΠΑ 2021–2027[37] ως «ομπρέλα» ευρωπαϊκών και εθνικών πόρων για την περίοδο 2021-2027, αποτελεί επίσης συμπληρωματική πηγή χρηματοδότησης για έργα και δράσεις στον τομέα της κυβερνοασφάλειας.

Ειδικότερα, το Επιχειρησιακό Πρόγραμμα «Ψηφιακός Μετασχηματισμός» χρηματοδοτεί πράξεις που συνδέονται άμεσα με την κυβερνοασφάλεια, όπως η αναβάθμιση των κεντρικών υποδομών ηλεκτρονικής διακυβέρνησης, η ενίσχυση των συστημάτων ταυτοποίησης και ελέγχου πρόσβασης, οι υπηρεσίες προστασίας δεδομένων και η ανάπτυξη μηχανισμών διαλειτουργικότητας ασφαλείας[38].

6.Β. Τακτικός Προϋπολογισμός & Πρόγραμμα Δημοσίων Επενδύσεων

Οι εθνικοί πόροι, συμπεριλαμβανομένου του Προγράμματος Δημοσίων Επενδύσεων, χρηματοδοτούν έργα που απαιτούν εθνική συμμετοχή ή αποτελούν στρατηγική προτεραιότητα. Η αξιοποίηση του Τακτικού Προϋπολογισμού και του ΠΔΕ λειτουργεί είτε ως πολλαπλασιαστής των ευρωπαϊκών χρηματοδοτήσεων, είτε ως πηγή χρηματοδότησης δράσεων και έργων εθνικού αμιγώς ενδιαφέροντος διασφαλίζοντας ότι δράσεις υποδομών, εκπαίδευσης και οργανωτικής ενίσχυσης στην κυβερνοασφάλεια υλοποιούνται με ευελιξία, ταχύτητα και συνέχεια.

---

[35] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en

[36] European Commission: Directorate-General for Research and Innovation, *Horizon Europe strategic plan 2025-2027*, Publications Office of the European Union, 2024, https://data.europa.eu/doi/10.2777/092911

[37] https://www.espa.gr/el/Documents/2127/Etairiko_Symfwno_Perifereiakis_Anaptyxis_ESPA_2021-2027_29-08-2021.pdf

[38] https://www.digitaltransform.gr/

7. Σχέδιο Δράσης της ΕΣΚ 2026 - 2030

Στρατηγικός Στόχος 1: Ανάπτυξη Ικανοτήτων και Ευαισθητοποίηση

Ο Στρατηγικός Στόχος 1, αποσκοπεί στη συστηματική ενδυνάμωση των ικανοτήτων κυβερνοασφάλειας, τη γεφύρωση του χάσματος δεξιοτήτων (skills gap) σε εθνικό επίπεδο και στην καλλιέργεια ώριμης κουλτούρας ασφάλειας σε ολόκληρη την Κοινωνία. Καλύπτει τον ιδιωτικό και τον δημόσιο τομέα, τις ΜΜΕ, την εκπαίδευση και το ανθρώπινο δυναμικό υψηλής εξειδίκευσης, ώστε η χώρα να διαθέτει τις δεξιότητες, τα εργαλεία και τις δομές που απαιτούνται για να προλαμβάνει, να ανιχνεύει και να αντιμετωπίζει αποτελεσματικά αναδυόμενες κυβερνοαπειλές.

Μέσω της στοχευμένης ανάπτυξης δεξιοτήτων, της ενίσχυσης της επιχειρησιακής ετοιμότητας και της προώθησης επενδύσεων και καινοτομίας, ο Στρατηγικός Στόχος 1 διαμορφώνει ένα ολοκληρωμένο πλαίσιο ενδυνάμωσης του εθνικού οικοσυστήματος κυβερνοασφάλειας. Με αυτόν τον τρόπο, συμβάλλει στην επίτευξη υψηλών επιπέδων κυβερνοανθεκτικότητας, την προστασία θεμελιωδών δικαιωμάτων στον κυβερνοχώρο και την ενίσχυση της εμπιστοσύνης σε μια ασφαλή, ανθεκτική και αξιόπιστη ψηφιακή κοινωνία.

Ειδικός Στόχος 1.Α: Ενίσχυση της Κυβερνοανθεκτικότητας και της Κυβερνο-Υγιεινής του Ιδιωτικού Τομέα και των Μικρομεσαίων Επιχειρήσεων

Ο Ειδικός Στόχος 1.Α επικεντρώνεται στη σταδιακή αναβάθμιση της κυβερνοανθεκτικότητας και της κυβερνο-υγιεινής των επιχειρήσεων, με ιδιαίτερη έμφαση στις μικρομεσαίες επιχειρήσεις, οι οποίες κυρίως λόγω μεγέθους δεν καλύπτονται από το ειδικό κανονιστικό πλαίσιο του ν. 5160/2024, πλην όμως αποτελούν τη ραχοκοκκαλιά της εθνικής οικονομίας. Προβλέπει την ουσιαστική κατανόηση των αναγκών τους, την ενίσχυση της συμμόρφωσης με διεθνώς αναγνωρισμένα πρότυπα και την παροχή πρακτικών εργαλείων και κατευθυντήριων γραμμών για την καθημερινή διαχείριση των κινδύνων.

Μέσα από στοχευμένες παρεμβάσεις, δράσεις ενημέρωσης και διασύνδεση με εθνικές και ευρωπαϊκές πρωτοβουλίες στήριξης, ο στόχος αυτός επιδιώκει να καταστήσει την κυβερνοασφάλεια οργανικό μέρος του επιχειρηματικού μοντέλου των ΜΜΕ. Έτσι, ενισχύεται η βιωσιμότητα και ανταγωνιστικότητά τους, περιορίζονται οι συστημικοί κίνδυνοι για την οικονομία και προωθείται μια κουλτούρα προληπτικής διαχείρισης των κυβερνοαπειλών.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
1.Α Ενίσχυση της Κυβερνοανθεκτικότητας και της Κυβερνο-Υγιεινής του Ιδιωτικού Τομέα και των Μικρομεσαίων Επιχειρήσεων	1.Α.1: Διενέργεια μελέτης για την αναγνώριση των συγκεκριμένων αναγκών κυβερνοασφάλειας των ΜΜΕ, εκτός πεδίου εφαρμογής του ν. 5160/2024
	1.Α.2: Προαγωγή της εφαρμογής Ευρωπαϊκών & Διεθνών Προτύπων Κυβερνοασφάλειας από οντότητες.
	1.Α.3: Εργαλειοθήκη Κυβερνο-ετοιμότητας για Μικρομεσαίες Επιχειρήσεις και Αυτοαπασχολούμενους

1.Α.1: Διενέργεια μελέτης για την αναγνώριση των συγκεκριμένων αναγκών κυβερνοασφάλειας των ΜΜΕ, εκτός πεδίου εφαρμογής του ν. 5160/2024

Η δράση στοχεύει στη διενέργεια μελέτης για την καταγραφή και ανάλυση των αναγκών κυβερνοασφάλειας των μικρομεσαίων επιχειρήσεων που δεν εμπίπτουν στο πεδίο εφαρμογής του ν. 5160/2024. Η μελέτη θα εντοπίσει τα κύρια κενά σε δεξιότητες, υποδομές και πρακτικές ασφάλειας, παρέχοντας προτάσεις για στοχευμένες παρεμβάσεις και μέτρα υποστήριξης με σκοπό την ενίσχυση της κυβερνοανθεκτικότητας της συγκεκριμένης κατηγορίας ΜΜΕ.

1.Α.2: Προαγωγή της εφαρμογής Ευρωπαϊκών & Διεθνών Προτύπων Κυβερνοασφάλειας από οντότητες.

Η δράση αποσκοπεί στην προώθηση και ενθάρρυνση της εφαρμογής ευρωπαϊκών και διεθνών προτύπων κυβερνοασφάλειας, όπως ISO 27001, ISO 22301 και ENISA guidelines, από επιχειρήσεις και λοιπές οντότητες του ιδιωτικού και δημόσιου τομέα. Μέσω ενημέρωσης, τεχνικής καθοδήγησης και κινήτρων , θα ενισχυθεί η υιοθέτηση βέλτιστων πρακτικών και η συνολική κυβερνοανθεκτικότητα των οργανισμών.

1.Α.3: Εργαλειοθήκη Κυβερνο-ετοιμότητας για Μικρομεσαίες Επιχειρήσεις και Αυτοαπασχολούμενους

Η δράση αποσκοπεί στην ενίσχυση της κυβερνοετοιμότητας και της ανθεκτικότητας των μικρομεσαίων επιχειρήσεων (ΜμΕ) και των αυτοαπασχολούμενων, μέσω της ανάπτυξης μίας Εργαλειοθήκης Κυβερνοασφάλειας (Cyber Readiness Toolkit) που θα προσφέρει πρακτικά εργαλεία, πρότυπα και κατευθυντήριες γραμμές για την πρόληψη και αντιμετώπιση κυβερνοαπειλών.

Η Εργαλειοθήκη θα περιλαμβάνει:

- Απλοποιημένα πρότυπα πολιτικών ασφάλειας (π.χ. χρήση κωδικών πρόσβασης, διαχείριση πρόσβασης, εφεδρικά αντίγραφα ασφαλείας).

- Οδηγούς αυτοαξιολόγησης κινδύνων και λίστες ελέγχου (checklists) για τον έλεγχο της ετοιμότητας.
- Εκπαιδευτικό και ενημερωτικό υλικό, με έμφαση στην κυβερνο-υγιεινή, την προστασία δεδομένων και την ασφαλή χρήση ψηφιακών υπηρεσιών.
- Διασύνδεση με διαθέσιμες εθνικές και ευρωπαϊκές πρωτοβουλίες στήριξης των ΜμΕ, όπως προγράμματα επιδότησης εργαλείων ή υπηρεσιών κυβερνοασφάλειας.

Ειδικός Στόχος 1.Β: Γεφύρωση του Ελλείματος Δεξιοτήτων ('Skills Gap') στην Κυβερνοασφάλεια

Ο Ειδικός Στόχος 1.Β στοχεύει στη συστηματική αντιμετώπιση του εθνικού ελλείμματος δεξιοτήτων κυβερνοασφάλειας, καλύπτοντας τόσο το ανθρώπινο δυναμικό της Δημόσιας Διοίκησης όσο και το ευρύτερο οικοσύστημα εκπαίδευσης, κατάρτισης και διά βίου μάθησης. Προβλέπει τη δημιουργία συνεκτικού πλαισίου πολιτικής για την εκπαίδευση και ευαισθητοποίηση, την ανάπτυξη εξειδικευμένων προγραμμάτων επανειδίκευσης και αναβάθμισης δεξιοτήτων, καθώς και την αξιοποίηση σύγχρονων εργαλείων προσομοίωσης και πρακτικής άσκησης.

Ιδιαίτερη βαρύτητα δίνεται στη διαμόρφωση ισχυρού πυρήνα εξειδικευμένων στελεχών κυβερνοασφάλειας στη Δημόσια Διοίκηση και στην ενδυνάμωση των ηγετικών ρόλων στον δημόσιο και ιδιωτικό τομέα, ώστε η κυβερνοασφάλεια να αντιμετωπίζεται ως στρατηγική προτεραιότητα. Παράλληλα, ο στόχος αυτός προωθεί τη διάχυση βασικών γνώσεων και δεξιοτήτων σε όλα τα επίπεδα εκπαίδευσης και στους πολίτες, συμβάλλοντας στη μακροπρόθεσμη καλλιέργεια κουλτούρας ασφάλειας και υπεύθυνης συμπεριφοράς στον κυβερνοχώρο.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
1.Β: Γεφύρωση του Ελλείματος Δεξιοτήτων ('Skills Gap') στην Κυβερνοασφάλεια	1.Β.1: Ανάπτυξη πλατφόρμας "cyber range"
	1.Β.2: Εκπόνηση Εθνικού Σχεδίου Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση στην Κυβερνοασφάλεια
	1.Β.3: Υλοποίηση ολοκληρωμένου προγράμματος εκπαίδευσης κυβερνοασφάλειας σε στελέχη της ΔΔ
	1.Β.4: Στοχευμένα προγράμματα ενημέρωσης για ανώτατες διοικήσεις δημόσιου και ιδιωτικού τομέα
	1.Β.5: Υλοποίηση ειδικών προγραμμάτων επανειδίκευσης (reskilling) και αναβάθμισης δεξιοτήτων (upskilling) για ΥΑΣΠΕ για το δημόσιο τομέα.

1.Β.1: Ανάπτυξη πλατφόρμας "cyber range" για την εκπαίδευση του προσωπικού με κρίσιμους ρόλους για την κυβερνοασφάλεια (όπως ΥΑΣΠΕ, διαχειριστές δικτύων, συστημάτων, εφαρμογών, βάσεων δεδομένων, κλπ.) του δημόσιου τομέα.

Η δράση αποσκοπεί στην αναβάθμιση και επανειδίκευση υπαλλήλων, κυρίως ειδικότητας Πληροφορικής αλλά και άλλων ειδικοτήτων, προκειμένου να αναλάβουν καθήκοντα Υπευθύνων Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ) σε φορείς της Δημόσιας Διοίκησης.

Το πρόγραμμα θα περιλαμβάνει εντατική εκπαίδευση σε κρίσιμα αντικείμενα όπως:

- Διακυβέρνηση ασφάλειας και κανονιστική συμμόρφωση.
- Διαχείριση κινδύνων και αντιμετώπιση περιστατικών.
- Τεχνικές και τεχνολογίες ασφάλειας πληροφοριακών συστημάτων.

Η εκπαίδευση θα συνοδεύεται από αξιολόγηση και πιστοποίηση επάρκειας σε συνεργασία με το ΕΚΔΔΑ, διασφαλίζοντας την κάλυψη των απαιτήσεων που προβλέπονται για τον ρόλο του ΥΑΣΠΕ στο πλαίσιο του ν. 5160/2024 (ενσωμάτωση της Οδηγίας NIS2).

Παράλληλα, θα εφαρμοστεί μηχανισμός καθοδήγησης (mentoring) από έμπειρα στελέχη κυβερνοασφάλειας, προκειμένου να ενισχυθεί η πρακτική ικανότητα και η αυτοπεποίθηση των νέων ΥΑΣΠΕ.

Η δράση στοχεύει στη δημιουργία ενός πυρήνα εξειδικευμένων στελεχών κυβερνοασφάλειας στη Δημόσια Διοίκηση, ενισχύοντας την επιχειρησιακή της ανθεκτικότητα και την ικανότητα προστασίας κρίσιμων ψηφιακών υποδομών.

1.Β.2: Εκπόνηση Εθνικού Σχεδίου Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση στην Κυβερνοασφάλεια

Η δράση αποσκοπεί στη διαμόρφωση Εθνικού Σχεδίου Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση στην Κυβερνοασφάλεια, με στόχο τη συστηματική ανάπτυξη δεξιοτήτων και την καλλιέργεια κουλτούρας ασφάλειας. Το σχέδιο θα καλύπτει όλες τις βαθμίδες εκπαίδευσης, από την πρωτοβάθμια έως την τριτοβάθμια, καθώς και την επαγγελματική και δια βίου μάθηση, καθορίζοντας προτεραιότητες, ρόλους, δείκτες επίδοσης και μηχανισμούς συντονισμού σε εθνικό επίπεδο.

1.Β.3: Υλοποίηση ολοκληρωμένου προγράμματος εκπαίδευσης κυβερνοασφάλειας σε στελέχη της ΔΔ

Η δράση αποσκοπεί στην ανάπτυξη και υλοποίηση ενός ολοκληρωμένου προγράμματος εκπαίδευσης κυβερνοασφάλειας για τα στελέχη της Δημόσιας Διοίκησης, με στόχο την ενίσχυση των δεξιοτήτων και της επιχειρησιακής τους ετοιμότητας. Το πρόγραμμα θα περιλαμβάνει θεματικές ενότητες προσαρμοσμένες στα επίπεδα ευθύνης και ρόλου κάθε στελέχους, καλύπτοντας τομείς όπως η διαχείριση κινδύνων, η αναφορά περιστατικών, η προστασία δεδομένων και η ασφάλεια πληροφοριακών συστημάτων.

Η εκπαίδευση θα βασίζεται σε συνδυασμό θεωρητικής κατάρτισης, πρακτικών ασκήσεων και προσομοιώσεων κυβερνοεπιθέσεων, ενώ θα συνοδεύεται από μηχανισμό πιστοποίησης γνώσεων. Στόχος είναι η δημιουργία ενός εξειδικευμένου και ευαισθητοποιημένου ανθρώπινου δυναμικού, ικανού να ενισχύει την ανθεκτικότητα και την κυβερνοασφάλεια της Δημόσιας Διοίκησης.

1.Β.4: Στοχευμένα προγράμματα ενημέρωσης για ανώτατες διοικήσεις δημόσιου και ιδιωτικού τομέα

Η δράση αποσκοπεί στην υλοποίηση στοχευμένων προγραμμάτων ενημέρωσης και διαδραστικών εργαστηρίων (workshops) για τα ανώτατα διοικητικά στελέχη και τις διοικήσεις οργανισμών του δημόσιου και ιδιωτικού τομέα, με στόχο την καλλιέργεια ισχυρής κουλτούρας κυβερνοανθεκτικότητας και υπεύθυνης ηγεσίας.

Τα προγράμματα θα εστιάζουν στις ευθύνες και υποχρεώσεις της διοίκησης σε σχέση με την κυβερνοασφάλεια, όπως:

- την έγκριση και εποπτεία προγραμμάτων διαχείρισης κινδύνων,
- τη διασφάλιση επαρκών πόρων και υποδομών ασφάλειας,
- την υποστήριξη συνεχούς εκπαίδευσης και ανάπτυξης δεξιοτήτων του προσωπικού.

Μέσω διαδραστικών σεναρίων και προσομοιώσεων κυβερνοκρίσεων, τα στελέχη θα ενισχύσουν την ικανότητά τους να λαμβάνουν κρίσιμες αποφάσεις υπό πίεση και να διαχειρίζονται περιστατικά με στρατηγική προσέγγιση.

Η δράση θα καλύπτει επίσης τις απαιτήσεις κανονιστικής συμμόρφωσης που απορρέουν από τον ν. 5160/2024, ενισχύοντας την κατανόηση των υποχρεώσεων των οργανισμών και προάγοντας την υιοθέτηση αρχών εταιρικής διακυβέρνησης που ενσωματώνουν την κυβερνοασφάλεια ως στρατηγική προτεραιότητα.

1.Β.5: Υλοποίηση ειδικών προγραμμάτων επανειδίκευσης (reskilling) και αναβάθμισης δεξιοτήτων (upskilling) για ΥΑΣΠΕ για το δημόσιο τομέα

Η δράση αποσκοπεί στην αναβάθμιση και επανειδίκευση υπαλλήλων, κυρίως ειδικότητας Πληροφορικής αλλά και άλλων ειδικοτήτων, προκειμένου να αναλάβουν καθήκοντα Υπευθύνων Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ) σε φορείς της Δημόσιας Διοίκησης.

Το πρόγραμμα θα περιλαμβάνει εντατική εκπαίδευση σε κρίσιμα αντικείμενα όπως:

- Διακυβέρνηση ασφάλειας και κανονιστική συμμόρφωση.
- Διαχείριση κινδύνων και αντιμετώπιση περιστατικών.
- Τεχνικές και τεχνολογίες ασφάλειας πληροφοριακών συστημάτων.

Η εκπαίδευση θα συνοδεύεται από αξιολόγηση και πιστοποίηση επάρκειας σε συνεργασία με το ΕΚΔΔΑ, διασφαλίζοντας την κάλυψη των απαιτήσεων που προβλέπονται για τον ρόλο του ΥΑΣΠΕ στο πλαίσιο του ν. 5160/2024.

Παράλληλα, θα εφαρμοστεί μηχανισμός καθοδήγησης (mentoring) από έμπειρα στελέχη κυβερνοασφάλειας, προκειμένου να ενισχυθεί η πρακτική ικανότητα και η αυτοπεποίθηση των νέων ΥΑΣΠΕ.

Η δράση στοχεύει στη δημιουργία ενός πυρήνα εξειδικευμένων στελεχών κυβερνοασφάλειας στη Δημόσια Διοίκηση, ενισχύοντας την επιχειρησιακή της ανθεκτικότητα και την ικανότητα προστασίας κρίσιμων ψηφιακών υποδομών.

Ειδικός Στόχος 1.Γ: Προώθηση των Επενδύσεων και της Καινοτομίας

Ο Ειδικός Στόχος 1.Γ εστιάζει στη δημιουργία ενός δυναμικού και καινοτόμου οικοσυστήματος κυβερνοασφάλειας, στο οποίο η έρευνα, η τεχνολογική ανάπτυξη, η επιχειρηματικότητα και η δημόσια πολιτική λειτουργούν συμπληρωματικά. Προωθεί τη στενή συνεργασία με ακαδημαϊκούς και ερευνητικούς φορείς, την ενίσχυση των δομών συντονισμού και δικτύωσης σε εθνικό επίπεδο, καθώς και την ενεργό συμμετοχή σε ευρωπαϊκά σχήματα συνεργασίας και χρηματοδότησης.

Μέσω στοχευμένων οικονομικών κινήτρων, μηχανισμών παρακολούθησης των επενδύσεων και εξειδικευμένων χρηματοδοτικών εργαλείων, ο στόχος αυτός επιδιώκει να κινητοποιήσει ιδιωτικούς και δημόσιους πόρους προς λύσεις κυβερνοασφάλειας που αξιοποιούν τεχνολογίες αιχμής και παρέχουν υψηλή προστιθέμενη αξία στις οντότητες. Με αυτό τον τρόπο, ενισχύεται η ανταγωνιστικότητα της εγχώριας αγοράς, επιταχύνεται η υιοθέτηση καινοτόμων τεχνολογιών και δημιουργούνται σταθερές βάσεις για τη βιώσιμη ανάπτυξη του εθνικού οικοσυστήματος κυβερνοασφάλειας.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
Ειδικός Στόχος 1.Γ: Προώθηση των Επενδύσεων και της Καινοτομίας	1.Γ.1: Ενίσχυση του ρόλου και των λειτουργιών του Εθνικού Κέντρου Συντονισμού (NCC-EL ScaleUP
	1.Γ.2: Συνέχιση ενισχυμένης συνεργασίας με ακαδημαϊκούς και ερευνητικούς φορείς σε θέματα κυβερνοασφάλειας
	1.Γ.3: Σχεδιασμός οικονομικών κινήτρων για επένδυση σε υπηρεσίες και εργαλεία κυβερνοασφάλειας
	1.Γ.4: Δημιουργία Εθνικού Μητρώου Ελλήνων Ερευνητών & Εμπειρογνωμόνων Κυβερνοασφάλειας
	1.Γ.5: Δημιουργία Παρατηρητηρίου Επενδύσεων στην Κυβερνοασφάλεια
	1.Γ.6: Δημιουργία Εθνικού Αποθεματικού Κυβερνοασφάλειας με σκοπό τη χρηματοδοτική υποστήριξη έργων και πρωτοβουλιών που ενισχύουν την κυβερνοανθεκτικότητα δημόσιων και ιδιωτικών οντοτήτων

1.Γ.1: Ενίσχυση του ρόλου και των λειτουργιών του Εθνικού Κέντρου Συντονισμού (NCC-EL ScaleUP)

Η δράση αποσκοπεί στην ενίσχυση του ρόλου και της λειτουργικής ικανότητας του Εθνικού Κέντρου Συντονισμού (NCC-EL) μέσω του έργου ScaleUP, με στόχο την προώθηση της καινοτομίας, των

επενδύσεων και της συνεργασίας στον τομέα της κυβερνοασφάλειας. Περιλαμβάνει την περαιτέρω ανάπτυξη μηχανισμών υποστήριξης του οικοσυστήματος, τη διεύρυνση των συνεργασιών με ερευνητικούς και επιχειρηματικούς φορείς και την αποτελεσματική αξιοποίηση των χρηματοδοτικών εργαλείων της ΕΕ.

1.Γ.2: Συνέχιση ενισχυμένης συνεργασίας με ακαδημαϊκούς και ερευνητικούς φορείς σε θέματα κυβερνοασφάλειας

Η δράση στοχεύει στη συνέχιση και διεύρυνση της συνεργασίας με ακαδημαϊκά και ερευνητικά ιδρύματα για την προώθηση της έρευνας, της καινοτομίας και της μεταφοράς τεχνογνωσίας στην κυβερνοασφάλεια. Επιδιώκεται η από κοινού ανάπτυξη ερευνητικών έργων, η ενίσχυση των εθνικών ικανοτήτων μέσω επιστημονικών συνεργειών και η διασύνδεση της ερευνητικής κοινότητας με το οικοσύστημα κυβερνοασφάλειας της χώρας.

1.Γ.3: Σχεδιασμός οικονομικών κινήτρων για επένδυση σε υπηρεσίες και εργαλεία κυβερνοασφάλειας

Η δράση αποσκοπεί στη διαμόρφωση πλαισίου οικονομικών και φορολογικών κινήτρων για την ενθάρρυνση επενδύσεων σε υπηρεσίες, προϊόντα και εργαλεία κυβερνοασφάλειας από φορείς του ιδιωτικού τομέα. Μέσω της δράσης θα προωθηθεί η ανάπτυξη της εγχώριας αγοράς κυβερνοασφάλειας, η ενίσχυση της καινοτομίας και η αύξηση της ανθεκτικότητας των επιχειρήσεων και οργανισμών απέναντι στις ψηφιακές απειλές.

1.Γ.4: Δημιουργία Εθνικού Μητρώου Ελλήνων Ερευνητών & Εμπειρογνωμόνων Κυβερνοασφάλειας

Η δράση στοχεύει στη δημιουργία Εθνικού Μητρώου Ελλήνων Ερευνητών και Εμπειρογνωμόνων Κυβερνοασφάλειας, το οποίο θα συγκεντρώνει και θα καταγράφει τα ερευνητικά προφίλ, τις ειδικότητες και τα πεδία δραστηριοποίησης της ερευνητικής κοινότητας και των ειδικών κυβερνοασφάλειας. Το Μητρώο θα αποτελέσει εργαλείο χαρτογράφησης, συνεργασίας και δικτύωσης μεταξύ ερευνητών, ακαδημαϊκών ιδρυμάτων και φορέων, ενισχύοντας τη συμμετοχή της Ελλάδας σε εθνικές και ευρωπαϊκές πρωτοβουλίες έρευνας και καινοτομίας στην κυβερνοασφάλεια. Παράλληλα θα αποτελέσει την βασική πηγή για τον εντοπισμό τεχνικών εμπειρογνωμόνων (Subject Matter Experts (SMEs) την πιστοποίησή τους και τη συνεργασία τους με την ΕΑΚ για την εισφορά εξειδικευμένης εμπειρογνωμοσύνης που αφορά πληροφοριακά και επικοινωνιακά συστήματα και τεχνολογίες.

1.Γ.5: Δημιουργία Παρατηρητηρίου Επενδύσεων στην Κυβερνοασφάλεια

Σκοπός της δράσης είναι η δημιουργία ενός Εθνικού Παρατηρητηρίου Επενδύσεων στην Κυβερνοασφάλεια, το οποίο θα συλλέγει, αναλύει και δημοσιοποιεί σε περιοδική βάση τεκμηριωμένα τομεακά στοιχεία σχετικά με τις επενδύσεις σε μέτρα ασφάλειας πληροφοριών και ανθεκτικότητας από φορείς του δημόσιου και ιδιωτικού τομέα. Το Παρατηρητήριο θα υποστηρίζει την τεκμηριωμένη λήψη αποφάσεων, την εποπτεία της διενέργειας αναλογικών επενδύσεων βάσει διενέργειας ανάλυσης κινδύνου, την αξιολόγηση πολιτικών έως και την αναθεώρηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας.

1.Γ.6: Δημιουργία Εθνικού Αποθεματικού Κυβερνοασφάλειας με σκοπό τη χρηματοδοτική υποστήριξη έργων και πρωτοβουλιών που ενισχύουν την κυβερνοανθεκτικότητα δημόσιων και ιδιωτικών οντοτήτων

Η δράση αποσκοπεί στη δημιουργία Εθνικού Αποθεματικού Κυβερνοασφάλειας, το οποίο θα λειτουργεί ως μηχανισμός χρηματοδοτικής ενίσχυσης έργων και πρωτοβουλιών που ενδυναμώνουν την κυβερνοανθεκτικότητα, την καινοτομία και το ανθρώπινο δυναμικό στον τομέα της κυβερνοασφάλειας.

Το Ταμείο θα:

- Χρηματοδοτεί έργα ανάπτυξης, υλοποίησης και πιλοτικής εφαρμογής λύσεων κυβερνοασφάλειας, ιδίως σε τεχνολογίες αιχμής όπως η τεχνητή νοημοσύνη, το blockchain και το cloud security.
- Προωθεί συνέργειες μεταξύ δημόσιων οργανισμών, επιχειρήσεων και ερευνητικών φορέων για τη μεταφορά τεχνογνωσίας και την ανάπτυξη καινοτόμων εφαρμογών.
- Ενισχύει προγράμματα εκπαίδευσης και ανάπτυξης δεξιοτήτων, συμβάλλοντας στη βιώσιμη ανάπτυξη του ανθρώπινου δυναμικού κυβερνοασφάλειας.
- Συμβάλλει στη διαμόρφωση οικονομικών κινήτρων για την απασχόληση και διατήρηση εξειδικευμένων στελεχών κυβερνοασφάλειας στον δημόσιο τομέα, ενισχύοντας τη θεσμική και επιχειρησιακή του ικανότητα.

Ειδικός Στόχος 1.Δ: Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας

Ο Ειδικός Στόχος 1.Δ αποσκοπεί στη συγκρότηση ενός ολοκληρωμένου εθνικού πλαισίου ετοιμότητας και απόκρισης σε περιστατικά κυβερνοασφάλειας, που συνδυάζει την ενημέρωση και ευαισθητοποίηση της Κοινωνίας με την ενίσχυση των επιχειρησιακών δομών και μηχανισμών. Περιλαμβάνει τη διαμόρφωση ενιαίας προσέγγισης για την επικοινωνία και διαχείριση περιστατικών, την ανάπτυξη στοχευμένων εκπαιδευτικών εργαλείων για διαφορετικές κατηγορίες φορέων και την υλοποίηση ασκήσεων και προσομοιώσεων σε εθνικό και διατομεακό επίπεδο.

Παράλληλα, ο στόχος αυτός ενισχύει τις εθνικές υπηρεσίες επιχειρησιακού συντονισμού, ανίχνευσης και απόκρισης, καθώς και τις τεχνικές ικανότητες ανάλυσης, δοκιμών και αξιολόγησης τρωτότητας. Από την εκπαίδευση μαθητών και εκπαιδευτικών έως τη λειτουργία εξειδικευμένων δομών και ομάδων απόκρισης, ο Ειδικός Στόχος 1.Δ συμβάλλει στη διαμόρφωση ενός συνεκτικού και διαλειτουργικού οικοσυστήματος, ικανού να ανταποκρίνεται έγκαιρα και αποτελεσματικά σε κρίσεις στον κυβερνοχώρο και να ενισχύει την εμπιστοσύνη των πολιτών και των οργανισμών στον κυβερνοχώρο.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
1.Δ: Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας	1.Δ.1: Εθνικό Σχέδιο Επικοινωνίας και Ευαισθητοποίησης σε Θέματα Κυβερνοασφάλειας
	1.Δ.2: Ανάπτυξη ολοκληρωμένου προγράμματος διενέργειας ασκήσεων με έμφαση στην αντιμετώπιση κρίσεων στο πεδίο εφαρμογής της Οδηγίας NIS2 και της Οδηγίας CER
	1.Δ.3: Κατάρτιση ενημερωτικού και εκπαιδευτικού υλικού (γενικό και ανά κατηγορία Φορέα)
	1.Δ.4: Διαμόρφωση πλαισίου επικοινωνιακής διαχείρισης περιστατικών
	1.Δ.5: Διενέργεια Δράσεων ευαισθητοποίησης σε α' βάθμια και β΄ βάθμια εκπαίδευση
	1.Δ.6: Βελτιστοποίηση της λειτουργίας του gSOC και των mini-SOC
	1.Δ.7: Εργαστήριο Αναλύσεων Δοκιμών και Μελετών Κυβερνοασφάλειας (LAB)
	1.Δ.8: Λειτουργία Ενοποιημένου Κέντρου Αναφοράς Κυβερνοασφάλειας (EL-SOC)
	1.Δ.9: Λειτουργία Ομάδας Απόκρισης Περιστατικών Κυβερνοασφάλειας (CSIRT)
	1.Δ.10: Διεξαγωγή Ελέγχων Τρωτότητας και Ανάλυσης Ευπαθειών

1.Δ.1: Εθνικό Σχέδιο Επικοινωνίας και Ευαισθητοποίησης σε Θέματα Κυβερνοασφάλειας

Η δράση αποσκοπεί στη διαμόρφωση και υλοποίηση ενός ενιαίου Εθνικού Σχεδίου Επικοινωνίας και Ευαισθητοποίησης για την κυβερνοασφάλεια, με στόχο την ενημέρωση πολιτών, επιχειρήσεων και δημόσιων φορέων σχετικά με τις απειλές και τις βέλτιστες πρακτικές ασφάλειας. Το σχέδιο θα περιλαμβάνει εκστρατείες ενημέρωσης, εκπαιδευτικό υλικό και συντονισμένες δράσεις με τα μέσα ενημέρωσης και τους αρμόδιους φορείς.

1.Δ.2: Ανάπτυξη ολοκληρωμένου προγράμματος διενέργειας ασκήσεων με έμφαση στην αντιμετώπιση κρίσεων στο πεδίο εφαρμογής της Οδηγίας NIS2 και της Οδηγίας CER

Η δράση στοχεύει στην ανάπτυξη και υλοποίηση ολοκληρωμένου προγράμματος ασκήσεων κυβερνοασφάλειας, προσανατολισμένου στην ετοιμότητα και διαχείριση περιστατικών και κρίσεων στο πεδίο εφαρμογής των Οδηγιών NIS2 και CER. Το πρόγραμμα θα περιλαμβάνει σενάρια προσομοίωσης, συμμετοχή δημόσιων και ιδιωτικών φορέων και αξιολόγηση των δυνατοτήτων απόκρισης σε εθνικό και διατομεακό επίπεδο.

1.Δ.3: Κατάρτιση ενημερωτικού και εκπαιδευτικού υλικού (γενικό και ανά κατηγορία Φορέα)

Η δράση προβλέπει την ανάπτυξη ολοκληρωμένου εκπαιδευτικού και ενημερωτικού προγράμματος κυβερνοασφάλειας, προσαρμοσμένου σε διαφορετικές ομάδες-στόχο των φορέων του δημόσιου και ιδιωτικού τομέα. Με τη συνεργασία φορέων όπως ο ENISA, τα NSFPs, η ΑΠΔΠΧ, η ΕΕΤΤ, η ΕΥΠ και η Διεύθυνση Δίωξης Κυβερνοεγκλήματος, θα παραχθεί υλικό σε πολλαπλές μορφές (παρουσιάσεις, έντυπα, ηλεκτρονικά μηνύματα, e-learning, FAQ) που θα ενισχύει τη γνώση, την πρόληψη και την υπεύθυνη συμπεριφορά σε θέματα ασφάλειας πληροφοριών. Παράλληλα, προβλέπονται δράσεις εκπαίδευσης εκπαιδευτών, ανάπτυξη hotline υποστήριξης και εφαρμογής online alerting για συνεχή ευαισθητοποίηση και ενίσχυση της κουλτούρας ασφάλειας.

1.Δ.4: Διαμόρφωση πλαισίου επικοινωνιακής διαχείρισης περιστατικών

Η δράση στοχεύει στη διαμόρφωση ενιαίου πλαισίου επικοινωνιακής διαχείρισης σημαντικών περιστατικών και κρίσεων κυβερνοασφάλειας, με στόχο τον έγκαιρο, συντονισμένο και αξιόπιστο τρόπο ενημέρωσης του κοινού και των εμπλεκόμενων φορέων. Το πλαίσιο θα καθορίζει διαδικασίες, ρόλους και πρωτόκολλα επικοινωνίας κατά τη διάρκεια και μετά από σημαντικά περιστατικά, συμβάλλοντας στη διαφάνεια, τη διαχείριση της φήμης και τη διατήρηση της εμπιστοσύνης των πολιτών.

1.Δ.5: Διενέργεια Δράσεων ευαισθητοποίησης σε α' βάθμια και β΄ βάθμια εκπαίδευση

Η δράση αποσκοπεί στη διενέργεια στοχευμένων δράσεων ευαισθητοποίησης για την κυβερνοασφάλεια σε μαθητές και εκπαιδευτικούς της πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης. Μέσω εκπαιδευτικών προγραμμάτων, βιωματικών δραστηριοτήτων και ψηφιακού υλικού, θα προωθηθεί η ασφαλής και υπεύθυνη χρήση του διαδικτύου, συμβάλλοντας στη διαμόρφωση κουλτούρας κυβερνοασφάλειας από νεαρή ηλικία.

1.Δ.6: Βελτιστοποίηση της λειτουργίας του gSOC και των mini-SOC

Η δράση στοχεύει στην ανάπτυξη ενός ολοκληρωμένου και αποδοτικού μοντέλου λειτουργίας για το Κυβερνητικό SOC (gSOC) και τα mini-SOC, με σκοπό την ενίσχυση της κυβερνοανθεκτικότητας και του συντονισμού των φορέων της Κεντρικής Κυβέρνησης. Το λειτουργικό πλαίσιο βασίζεται σε ένα δομημένο σύστημα επιχειρησιακής διαχείρισης της κυβερνοασφάλειας, το οποίο συνδυάζει οργανωτικές, τεχνικές και επιχειρησιακές λειτουργίες.

Οι βασικές ενέργειες περιλαμβάνουν:

- Καθορισμό προτύπου καταγραφής οργανωτικής και τεχνικής κατάστασης: Συστηματική αποτύπωση υποδομών, δεδομένων, ανθρώπινων πόρων και εργαλείων κυβερνοασφάλειας ανά φορέα.

- Αξιολόγηση κινδύνων κυβερνοασφάλειας μέσω κοινής μεθοδολογίας, ώστε να επιτευχθεί ενιαία προσέγγιση στην αναγνώριση, ανάλυση και αντιμετώπιση απειλών.
- Ανάλυση της υφιστάμενης κατάστασης των φορέων, με στόχο τη βελτιστοποίηση της οργανωτικής και λειτουργικής διασύνδεσης του gSOC με τα mini-SOC.
- Καθορισμό λειτουργικού και οργανωτικού μοντέλου για το gSOC και τα mini-SOC, με σαφή προσδιορισμό ρόλων, αρμοδιοτήτων και απαιτούμενων υποδομών.
- Ανάπτυξη τυποποιημένων διαδικασιών λειτουργίας, που θα καλύπτουν την παρακολούθηση, τον εντοπισμό και την απόκριση σε περιστατικά κυβερνοασφάλειας.
- Θέσπιση μηχανισμών επικοινωνίας και συνεργασίας μεταξύ gSOC, mini-SOC και φορέων, για άμεση ανταλλαγή πληροφοριών, βελτίωση της επίγνωσης απειλών και συντονισμένη απόκριση σε περιστατικά.
- Διασύνδεση του gSOC με την υποδομή του EL-SOC.

Η δράση συμβάλει στη διαμόρφωση ενός ενιαίου, διαλειτουργικού οικοσυστήματος ασφάλειας, ενισχύοντας τη συνοχή, την αποτελεσματικότητα και τη δυνατότητα έγκαιρης αντίδρασης σε κυβερνοεπιθέσεις σε εθνικό επίπεδο.

1.Δ.7: Εργαστήριο Αναλύσεων Δοκιμών και Μελετών Κυβερνοασφάλειας (LAB)

Λειτουργία Εργαστηρίου Αναλύσεων, Δοκιμών και Μελετών Κυβερνοασφάλειας (LAB) για την υποστήριξη της ΕΑΚ σε εξειδικευμένες τεχνικές και ερευνητικές δραστηριότητες. Το εργαστήριο θα παρέχει δυνατότητες προσομοίωσης και δοκιμών κυβερνοεπιθέσεων, αξιολόγησης τεχνολογικών λύσεων, ανάλυσης κακόβουλου λογισμικού, καθώς και εκπόνησης μελετών και τεχνικών αξιολογήσεων σε θέματα ασφάλειας πληροφοριακών συστημάτων. Παράλληλα, θα λειτουργεί ως κόμβος τεχνογνωσίας για την υποστήριξη πολιτικών, κανονιστικών παρεμβάσεων και αναπτυξιακών δράσεων, ενισχύοντας την τεχνική ικανότητα και την επιχειρησιακή ετοιμότητα της ΕΑΚ.

1.Δ.8: Λειτουργία Ενοποιημένου Κέντρου Αναφοράς Κυβερνοασφάλειας (EL-SOC)

Συνέχιση της ανάπτυξης και επιχειρησιακής υλοποίησης του Ενοποιημένου Κέντρου Αναφοράς Κυβερνοασφάλειας στην Εθνική Αρχή Κυβερνοασφάλειας, όπως προβλέπεται στο άρθρο 31 του ν. 5002/2022, το οποίο αποτελεί το μοναδικό σημείο σε εθνικό επίπεδο για τη συγκέντρωση της πληροφορίας από το Εθνικό Δίκτυο SOC και υλοποιεί τις απαιτήσεις του Κανονισμού (ΕΕ) Cyber Solidarity Act.

1.Δ.9: Λειτουργία Ομάδας Απόκρισης Περιστατικών Κυβερνοασφάλειας (CSIRT)

Λειτουργία της Ομάδας Απόκρισης Περιστατικών Κυβερνοασφάλειας (CSIRT) της ΕΑΚ, με αρμοδιότητα την παρακολούθηση, ανίχνευση, ανάλυση και αντιμετώπιση κυβερνοπεριστατικών που επηρεάζουν φορείς του δημόσιου και ιδιωτικού τομέα. Η δράση περιλαμβάνει τη διαρκή αναβάθμιση του CSIRT της ΕΑΚ, την ενίσχυση της επιχειρησιακής του ετοιμότητας, τη διαχείριση αναφορών περιστατικών, την παροχή άμεσης τεχνικής υποστήριξης και καθοδήγησης, τη διενέργεια ψηφιακών αναλύσεων, καθώς και την έκδοση προειδοποιήσεων, οδηγιών και τεχνικών ανακοινώσεων.

1.Δ.10: Διεξαγωγή Ελέγχων Τρωτότητας και Ανάλυσης Ευπαθειών

Διενέργεια στοχευμένων ελέγχων σε φορείς του δημόσιου και ιδιωτικού τομέα, με έμφαση στις Βασικές Οντότητες (Essential Entities) και τις Σημαντικές Οντότητες (Important Entities) όπως

ορίζονται στο ν. 5160/2024. Οι επιθεωρήσεις και οι έλεγχοι (τακτικοί ή έκτακτοι) αφορούν στην αξιολόγηση της συμμόρφωσης με τις απαιτήσεις κυβερνοασφάλειας, μέσω επιτόπιων ή/και απομακρυσμένων αξιολογήσεων, εξέτασης τεκμηρίωσης, και ανάλυσης των τεχνικών και οργανωτικών μέτρων που έχουν υλοποιηθεί. Η δράση περιλαμβάνει τη σύνταξη αναφορών ευρημάτων, συστάσεων και απαιτούμενων διορθωτικών ενεργειών, με στόχο την έγκαιρη αναγνώριση κινδύνων, την ενίσχυση της εφαρμογής βέλτιστων πρακτικών και την επιβολή ποινών και προστίμων σε περιπτώσεις μη συμμόρφωσης.

Στρατηγικός Στόχος 2: Ενίσχυση της Εθνικής, Ευρωπαϊκής και Διεθνούς Συνεργασίας

Ο Στρατηγικός Στόχος 2 αποσκοπεί στη συγκρότηση ενός συνεκτικού πλαισίου συνεργασίας σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο, που ενισχύει την ικανότητα της χώρας να προλαμβάνει, να αποτρέπει και να αντιμετωπίζει σύνθετες κυβερνοαπειλές. Βασίζεται στην αρχή ότι η κυβερνοασφάλεια είναι συλλογική ευθύνη και απαιτεί ισχυρές συμμαχίες μεταξύ κρατικών αρχών, οργανισμών επιβολής του νόμου, ρυθμιστικών φορέων, διεθνών οργανισμών και του ιδιωτικού τομέα.

Μέσα από την ανάπτυξη αξιόπιστων μηχανισμών ανταλλαγής πληροφοριών, αμοιβαίας συνδρομής και κοινής δράσης, ο στόχος αυτός ενισχύει τη θέση της Ελλάδας ως υπεύθυνου και ενεργού εταίρου στα ευρωπαϊκά και διεθνή οικοσυστήματα κυβερνοασφάλειας. Ταυτόχρονα, συμβάλλει στην προστασία των θεμελιωδών δικαιωμάτων στον κυβερνοχώρο, στην ενίσχυση της εμπιστοσύνης στην ψηφιακή οικονομία και στη σύγκλιση με τα πιο ώριμα κράτη-μέλη της ΕΕ ως προς την κυβερνοανθεκτικότητα.

Ειδικός Στόχος 2.Α: Ενίσχυση των Μηχανισμών Πρόληψης και Αντιμετώπισης του Κυβερνοεγκλήματος

Ο Ειδικός Στόχος 2.Α επικεντρώνεται στη συστηματική ενίσχυση της ικανότητας της χώρας να προλαμβάνει, να διερευνά και να αντιμετωπίζει αποτελεσματικά το κυβερνοέγκλημα, αξιοποιώντας σύγχρονα εργαλεία, μεθοδολογίες και τεχνολογικές λύσεις. Στοχεύει στην αναβάθμιση του επιχειρησιακού ρόλου των αρχών επιβολής του νόμου, την ενίσχυση των δυνατοτήτων ψηφιακής έρευνας και ανάλυσης, καθώς και στην κατανόηση νέων μορφών ψηφιακής εγκληματικότητας, όπως το λυτρισμικό (ransomware) και τα deepfakes.

Μέσω της ανάπτυξης εξειδικευμένων πολιτικών, σχεδίων δράσης και προγραμμάτων εκπαίδευσης για αστυνομικούς, εισαγγελείς και δικαστές, ο στόχος αυτός ενδυναμώνει τον θεσμικό και επιχειρησιακό ιστό του κράτους δικαίου στον ψηφιακό χώρο. Παράλληλα, προωθεί την ευθυγράμμιση με τις ευρωπαϊκές και διεθνείς βέλτιστες πρακτικές, ενισχύοντας την αποτρεπτική ικανότητα της χώρας και την προστασία πολιτών, επιχειρήσεων και δημοκρατικών θεσμών από εξελισσόμενες μορφές κυβερνοεγκλήματος.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
2.Α: Ενίσχυση των Μηχανισμών Πρόληψης και Αντιμετώπισης του Κυβερνοεγκλήματος	2.Α.1: Αξιοποίηση σύγχρονων εργαλείων, τεχνικών και μηχανισμών συνεργασίας για την πάταξη του κυβερνοεγκλήματος
	2.Α.2: Ανάπτυξη και υλοποίηση προγραμμάτων εκπαίδευσης για στελέχη επιβολής του νόμου (όπως αστυνομικούς, εισαγγελείς και δικαστές) σε θέματα που αφορούν το κυβερνοέγκλημα

	2.Α.3: Επικαιροποίηση πολιτικής αντιμετώπισης του Λυτρισμικού (Ransomware) για το γενικό πληθυσμό
	2.Α.4: Ανάπτυξη Σχεδίου Δράσης για την Αντιμετώπιση Επιθέσεων μέσω Deepfakes

2.Α.1: Δημιουργία και αξιοποίηση σύγχρονων εργαλείων και τεχνικών για την πάταξη του κυβερνοεγκλήματος

Η παρούσα δράση αφορά την ενίσχυση των δυνατοτήτων των αρμόδιων αρχών για την πρόληψη, την ανίχνευση και την αντιμετώπιση του κυβερνοεγκλήματος μέσω της συστηματικής αξιοποίησης σύγχρονων εργαλείων ψηφιακής έρευνας, τεχνικών ανάλυσης πληροφοριών και επιχειρησιακών συστημάτων υποστήριξης. Ιδιαίτερη έμφαση δίνεται στην αναβάθμιση των επιχειρησιακών δυνατοτήτων των υπηρεσιών πρώτης γραμμής, με στόχο τη βελτίωση της ταχύτητας ανταπόκρισης, της ακρίβειας της διερεύνησης και της αποτελεσματικότητας της καταστολής. Παράλληλα, η δράση εστιάζει στην ενδυνάμωση των μηχανισμών συνεργασίας τόσο σε επιχειρησιακό επίπεδο, μέσω κοινών επιχειρήσεων, ανταλλαγής επιχειρησιακών δεδομένων και συντονισμένων δράσεων, όσο και σε στρατηγικό επίπεδο, μέσω μόνιμων δομών συνεργασίας, κοινών σχεδιασμών, ανταλλαγής βέλτιστων πρακτικών και συμμετοχής σε ευρωπαϊκά και διεθνή δίκτυα. Η διττή αυτή προσέγγιση επιδιώκει να ενισχύσει τη συνολική ανθεκτικότητα της χώρας απέναντι στις σύγχρονες κυβερνοαπειλές.

2.Α.2: Ανάπτυξη και υλοποίηση προγραμμάτων εκπαίδευσης για στελέχη επιβολής του νόμου (όπως αστυνομικούς, εισαγγελείς και δικαστές) σε θέματα που αφορούν το κυβερνοέγκλημα

Η δράση αφορά στην ανάπτυξη και υλοποίηση εξειδικευμένων προγραμμάτων εκπαίδευσης και επιμόρφωσης για στελέχη επιβολής του νόμου, όπως αστυνομικούς, εισαγγελικούς λειτουργούς και δικαστές, σε αντικείμενα που άπτονται του κυβερνοεγκλήματος και της ψηφιακής εγκληματολογίας. Στόχος της δράσης είναι η ενίσχυση των γνώσεων και των δεξιοτήτων τους τόσο στο τεχνικό όσο και στο νομικό σκέλος της διερεύνησης, ώστε να διασφαλίζεται η αποτελεσματική αντιμετώπιση σύνθετων ψηφιακών υποθέσεων και η ορθή απονομή της δικαιοσύνης. Η δράση προβλέπει την αξιοποίηση ευρωπαϊκών και διεθνών δομών εκπαίδευσης, όπως η CEPOL (European Union Agency for Law Enforcement Training), καθώς και η συνεργασία με πανεπιστημιακά ιδρύματα, ερευνητικά κέντρα και εξειδικευμένους φορείς κυβερνοασφάλειας. Παράλληλα, δίνεται έμφαση στη διοργάνωση κοινών σεμιναρίων, εργαστηρίων και ασκήσεων προσομοίωσης, τόσο σε εθνικό όσο και σε διεθνές επίπεδο, με στόχο τη συνεχή επικαιροποίηση των γνώσεων, την ανταλλαγή βέλτιστων πρακτικών και την ενίσχυση της διαλειτουργικότητας μεταξύ των εμπλεκόμενων αρχών.

2.Α.3: Επικαιροποίηση πολιτικής αντιμετώπισης του Λυτρισμικού (Ransomware) για το γενικό πληθυσμό (Ransomware) για το γενικό πληθυσμό

Η δράση αφορά στη διαμόρφωση και συνεχή επικαιροποίηση ενός ολοκληρωμένου πλαισίου πολιτικής για την πρόληψη και αντιμετώπιση επιθέσεων λυτρισμικού (ransomware), με έμφαση στην προστασία του γενικού πληθυσμού. Στόχος της είναι η ενίσχυση της ψηφιακής εγρήγορσης και της ανθεκτικότητας

των πολιτών απέναντι στις σύγχρονες μορφές ψηφιακού εκβιασμού, μέσα από στοχευμένες δράσεις ενημέρωσης, καμπάνιες ευαισθητοποίησης, παροχή πρακτικών οδηγιών αυτοπροστασίας και διάχυση αξιόπιστης, επικαιροποιημένης πληροφόρησης. Η δράση ενισχύεται μέσω της αξιοποίησης διεθνών πρωτοβουλιών και συνεργασιών, όπως το Project “No More Ransom”, το οποίο προσφέρει δωρεάν εργαλεία αποκρυπτογράφησης, ενημέρωση για ενεργές απειλές και καθοδήγηση προς τα θύματα ransomware. Παράλληλα, προβλέπεται η διασύνδεση με λοιπές ευρωπαϊκές και διεθνείς πρωτοβουλίες, με στόχο την έγκαιρη προειδοποίηση, τη συνεχή επικαιροποίηση της πληροφόρησης και την ενίσχυση των δυνατοτήτων πρόληψης.

2.Α.4: Ανάπτυξη Σχεδίου Δράσης για την Αντιμετώπιση Επιθέσεων μέσω Deepfakes

Η δράση αποσκοπεί στην ανάπτυξη ενός ολοκληρωμένου Σχεδίου Δράσης για την πρόληψη, ανίχνευση και αντιμετώπιση επιθέσεων που αξιοποιούν τεχνολογίες δημιουργίας παραποιημένου ψηφιακού περιεχομένου (deepfakes). Το Σχέδιο Δράσης θα καθορίζει τις βασικές αρχές, μηχανισμούς και διαδικασίες που απαιτούνται για την προστασία οργανισμών, δημόσιων φορέων και της κοινωνίας από επιθέσεις παραπληροφόρησης, εξαπάτησης, χειραγώγησης ή υποκλοπής ταυτότητας που βασίζονται σε προηγμένες τεχνικές τεχνητής νοημοσύνης.

Η δράση περιλαμβάνει τον προσδιορισμό απαιτήσεων για τεχνολογίες ανίχνευσης παραποιημένου περιεχομένου, την ανάπτυξη πρωτοκόλλων συνεργασίας μεταξύ αρμόδιων φορέων, καθώς και την καλλιέργεια ικανοτήτων έγκαιρης αναγνώρισης και διαχείρισης σχετικών περιστατικών. Παράλληλα, προωθεί την ευθυγράμμιση με ευρωπαϊκές κατευθύνσεις και διεθνείς βέλτιστες πρακτικές, συμβάλλοντας στη θωράκιση του θεσμικού πλαισίου και στη διασφάλιση της εμπιστοσύνης στην ψηφιακή επικοινωνία και ενημέρωση.

Ειδικός Στόχος 2.Β: Ενίσχυση της Ευρωπαϊκής και Διεθνούς Συνεργασίας

Ο Ειδικός Στόχος 2.Β στοχεύει στη διαμόρφωση μιας σαφούς, συνεκτικής και προδραστικής εθνικής στάσης στο διεθνές περιβάλλον κυβερνοασφάλειας. Προβλέπει τη θέσπιση ειδικότερης στρατηγικής διεθνούς συνεργασίας, η οποία καθοδηγεί τη συμμετοχή της Ελλάδας σε ευρωπαϊκά και διεθνή φόρα, οργανισμούς και πρωτοβουλίες, και ενισχύει τους μηχανισμούς διαμόρφωσης και εκπροσώπησης εθνικών θέσεων.

Με την ενίσχυση της εξωστρέφειας της ΕΑΚ και την ενεργό συμμετοχή της σε δίκτυα, ομάδες εργασίας και πολιτικές διαδικασίες, ο στόχος αυτός συμβάλλει στην αναβάθμιση του ρόλου της Ελλάδας ως αξιόπιστου εταίρου στον ευρωπαϊκό και διεθνή διάλογο. Η ευθυγράμμιση με την Στρατηγική Κυβερνοασφάλειας της ΕΕ για την Ψηφιακή Δεκαετία, σε συνδυασμό με την ανάδειξη εθνικών προτεραιοτήτων, ενισχύει τη συλλογική κυβερνοανθεκτικότητα και υποστηρίζει την προστασία κρίσιμων αλυσίδων αξίας και στρατηγικών υποδομών.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
2.Β: Ενίσχυση της Ευρωπαϊκής και Διεθνούς Συνεργασίας	2.Β.1: Θέσπιση Στρατηγικής για τη Διεθνή Συνεργασία σε Θέματα Κυβερνοασφάλειας

	2.Β.2: Ενίσχυση της Εξωστρέφειας και της Διεθνούς Παρουσίας της ΕΑΚ
	2.Β.3: Ενίσχυση Συνεργασίας στο πλαίσιο διαμόρφωσης της Ευρωπαϊκής Πολιτικής Κυβερνοασφάλειας

2.Β.1: Θέσπιση Στρατηγικής για τη Διεθνή Συνεργασία σε Θέματα Κυβερνοασφάλειας

Η δράση αποσκοπεί στη θέσπιση ειδικότερης στρατηγικής προσέγγισης για τη διεθνή συνεργασία στην Κυβερνοασφάλεια, με σκοπό την καθοδήγηση της συμμετοχής της χώρας σε ευρωπαϊκές και διεθνείς πρωτοβουλίες, καθώς και την ανάπτυξη ενός εθνικού μηχανισμού διαμόρφωσης και εκπροσώπησης εθνικών θέσεων.

Η στρατηγική θα:

- Καθορίσει το πλαίσιο ουσιαστικής ενίσχυσης συμμετοχής της Ελλάδας στον τομέα της κυβερνοασφάλειας σε διεθνείς πρωτοβουλίες και οργανισμούς, όπως ο ΟΗΕ, ο ΟΟΣΑ, το ΝΑΤΟ, ο ΟΑΣΕ και η ΕΕ.
- Θεσπίσει μηχανισμό διαβούλευσης και διαμόρφωσης εθνικών θέσεων, που θα συντονίζει όλους τους συναρμόδιους φορείς για την εκπροσώπηση της χώρας σε ευρωπαϊκά και διεθνή φόρα κυβερνοασφάλειας.
- Εναρμονιστεί με την ευρωπαϊκή στρατηγική κυβερνοασφάλειας και τις προτεραιότητες της Ψηφιακής Δεκαετίας, προωθώντας τη συνεργασία για τη συλλογική κυβερνοανθεκτικότητα και την ασφάλεια κρίσιμων αλυσίδων αξίας.
- Ενισχύσει τη διπλωματική παρουσία της Ελλάδας στον κυβερνοχώρο, μέσω της συστηματικής εκπροσώπησης σε διεθνείς διαπραγματεύσεις, ομάδες εργασίας και μηχανισμούς ανάπτυξης πολιτικής.

Η δράση συμβάλλει στην ενίσχυση του ρόλου της Ελλάδας ως αξιόπιστου και ενεργού εταίρου στον ευρωπαϊκό και διεθνή διάλογο για την κυβερνοασφάλεια, ενισχύοντας παράλληλα τη συνοχή και στρατηγική καθοδήγηση της εθνικής συμμετοχής.

2.Β.2: Ενίσχυση της Εξωστρέφειας και της Διεθνούς Παρουσίας της ΕΑΚ

Η δράση αποσκοπεί στην ενίσχυση της εξωστρέφειας και της διεθνούς παρουσίας της ΕΑΚ μέσω της ενεργού συμμετοχής σε συνέδρια, φόρουμ και συναντήσεις υψηλού επιπέδου, καθώς και μέσω της διοργάνωσης θεματικών εκδηλώσεων σε εθνικό και διεθνές επίπεδο. Στο πλαίσιο αυτό, η ΕΑΚ θα αναπτύσσει πρωτοβουλίες που ενισχύουν τη συνεργασία και τη δικτύωση μεταξύ φορέων, υποστηρίζουν την ανταλλαγή βέλτιστων πρακτικών και προβάλλουν τον ρόλο της Ελλάδας στο διεθνές οικοσύστημα κυβερνοασφάλειας. Η δράση συμβάλλει στη διεύρυνση της εθνικής κοινότητας κυβερνοασφάλειας και στην ενίσχυση της συμμετοχής της χώρας σε διεθνείς στρατηγικές πρωτοβουλίες.

2.Β.3: Ενίσχυση Συνεργασίας στο πλαίσιο διαμόρφωσης της Ευρωπαϊκής Πολιτικής Κυβερνοασφάλειας

Ενίσχυση των συνεργασιών της ΕΑΚ σε ευρωπαϊκό και διεθνές επίπεδο, μέσω της συστηματικής συμμετοχής σε θεσμικά όργανα, ομάδες εργασίας και δίκτυα αλλά και διεθνείς οργανισμούς, οι οποίοι συμβάλλουν στη διαμόρφωση της ευρωπαϊκής και διεθνούς πολιτικής κυβερνοασφάλειας.

Ειδικός Στόχος 2.Γ: Θέσπιση Αξιόπιστων Μηχανισμών Ανταλλαγής Πληροφοριών

Ο Ειδικός Στόχος 2.Γ επικεντρώνεται στη δημιουργία και λειτουργία αξιόπιστων, ασφαλών και διαλειτουργικών μηχανισμών ανταλλαγής πληροφοριών για την αντιμετώπιση των κυβερνοαπειλών. Στοχεύει στη συγκρότηση ενός εθνικού κόμβου πληροφόρησης (Cyber Threat Intelligence Hub), ο οποίος θα συγκεντρώνει, αναλύει και θα διαχέει έγκαιρα και χρήσιμα δεδομένα σχετικά με απειλές, ευπάθειες και περιστατικά, προς δημόσιους και ιδιωτικούς φορείς.

Μέσω της διασύνδεσης με ευρωπαϊκές και διεθνείς πλατφόρμες ανταλλαγής πληροφοριών, ο στόχος αυτός ενισχύει την εμπιστοσύνη μεταξύ των ενδιαφερόμενων μερών και διευκολύνει τον συντονισμένο, τεκμηριωμένο και έγκαιρο τρόπο λήψης αποφάσεων σε περιβάλλον αυξημένης αβεβαιότητας.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
2.Γ: Θέσπιση Αξιόπιστων Μηχανισμών Ανταλλαγής Πληροφοριών	2.Γ.1: Πλατφόρμα διαμοιρασμού πληροφοριών περί απειλών (threat intelligence)

2.Γ.1: Πλατφόρμα διαμοιρασμού πληροφοριών περί απειλών (threat intelligence)

Η δράση στοχεύει στη δημιουργία ενός εθνικού κόμβου πληροφόρησης για απειλές στον κυβερνοχώρο (Cyber Threat Intelligence Hub) για τη συγκέντρωση, ανάλυση και ανταλλαγή έγκαιρων και αξιόπιστων πληροφοριών σχετικά με ψηφιακές απειλές, ευπάθειες και περιστατικά. Ο κόμβος θα λειτουργεί ως πλατφόρμα διαμοιρασμού threat intelligence μεταξύ οργανισμών και παρόχων κρίσιμων υπηρεσιών, ενισχύοντας τον συντονισμό και την ικανότητα έγκαιρης απόκρισης σε αναδυόμενες απειλές. Παράλληλα, θα διασφαλίζεται η διαλειτουργικότητα με ευρωπαϊκές και διεθνείς πλατφόρμες ανταλλαγής πληροφοριών, προάγοντας την εμπιστοσύνη, τη συνεργασία και την ενίσχυση της συλλογικής κυβερνοανθεκτικότητας της χώρας.

Ειδικός Στόχος 2.Δ: Θέσπιση Διαδικασιών Αμοιβαίας Συνδρομής

Ο Ειδικός Στόχος 2.Δ αποσκοπεί στην εγκαθίδρυση σαφών, εφαρμόσιμων και αποτελεσματικών διαδικασιών αμοιβαίας συνδρομής μεταξύ των εμπλεκόμενων φορέων, με ιδιαίτερη έμφαση στις ανάγκες των Οργανισμών Τοπικής Αυτοδιοίκησης. Αντιμετωπίζει την κυβερνοασφάλεια ως κοινή υπόθεση, διασφαλίζοντας ότι οι φορείς με μικρότερη ωριμότητα ή περιορισμένους πόρους δεν μένουν εκτεθειμένοι, αλλά υποστηρίζονται για να αναπτύξουν βασικές ικανότητες προστασίας και απόκρισης.

Μέσω της ενίσχυσης των δεξιοτήτων, των διαδικασιών και των μηχανισμών υποστήριξης των ΟΤΑ, ο στόχος αυτός συμβάλλει στην προστασία των τοπικών ψηφιακών υποδομών και υπηρεσιών, που συνδέονται άμεσα με την καθημερινότητα των πολιτών. Ταυτόχρονα, ενδυναμώνει τον εθνικό ιστό

κυβερνοασφάλειας, δημιουργώντας ένα πολυεπίπεδο σύστημα αλληλοβοήθειας, όπου η εμπειρία, η τεχνογνωσία και οι πόροι μπορούν να κινητοποιούνται συντονισμένα σε περιπτώσεις κρίσεων ή σοβαρών περιστατικών.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
2.Δ: Θέσπιση Διαδικασιών Αμοιβαίας Συνδρομής	2.Δ.1: Ενίσχυση Κυβερνοανθεκτικότητας ΟΤΑ

2.Δ.1: Ενίσχυση Κυβερνοανθεκτικότητας ΟΤΑ

Η δράση αποσκοπεί στην ουσιαστική ενίσχυση της κυβερνοανθεκτικότητας των Οργανισμών Τοπικής Αυτοδιοίκησης (ΟΤΑ) σε τοπικό και περιφερειακό επίπεδο, μέσα από την ανάπτυξη των αναγκαίων δεξιοτήτων, ικανοτήτων και βασικών διαδικασιών κυβερνοασφάλειας. Στοχεύει στη δημιουργία ενός ώριμου και σταθερού πλαισίου προστασίας για τις ψηφιακές υποδομές και τα δεδομένα των ΟΤΑ, ενισχύοντας την ικανότητά τους να προλαμβάνουν, να ανιχνεύουν και να αντιμετωπίζουν απειλές. Με τον τρόπο αυτό, οι τοπικές αρχές αποκτούν τα θεμελιώδη εργαλεία και τη γνώση που απαιτούνται για να ανταποκριθούν αποτελεσματικά στις σύγχρονες προκλήσεις κυβερνοασφάλειας, συμβάλλοντας στη συνολική ψηφιακή ασφάλεια και ανθεκτικότητα των τοπικών κοινοτήτων.

Στρατηγικός Στόχος 3: Ένα σύστημα διακυβέρνησης της κυβερνοασφάλειας για το σύνολο της κοινωνίας

Ο Στρατηγικός Στόχος 3 αποσκοπεί στη διαμόρφωση ενός ολοκληρωμένου, συνεκτικού και διαφανούς συστήματος διακυβέρνησης της κυβερνοασφάλειας, το οποίο καλύπτει το σύνολο της Δημόσιας Διοίκησης, των κρίσιμων υποδομών, της αγοράς και της Κοινωνίας. Εδράζεται σε σαφείς ρόλους, θεσμικούς μηχανισμούς συντονισμού, τυποποιημένες διαδικασίες διαχείρισης κινδύνων και κρίσεων, καθώς και σε ισχυρά εργαλεία εποπτείας και συμμόρφωσης, ώστε οι πολιτικές και τα μέτρα κυβερνοασφάλειας να εφαρμόζονται με συνέπεια και λογοδοσία.

Μέσα από την ανάπτυξη εθνικών πλαισίων εκτίμησης κινδύνων, την ενίσχυση της εθνικής διακυβέρνησης, τη θέσπιση εξειδικευμένων μέτρων για κρίσιμες τεχνολογίες και τη δημιουργία αποτελεσματικών μηχανισμών αναφοράς περιστατικών, ο στόχος αυτός διασφαλίζει ότι η κυβερνοασφάλεια δεν αποτελεί αποσπασματική τεχνική λειτουργία, αλλά θεμελιώδες στοιχείο ενός σύγχρονου κράτους δικαίου, της οικονομικής ανάπτυξης και της προστασίας των θεμελιωδών δικαιωμάτων στον κυβερνοχώρο.

Ειδικός Στόχος 3.Α: Ανάπτυξη Πλαισίων Διαχείρισης Κρίσεων Κυβερνοασφάλειας

Ο Ειδικός Στόχος 3.Α επικεντρώνεται στη δημιουργία και θεσμοθέτηση ολοκληρωμένων πλαισίων διαχείρισης κρίσεων κυβερνοασφάλειας, τα οποία διασφαλίζουν ότι η χώρα μπορεί να ανταποκριθεί συντονισμένα και αποτελεσματικά σε περιστατικά μεγάλης κλίμακας. Περιλαμβάνει την ενσωμάτωση της επιχειρησιακής συνέχειας και της ανάκαμψης από καταστροφές στον σχεδιασμό των κρίσιμων φορέων, καθώς και την ανάπτυξη εθνικών σχεδίων και μηχανισμών αντιμετώπισης κυβερνοκρίσεων που συνδέονται με τα ευρωπαϊκά και διεθνή δίκτυα συνεργασίας.

Με τη συστηματική διενέργεια ασκήσεων, την αποσαφήνιση ρόλων και αρμοδιοτήτων και την ευθυγράμμιση με το κανονιστικό πλαίσιο, όπως ιδίως ο ν. 5160/2024, ο στόχος αυτός ενισχύει την ετοιμότητα της χώρας να προστατεύει κρίσιμες λειτουργίες, να περιορίζει επιπτώσεις και να αποκαθιστά γρήγορα την ομαλή λειτουργία της κοινωνίας και της οικονομίας.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
3.Α: Ανάπτυξη Πλαισίων Διαχείρισης Κρίσεων Κυβερνοασφάλειας	3.Α.1: Ενίσχυση επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές
	3.Α.2: Εθνικός σχεδιασμός διαχείρισης κρίσεων

3.Α.1: Ενίσχυση επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές

Η δράση στοχεύει στην ανάπτυξη και εφαρμογή ενιαίων σχεδίων επιχειρησιακής συνέχειας (Business Continuity Plans – BCP) και σχεδίων ανάκαμψης από καταστροφές (Disaster Recovery Plans – DRP) για οργανισμούς που παρέχουν κρίσιμες υπηρεσίες, με σκοπό τη διασφάλιση της αδιάλειπτης λειτουργίας τους σε περιπτώσεις έκτακτης ανάγκης, όπως κυβερνοεπιθέσεις ή φυσικές καταστροφές.

Περιλαμβάνει τη θέσπιση πλαισίου ασκήσεων προσομοίωσης για την αξιολόγηση της ετοιμότητας και της ανθεκτικότητας οργανισμών, καθώς και τη δημιουργία κεντρικού κόμβου επιχειρησιακής συνέχειας και διαχείρισης κρίσεων, ο οποίος θα παρέχει τεχνική υποστήριξη, δυνατότητες προσωρινής φιλοξενίας κρίσιμων λειτουργιών και ασφαλή ανάκτηση δεδομένων. Μέσω αυτών των δράσεων ενισχύεται η συνολική κυβερνοανθεκτικότητα και η ικανότητα έγκαιρης αποκατάστασης κρίσιμων λειτουργιών σε εθνικό επίπεδο.

3.Α.2: Εθνικός σχεδιασμός διαχείρισης κρίσεων

Η δράση αποσκοπεί στην εκπόνηση Εθνικού Σχεδίου αντιμετώπισης περιστατικών μεγάλης κλίμακας και κρίσεων στον κυβερνοχώρο, το οποίο θα διασφαλίζει τον συντονισμένο και έγκαιρο χειρισμό κρίσεων μεγάλης κλίμακας που επηρεάζουν κρίσιμες υπηρεσίες, υποδομές ή ακόμη και πτυχές της εθνικής ασφάλειας.

Το σχέδιο θα:

- Καθορίζει ρόλους, διαδικασίες και αρμοδιότητες όλων των εμπλεκόμενων φορέων (δημόσιων και ιδιωτικών), εξασφαλίζοντας αποτελεσματικό συντονισμό και επικοινωνία σε περιπτώσεις έκτακτων περιστατικών.
- Περιλαμβάνει εθνικό μηχανισμό απόκρισης σε κυβερνοκρίσεις, με σαφείς γραμμές εντολών, ιεραρχία αποφάσεων και διασύνδεση με τα ευρωπαϊκά και διεθνή δίκτυα συνεργασίας (π.χ. δίκτυο CSIRT, CyCLONe, ENISA, ΕΕ).
- Ενσωματώνει διαδικασίες προσομοίωσης και ασκήσεων ετοιμότητας, ώστε να αξιολογείται και να ενισχύεται η επιχειρησιακή ετοιμότητα των εμπλεκόμενων φορέων.
- Ευθυγραμμίζεται με τις απαιτήσεις του ν. 5160/2024, διασφαλίζοντας ενιαία και συνεκτική διαχείριση κυβερνοκρίσεων σε εθνικό επίπεδο.
- Ευθυγραμμίζεται με τις αντίστοιχες διαδικασίες διαχείρισης κρίσεων σε ευρωπαϊκό επίπεδο.

Ειδικός Στόχος 3.Β: Ασφαλής Ψηφιακή Ταυτότητα και Εμπιστοσύνη στις Δημόσιες Ψηφιακές Υπηρεσίες

Ο Ειδικός Στόχος 3.Β αποσκοπεί στη θωράκιση της αξιοπιστίας και της ασφάλειας των δημόσιων ψηφιακών υπηρεσιών, ενισχύοντας την εμπιστοσύνη πολιτών και επιχειρήσεων στο ψηφιακό κράτος. Εστιάζει στη συστηματική αναβάθμιση της προστασίας κυβερνητικών ψηφιακών υποδομών, στην υιοθέτηση ενιαίων πολιτικών ασφάλειας και στην εφαρμογή σύγχρονων τεχνικών μηχανισμών που διασφαλίζουν τη διαθεσιμότητα, την ακεραιότητα και την εμπιστευτικότητα των υπηρεσιών.

Με την κεντρική οργάνωση της προστασίας κρίσιμων ψηφιακών σημείων επαφής με τον πολίτη, ο στόχος αυτός συμβάλλει στην ενδυνάμωση της ψηφιακής ταυτότητας του Δημοσίου, στην αποτροπή περιστατικών που πλήττουν τη δημόσια εικόνα και στην εμπέδωση της αντίληψης ότι οι ψηφιακές υπηρεσίες του κράτους αποτελούν ασφαλές και αξιόπιστο κανάλι συναλλαγών.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
3.Β: Ασφαλής Ψηφιακή Ταυτότητα και Εμπιστοσύνη στις Δημόσιες Ψηφιακές Υπηρεσίες	3.Β.1: Αναβάθμιση προστασίας κυβερνητικών ιστοτόπων

3.Β.1: Αναβάθμιση προστασίας κυβερνητικών ιστοτόπων

Η δράση αποσκοπεί στην αναβάθμιση και κεντρική διαχείριση της προστασίας κυβερνητικών ιστοτόπων, με στόχο την ενίσχυση της ασφάλειας, τη διασφάλιση της διαθεσιμότητας και της αξιοπιστίας τους. Περιλαμβάνει την εφαρμογή σύγχρονων μηχανισμών, όπως Web Application Firewalls, προστασία από DDoS επιθέσεις, ισχυρή κρυπτογράφηση επικοινωνιών και συνεχή παρακολούθηση απειλών. Παράλληλα, θεσπίζει ενιαίες πολιτικές ασφάλειας και διαδικασίες άμεσης απόκρισης, ενισχύοντας την εμπιστοσύνη των πολιτών στις ψηφιακές υπηρεσίες του Δημοσίου.

Ειδικός Στόχος 3.Γ: Θέσπιση Εθνικού Πλαισίου Εκτίμησης Κινδύνων Κυβερνοασφάλειας

Ο Ειδικός Στόχος 3.Γ στοχεύει στη δημιουργία ενός ενοποιημένου και τεκμηριωμένου πλαισίου εκτίμησης κινδύνων κυβερνοασφάλειας σε εθνικό επίπεδο. Προβλέπει την παραγωγή τακτικών αναφορών για το τοπίο απειλών, την καταγραφή των εθνικών πληροφοριακών πόρων και υποδομών, καθώς και την εκπόνηση ολοκληρωμένης Εθνικής Εκτίμησης Κινδύνων που θα καθοδηγεί τις στρατηγικές προτεραιότητες και τις επενδύσεις.

Με την αξιοποίηση δεδομένων από επιχειρησιακούς μηχανισμούς, τη συνεργασία με αρμόδιους φορείς και την ενσωμάτωση διεθνών μεθοδολογιών, ο στόχος αυτός ενισχύει τη στρατηγική επίγνωση της χώρας. Επιτρέπει τη στοχευμένη λήψη μέτρων πρόληψης και απόκρισης, εξασφαλίζοντας ότι οι πολιτικές κυβερνοασφάλειας βασίζονται σε αντικειμενικά στοιχεία, ανάλυση σεναρίων και σαφή κατανόηση των κινδύνων για κρίσιμες υποδομές, υπηρεσίες και την κοινωνία.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
3.Γ: Θέσπιση Εθνικού Πλαισίου Εκτίμησης Κινδύνων Κυβερνοασφάλειας	3.Γ.1: Εκπόνηση threat landscape reports
	3.Γ.2: Ανάπτυξη και διαχείριση μητρώου υποδομών (hardware), λογισμικού (software) και άυλων πληροφοριακών αγαθών σε κρίσιμους τομείς (δημόσιο, κρίσιμες υποδομές)
	3.Γ.3: Εκπόνηση εθνικής εκτίμησης κινδύνων κυβερνοασφάλειας

3.Γ.1: Εκπόνηση threat landscape reports

Η δράση αποσκοπεί στην εκπόνηση τακτικών αναφορών για το τοπίο απειλών (threat landscape reports) στο πλαίσιο ενός Εθνικού Πλαισίου Εκτίμησης Κινδύνων Κυβερνοασφάλειας.

Οι αναφορές θα βασίζονται στη συστηματική συλλογή και ανάλυση δεδομένων από εθνικές και διεθνείς πηγές, προκειμένου να εντοπίζονται τάσεις, αναδυόμενες απειλές και τρωτά σημεία που επηρεάζουν κρίσιμες υποδομές και οργανισμούς.

Η δράση θα συμβάλει στη βελτίωση της στρατηγικής επίγνωσης και στον έγκαιρο σχεδιασμό μέτρων πρόληψης και απόκρισης, ενισχύοντας την εθνική ικανότητα εκτίμησης και διαχείρισης κινδύνων κυβερνοασφάλειας.

3.Γ.2: Ανάπτυξη και διαχείριση μητρώου υποδομών (hardware), λογισμικού (software) και άυλων πληροφοριακών αγαθών σε κρίσιμους τομείς (δημόσιο, κρίσιμες υποδομές)

Η δράση αποσκοπεί στη δημιουργία και συνεχή ενημέρωση ενός ολοκληρωμένου εθνικού μητρώου υποδομών, λογισμικού και πληροφοριακών αγαθών, με στόχο την ενίσχυση της ανθεκτικότητας κρίσιμων συστημάτων έναντι κυβερνοαπειλών και τη βελτίωση της διαχείρισης κινδύνων.

Σε συνέχεια της υλοποίησης, τα δεδομένα θα αξιοποιηθούν για :

- Καταγραφή και κατηγοριοποίηση πληροφοριακών αγαθών (information assets) και τήρηση σχετικού αποθετηρίου.
- Ελέγχους και αξιολόγηση ασφάλειας για την προστασία λογισμικού, εφαρμογών, δικτύων και υποδομών, μέσω διαδικασιών δοκιμών και τεχνικών ελέγχων.
- Έκδοση κατευθυντήριων γραμμών και οδηγιών για την προστασία των πληροφοριακών αγαθών, καλύπτοντας θέματα όπως κρυπτογράφηση, διαχείριση δεδομένων, αποθήκευση, καταστροφή, απομακρυσμένη πρόσβαση και δικτυακή ασφάλεια.

Η δράση συμβάλλει στη διαμόρφωση μιας ενοποιημένης και τεκμηριωμένης προσέγγισης για την προστασία των εθνικών πληροφοριακών πόρων και τη διασφάλιση της επιχειρησιακής συνέχειας κρίσιμων λειτουργιών.

3.Γ.3: Εκπόνηση εθνικής εκτίμησης κινδύνων κυβερνοασφάλειας

Η δράση αποσκοπεί στην εκπόνηση μιας ολοκληρωμένης Εθνικής Εκτίμησης Κινδύνων Κυβερνοασφάλειας, η οποία θα προσδιορίζει, θα αναλύει και θα αξιολογεί τις κύριες απειλές, τις ευπάθειες και τις δυνητικές επιπτώσεις σε κρίσιμες υποδομές, δημόσιους φορείς, επιχειρήσεις και την κοινωνία. Η εκτίμηση θα αποτελέσει κεντρικό εργαλείο στρατηγικού σχεδιασμού, παρέχοντας μια τεκμηριωμένη εικόνα των εθνικών προτεραιοτήτων, των υφιστάμενων κενών και των απαιτήσεων για τη διαχείριση κινδύνων.

Το έργο θα συμπεριλαμβάνει την ανάλυση σεναρίων, την αξιοποίηση δεδομένων από εθνικούς επιχειρησιακούς μηχανισμούς, καθώς και τη συνεργασία με αρμόδιους φορείς και την ερευνητική κοινότητα. Τα αποτελέσματα της Εθνικής Εκτίμησης Κινδύνων Κυβερνοασφάλειας θα υποστηρίζουν τη διαμόρφωση πολιτικών, την ανάπτυξη μέτρων πρόληψης και απόκρισης, καθώς και την ενημέρωση της εθνικής στρατηγικής κυβερνοασφάλειας, ενισχύοντας τη συνολική κυβερνοανθεκτικότητα της χώρας.

Ειδικός Στόχος 3.Δ: Ενίσχυση της Διακυβέρνησης Κυβερνοασφάλειας

Ο Ειδικός Στόχος 3.Δ επικεντρώνεται στην εδραίωση ενός στιβαρού συστήματος εθνικής διακυβέρνησης της κυβερνοασφάλειας, που συνδυάζει θεσμικές δομές συντονισμού, σαφή κατανομή αρμοδιοτήτων και αποτελεσματικούς μηχανισμούς εποπτείας και συμμόρφωσης. Προβλέπει τη συγκρότηση συντονιστικών οργάνων, την οργάνωση και υποστήριξη των ΥΑΣΠΕ και των δομών κυβερνοασφάλειας καταρχήν στα Υπουργεία, καθώς και την πλήρη αξιοποίηση του κανονιστικού πλαισίου του ν. 5160/2024.

Μέσω της έκδοσης τομεακών πολιτικών και προτύπων, της ανάπτυξης συστημάτων ελέγχων και της θέσπισης πλαισίων εκπαίδευσης και πιστοποίησης για επιθεωρητές, ο στόχος αυτός διασφαλίζει ότι η εθνική πολιτική κυβερνοασφάλειας εφαρμόζεται ενιαία, με συνέπεια και διαφάνεια. Ενισχύει τη λογοδοσία, διευκολύνει τη σύγκλιση με τα ευρωπαϊκά πρότυπα και διαμορφώνει ένα ώριμο περιβάλλον διακυβέρνησης, στο οποίο οι φορείς γνωρίζουν τις υποχρεώσεις τους και υποστηρίζονται για να τις εκπληρώνουν.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
3.Δ: Ενίσχυση της Διακυβέρνησης Κυβερνοασφάλειας	3.Δ.1: Θέσπιση Συντονιστικής Επιτροπής Κυβερνοασφάλειας για τη Δημόσια Διοίκηση
	3.Δ.2: Ανάπτυξη και εφαρμογή ενιαίου συντονιστικού πλαισίου για τους ΥΑΣΠΕ στη Δημόσια Διοίκηση
	3.Δ.3: Διαμόρφωση Πλαισίου Λειτουργίας Οργανικών Μονάδων Κυβερνοασφάλειας Φορέων της Κεντρικής Διοίκησης
	3.Δ.4: Ανάπτυξη και Εφαρμογή της Δευτερογενούς Νομοθεσίας του ν. 5160/2024 (Οδηγία NIS2)
	3.Δ.5: Ανάπτυξη-έκδοση τομεακών πολιτικών και προτύπων κυβερνοασφάλειας
	3.Δ.6: Ανάπτυξη συστήματος ελέγχων (audit) εφαρμογής των απαιτήσεων ασφάλειας
	3.Δ.7: Ανάπτυξη Εγχειριδίου Οργάνωσης Πλαισίου Διακυβέρνησης Κυβερνοασφάλειας για Δημόσιους Φορείς

	3.Δ.8: Δημιουργία Πλαισίου Εκπαίδευσης και Πιστοποίησης Επιθεωρητών Κυβερνοασφάλειας
	3.Δ.9: Ανάπτυξη πλαισίου πολιτικών σχετικών με την ασφάλεια των υποθαλάσσιων καλωδίων επικοινωνιών
	3.Δ.10: Θέσπιση Πλαισίου Ρύθμισης και Πιστοποίησης Παρόχων Κυβερνοασφάλισης (Cyber Insurance)

3.Δ.1: Θέσπιση Συντονιστικής Επιτροπής Κυβερνοασφάλειας για τη Δημόσια Διοίκηση

Η δράση αποσκοπεί στη θεσμοθέτηση και λειτουργία Συντονιστικής Επιτροπής Κυβερνοασφάλειας για τη Δημόσια Διοίκηση, ως μηχανισμού στρατηγικού συντονισμού και παρακολούθησης της εφαρμογής πολιτικών κυβερνοασφάλειας, υπό το συντονισμό και με την υποστήριξη της ΕΑΚ. Η Επιτροπή θα συγκεντρώνει εκπροσώπους διοικήσεων αρμόδιων υπουργείων και φορέων, προωθώντας την ενοποίηση διαδικασιών, την ανταλλαγή πληροφοριών και τη διασφάλιση συνεκτικής προσέγγισης στη διαχείριση κινδύνων κυβερνοασφάλειας στη δημόσια διοίκηση. Η Επιτροπή θα συνεδριάζει τουλάχιστον δύο φορές ετησίως με στόχο την ενίσχυση της συλλογικής δέσμευσης, καθώς και δέσμευσης ανά Υπουργείο, την ανάδειξη των καλών πρακτικών, την παρουσίαση αποτελεσμάτων, ενεργειών και προκλήσεων ανά τομέα ευθύνης.

3.Δ.2: Ανάπτυξη και εφαρμογή ενιαίου συντονιστικού πλαισίου για τους ΥΑΣΠΕ στη Δημόσια Διοίκηση

Η δράση αποσκοπεί στην ανάπτυξη και εφαρμογή ενιαίου συντονιστικού πλαισίου για τους Υπεύθυνους Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ) για τη Δημόσια Διοίκηση, με στόχο την ενίσχυση της συνεργασίας και της συνέπειας στην εφαρμογή πολιτικών κυβερνοασφάλειας σε εθνικό επίπεδο. Το πλαίσιο θα καθορίζει κοινές αρμοδιότητες, πρότυπα λειτουργίας και μηχανισμούς ανταλλαγής πληροφοριών, διευκολύνοντας τον συντονισμό και την ομοιογενή ανταπόκριση όλων των κρίσιμων φορέων σε θέματα ασφάλειας πληροφοριών.

3.Δ.3: Διαμόρφωση Πλαισίου Λειτουργίας Οργανικών Μονάδων Κυβερνοασφάλειας Φορέων της Κεντρικής Διοίκησης

Η δράση αποσκοπεί στη διαμόρφωση θεσμικού και επιχειρησιακού πλαισίου λειτουργίας για τις Δομές Κυβερνοασφάλειας καταρχήν των Υπουργείων, με στόχο την ενίσχυση του έργου των Υπευθύνων Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ) και τη βελτίωση της κυβερνοανθεκτικότητας της Δημόσιας Διοίκησης. Οι οργανικές μονάδες Κυβερνοασφάλειας θα υποστηρίζουν την εφαρμογή πολιτικών ασφάλειας, την υποβολή αναφορών περιστατικών και τη διενέργεια αξιολογήσεων, συμβάλλοντας στη συμμόρφωση με τον ν. 5160/2024 και τη νέα Εθνική Στρατηγική Κυβερνοασφάλειας.

3.Δ.4: Ανάπτυξη και Εφαρμογή της Δευτερογενούς Νομοθεσίας του ν. 5160/2024 (Οδηγία NIS2)

Η δράση αποσκοπεί στην πλήρη εφαρμογή του προγράμματος δευτερογενούς νομοθεσίας που εκπονεί η Εθνική Αρχή Κυβερνοασφάλειας βάσει του ν. 5160/2024. Το πρόγραμμα περιλαμβάνει την έκδοση κανονιστικών πράξεων, τεχνικών προτύπων και οδηγιών εφαρμογής που θα εξειδικεύουν τις υποχρεώσεις των φορέων, τα μέτρα ασφάλειας, τις διαδικασίες αναφοράς περιστατικών και τους μηχανισμούς εποπτείας, διασφαλίζοντας τη συνοχή και την αποτελεσματικότητα του εθνικού πλαισίου κυβερνοασφάλειας.

3.Δ.5: Ανάπτυξη-έκδοση τομεακών πολιτικών και προτύπων κυβερνοασφάλειας

Η δράση στοχεύει στην ανάπτυξη και έκδοση τομεακών πολιτικών και προτύπων κυβερνοασφάλειας, σύμφωνα με το πλαίσιο του ν. 5160/2024 και τις κατευθυντήριες γραμμές της ΕΑΚ. Οι πολιτικές αυτές θα προσαρμόζονται στις ιδιαιτερότητες κάθε κρίσιμου τομέα, καθορίζοντας ελάχιστες απαιτήσεις ασφάλειας, διαδικασίες διαχείρισης κινδύνων και μηχανισμούς εποπτείας, με σκοπό την ενίσχυση της συνέπειας και της ωριμότητας του εθνικού συστήματος κυβερνοασφάλειας.

3.Δ.6: Ανάπτυξη συστήματος ελέγχων (audit) εφαρμογής των απαιτήσεων ασφάλειας

Η δράση αποσκοπεί στην ανάπτυξη ενός ολοκληρωμένου συστήματος ελέγχων (audit) για την παρακολούθηση και αξιολόγηση της συμμόρφωσης των οργανισμών με τις απαιτήσεις ασφάλειας που απορρέουν από τον ν. 5160/2024, λειτουργώντας με πλήρη λειτουργική ανεξαρτησία.

Το σύστημα θα επιτρέπει τον συστηματικό έλεγχο της εφαρμογής των τεχνικών και οργανωτικών μέτρων ασφάλειας, σύμφωνα με το εθνικό κανονιστικό πλαίσιο, και θα υποστηρίζει τη συνεχή βελτίωση της κυβερνοανθεκτικότητας των υπόχρεων οντοτήτων, καθώς και την αποτρεπτική ισχύ του δικαίου κυβερνοασφάλειας και του κυρωτικού πλαισίου.

Ειδικότερα, θα περιλαμβάνει:

- Ενιαία μεθοδολογία και διαδικασίες ελέγχου, εναρμονισμένες με τις απαιτήσεις του ν. 5160/2024, τις σχετικές κανονιστικές πράξεις και εκτελεστικά μέτρα.
- Μηχανισμό τεκμηρίωσης, παρακολούθησης και αναφοράς των αποτελεσμάτων ελέγχου προς την Εθνική Αρχή Κυβερνοασφάλειας.
- Δράσεις συμμόρφωσης και επαναξιολόγησης, που θα διασφαλίζουν τη συνεχή προσαρμογή στις εξελισσόμενες απαιτήσεις του ν. 5160/2024.

Η δράση συμβάλλει στην ενίσχυση της εθνικής διακυβέρνησης κυβερνοασφάλειας, προάγοντας τη διαφάνεια, τη λογοδοσία και τον συντονισμό μεταξύ των βασικών και σημαντικών οντοτήτων και της Εθνικής Αρχής Κυβερνοασφάλειας.

3.Δ.7: Ανάπτυξη Εγχειριδίου Οργάνωσης Πλαισίου Διακυβέρνησης Κυβερνοασφάλειας για Δημόσιους Φορείς

Η δράση αποσκοπεί Ανάπτυξη ενός ολοκληρωμένου εγχειριδίου (governance blueprint) για τους δημόσιους φορείς, το οποίο θα παρέχει πρότυπες κατευθύνσεις για τη διαμόρφωση ενός εσωτερικού στρατηγικού πλαισίου διακυβέρνησης της κυβερνοασφάλειας. Το εγχειρίδιο θα υποστηρίζει τους φορείς στη δημιουργία, προσαρμογή και τεκμηρίωση μηχανισμών διακυβέρνησης σύμφωνα με τις απαιτήσεις του ν. 5160/2024 και των σχετικών ευρωπαϊκών και διεθνών προτύπων.

3.Δ.8: Δημιουργία Πλαισίου Εκπαίδευσης και Πιστοποίησης Επιθεωρητών Κυβερνοασφάλειας

Ανάπτυξη ολοκληρωμένου πλαισίου εκπαίδευσης και πιστοποίησης Επιθεωρητών Κυβερνοασφάλειας, το οποίο θα καθορίζει τις απαιτούμενες γνώσεις, δεξιότητες και ικανότητες, καθώς και τα κριτήρια αξιολόγησης και επαναπιστοποίησης. Το πλαίσιο θα περιλαμβάνει πρότυπο πρόγραμμα εκπαίδευσης, εκπαιδευτικό υλικό, διαδικασίες διενέργειας εξετάσεων και μηχανισμούς διασφάλισης ποιότητας, με στόχο τη δημιουργία αξιόπιστου μητρώου πιστοποιημένων επιθεωρητών και την ενίσχυση της συμμόρφωσης των φορέων με τις εθνικές και ευρωπαϊκές απαιτήσεις κυβερνοασφάλειας.

3.Δ.9: Ανάπτυξη πλαισίου πολιτικών σχετικών με την ασφάλεια των υποθαλάσσιων καλωδίων επικοινωνιών

Η δράση αποσκοπεί στην ανάπτυξη πλαισίου πολιτικών ενίσχυσης της ασφάλειας των υπαρχόντων και νέων υποβρυχίων καλωδίων επικοινωνιών με βάση τις απαιτήσεις του ν. 5160/2024 και τις σχετικές ευρωπαϊκές πρωτοβουλίες, σχετικά με ασφαλείς και ανθεκτικές υποδομές υποβρύχιων καλωδίων. Στόχος της δράσης είναι η υλοποίηση σειράς συντονισμένων δράσεων για την αντιμετώπιση των απειλών και την ενίσχυση της ανθεκτικότητας της υποθαλάσσιας καλωδιακής υποδομής, σε όλα τα στάδια του κύκλου ανθεκτικότητας, από την πρόληψη, την ανίχνευση, την αντιμετώπιση και την αποκατάσταση έως την αποτροπή.

3.Δ10: Θέσπιση Πλαισίου Ρύθμισης και Πιστοποίησης Παρόχων Κυβερνοασφάλισης (Cyber Insurance)

Η δράση στοχεύει στη θέσπιση ενός συνεκτικού και αξιόπιστου πλαισίου ρύθμισης της αγοράς παρόχων κυβερνοασφάλισης (cyber insurance), με σκοπό την ενίσχυση της διαφάνειας, της ποιότητας των υπηρεσιών και της προστασίας των οργανισμών που επιλέγουν ασφαλιστική κάλυψη έναντι κυβερνοαπειλών. Το ρυθμιστικό πλαίσιο θα καθορίζει ελάχιστες απαιτήσεις, κριτήρια συμμόρφωσης και διαδικασίες αξιολόγησης των παρόχων, συμπεριλαμβανομένων ελέγχων αξιοπιστίας, επάρκειας τεχνικών γνώσεων και τήρησης προτύπων ασφάλειας.

Η δράση αποσκοπεί επίσης στη διασφάλιση ότι τα ασφαλιστικά προϊόντα κυβερνοασφάλισης ανταποκρίνονται σε πραγματικές ανάγκες της αγοράς, ενθαρρύνουν την υιοθέτηση βέλτιστων πρακτικών κυβερνοασφάλειας και συμβάλλουν στη μείωση του συστημικού κινδύνου. Μέσω της ρύθμισης της αγοράς, ενισχύεται η εμπιστοσύνη των επιχειρήσεων και οργανισμών προς τους παρόχους, διαμορφώνεται ένα πιο ώριμο και σταθερό οικοσύστημα κυβερνοασφάλισης και υποστηρίζεται η ανάπτυξη προϊόντων που ευθυγραμμίζονται με ευρωπαϊκά και διεθνή πρότυπα διαχείρισης κινδύνων.

Ειδικός Στόχος 3.Ε: Θέσπιση Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας

Ο Ειδικός Στόχος 3.Ε αποσκοπεί στην εφαρμογή εξειδικευμένων πλαισίων διαχείρισης κινδύνων για κρίσιμες τεχνολογίες και τομείς, ώστε η ασφάλεια να ενσωματώνεται συστηματικά στον σχεδιασμό και τη λειτουργία των ψηφιακών υποδομών. Καλύπτει, μεταξύ άλλων, τα δίκτυα 5G, τα συστήματα Τεχνητής Νοημοσύνης, το Internet of Things, τα έργα ΤΠΕ του Δημοσίου και τις υπηρεσίες cloud, προωθώντας αρχές όπως το security by design, το zero trust και την ψηφιακή κυριαρχία.

Σε συνδυασμό με μηχανισμούς ελέγχου συμμόρφωσης και τη ρύθμιση αγορών όπως η κυβερνοασφάλιση, ο στόχος αυτός ενισχύει τη δυνατότητα των οργανισμών να αναγνωρίζουν, να αξιολογούν και να μειώνουν συστηματικά τους κινδύνους. Παράλληλα, στηρίζει την ανάπτυξη ώριμων αγορών υπηρεσιών και προϊόντων ασφάλειας που ευθυγραμμίζονται με τα ευρωπαϊκά και διεθνή πρότυπα και συμβάλλουν στη μείωση του συστημικού κινδύνου για την οικονομία και την κοινωνία.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
3.Ε: Θέσπιση Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας	3.Ε.1: Εφαρμογή ολοκληρωμένου πλαισίου κυβερνοασφάλειας για τα δίκτυα 5G
	3.Ε.2: Εφαρμογή πλαισίου μέτρων και δράσεων για την Τεχνητή Νοημοσύνη & την Κυβερνοασφάλεια
	3.Ε.3: Εφαρμογή πλαισίου μέτρων και δράσεων για το Internet of Things (IoT)
	3.Ε.4: Θέσπιση αρχών ασφαλούς σχεδιασμού για νέα συστήματα ΤΠΕ του Δημόσιου Τομέα
	3.Ε.5: Ανάπτυξη εθνικού πλαισίου ασφαλούς μετάβασης υπηρεσιών στο Υπολογιστικό Νέφος
	3.Ε.6. Διεξαγωγή Ελέγχων ΕΑΚ

3.Ε.1: Εφαρμογή ολοκληρωμένου πλαισίου κυβερνοασφάλειας για τα δίκτυα 5G

Η δράση στοχεύει στην εφαρμογή ολοκληρωμένου πλαισίου κυβερνοασφάλειας για τα δίκτυα 5G, σύμφωνα με τις ευρωπαϊκές κατευθυντήριες γραμμές και την εργαλειοθήκη της ΕΕ για την ασφάλεια των δικτύων 5G (EU 5G Cybersecurity Toolbox). Το πλαίσιο θα περιλαμβάνει μέτρα διαχείρισης κινδύνων, απαιτήσεις ασφάλειας για παρόχους και προμηθευτές, καθώς και μηχανισμούς παρακολούθησης και συμμόρφωσης, διασφαλίζοντας την ανθεκτικότητα και την ασφάλεια των κρίσιμων επικοινωνιακών υποδομών της χώρας.

3.Ε.2: Εφαρμογή πλαισίου μέτρων και δράσεων για την Τεχνητή Νοημοσύνη & την Κυβερνοασφάλεια

Η δράση αποσκοπεί στην ανάπτυξη και εφαρμογή εθνικού πλαισίου μέτρων και δράσεων για την ενσωμάτωση της κυβερνοασφάλειας στα συστήματα Τεχνητής Νοημοσύνης. Το πλαίσιο θα καλύπτει τη διαχείριση κινδύνων, την ασφάλεια δεδομένων και αλγορίθμων, καθώς και την ευθυγράμμιση με τον Ευρωπαϊκό Κανονισμό για την Τεχνητή Νοημοσύνη (AI Act), προωθώντας την ασφαλή και αξιόπιστη χρήση της ΤΝ σε δημόσιο και ιδιωτικό τομέα.

3.Ε.3: Εφαρμογή πλαισίου μέτρων και δράσεων για το Internet of Things (IoT)

Η δράση στοχεύει στην ανάπτυξη και εφαρμογή ολοκληρωμένου πλαισίου μέτρων και δράσεων για την ασφάλεια του Internet of Things (IoT), σύμφωνα με τα ευρωπαϊκά πρότυπα και τον Κανονισμό για

την Κυβερνοανθεκτικότητα (CRA). Το πλαίσιο θα καθορίζει απαιτήσεις ασφάλειας για συσκευές και δίκτυα IoT, διαδικασίες αξιολόγησης συμμόρφωσης και μηχανισμούς παρακολούθησης, ενισχύοντας την προστασία κρίσιμων υποδομών και καταναλωτών.

3.Ε.4: Θέσπιση αρχών ασφαλούς σχεδιασμού για νέα συστήματα ΤΠΕ του Δημόσιου Τομέα

Η δράση αποσκοπεί στην καθιέρωση πρακτικών ασφαλούς σχεδιασμού για όλα τα νέα πληροφοριακά συστήματα, εφαρμογές και ψηφιακές υπηρεσίες του Δημοσίου, με βάση τις αρχές του security by design και zero trust. Οι αρχές αυτές θα διασφαλίζουν την ενσωμάτωση ισχυρών μηχανισμών ταυτοποίησης και πρόσβασης, την κρυπτογράφηση δεδομένων, τον δικτυακό διαχωρισμό και τη συνεχή επαλήθευση ταυτότητας χρηστών και συστημάτων. Παράλληλα, θα εκδοθούν πρότυπες τεχνικές προδιαγραφές ασφάλειας για τα έργα ΤΠΕ του Δημοσίου, επιβεβαιώνοντας ότι η ασφάλεια αποτελεί θεμελιώδες και ενσωματωμένο στοιχείο του ψηφιακού μετασχηματισμού της χώρας.

3.Ε.5: Ανάπτυξη εθνικού πλαισίου ασφαλούς μετάβασης υπηρεσιών στο Υπολογιστικό Νέφος

Η δράση στοχεύει στην ανάπτυξη ενός εθνικού πλαισίου για την ασφαλή και ανθεκτική μετάβαση υπηρεσιών και δεδομένων στο υπολογιστικό νέφος. Το πλαίσιο θα καθορίζει κατευθυντήριες γραμμές για την ταξινόμηση δεδομένων και υπηρεσιών ανάλογα με την κρισιμότητα και την ευαισθησία τους, επιτρέποντας την επιλογή κατάλληλων επιπέδων προστασίας και ασφάλειας. Παράλληλα, θα προωθεί τη χρήση εγχώριων υποδομών νεφοϋπολογιστικής και πιστοποιημένων παρόχων, ενισχύοντας την ψηφιακή κυριαρχία και τη συμμόρφωση με τα εθνικά και ευρωπαϊκά πρότυπα κυβερνοασφάλειας.

Η δράση θα υποστηρίξει την υιοθέτηση αρχών «security by design» και «data sovereignty», καθώς και τη σταδιακή μείωση της εξάρτησης από παρόχους εκτός Ε.Ε. ή άλλων στρατηγικών εταιρών, συμβάλλοντας στη δημιουργία ενός αξιόπιστου και ασφαλούς οικοσυστήματος cloud σε εθνικό επίπεδο.

3.Ε.6. Διεξαγωγή Ελέγχων ΕΑΚ

Διενέργεια στοχευμένων ελέγχων σε φορείς του δημόσιου και ιδιωτικού τομέα, με έμφαση στις Βασικές Οντότητες (Essential Entities) και τις Σημαντικές Οντότητες (Important Entities) όπως ορίζονται στο ν. 5160/2024. Οι έλεγχοι αφορούν την αξιολόγηση της συμμόρφωσης με τις απαιτήσεις κυβερνοασφάλειας, μέσω επιτόπιων και απομακρυσμένων αξιολογήσεων, εξέτασης τεκμηρίωσης, και ανάλυσης των τεχνικών και οργανωτικών μέτρων που έχουν υλοποιηθεί. Η δράση περιλαμβάνει την υλοποίηση ενός προγράμματος περιοδικών αλλά και έκτακτων ελέγχων και επιθεωρήσεων, τη σύνταξη αναφορών ευρημάτων, συστάσεων και απαιτούμενων διορθωτικών ενεργειών, με στόχο την έγκαιρη αναγνώριση κινδύνων, την ενίσχυση της εφαρμογής βέλτιστων πρακτικών και τη συνολική αύξηση της κυβερνοανθεκτικότητας των οντοτήτων.

Ειδικός Στόχος 3.ΣΤ: Ενίσχυση Μηχανισμών Αναφοράς Περιστατικών Κυβερνοασφάλειας

Ο Ειδικός Στόχος 3.ΣΤ στοχεύει στη δημιουργία ενός ενιαίου, αποδοτικού και φιλικού προς τους φορείς συστήματος αναφοράς περιστατικών κυβερνοασφάλειας, το οποίο υποστηρίζει την ανταλλαγή πληροφοριών, τη συντονισμένη απόκριση και την αποτελεσματική εποπτεία. Προβλέπει την ανάπτυξη κεντρικού μηχανισμού κοινοποίησης περιστατικών και την εγκαθίδρυση εθνικής γραμμής υποστήριξης

(Cyber Hotline), που λειτουργεί ως σημείο άμεσης καθοδήγησης και επιχειρησιακής διασύνδεσης με τους αρμόδιους μηχανισμούς.

Με τη μείωση των διοικητικών βαρών, την ενοποίηση των ροών πληροφόρησης και την ενίσχυση της διαφάνειας, ο στόχος αυτός συμβάλλει στη συστηματική καταγραφή, ανάλυση και αξιοποίηση των περιστατικών ως πηγή μάθησης και βελτίωσης. Ενδυναμώνει την εμπιστοσύνη των φορέων προς την Εθνική Αρχή Κυβερνοασφάλειας, διευκολύνει τη συμμόρφωση με τις κανονιστικές υποχρεώσεις και ενισχύει την επιχειρησιακή ικανότητα της χώρας να ανταποκρίνεται σε απειλές και κρίσεις στον κυβερνοχώρο.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
3.ΣΤ: Ενίσχυση Μηχανισμών Αναφοράς Περιστατικών Κυβερνοασφάλειας	3.ΣΤ.1: Κεντρικός Μηχανισμός Συντονισμένης Αναφοράς Περιστατικών Κυβερνοασφάλειας
	3.ΣΤ.2: Δημιουργία Cyber hotline

3.ΣΤ.1: Κεντρικός Μηχανισμός Συντονισμένης Αναφοράς Περιστατικών Κυβερνοασφάλειας

Η δράση στοχεύει στην ανάπτυξη ενιαίας πλατφόρμας συντονισμένης κοινοποίησης περιστατικών κυβερνοασφάλειας, στο πλαίσιο του Κεντρικού Μηχανισμού Αναφοράς, η οποία θα επιτρέπει την ολοκληρωμένη και αποδοτική αναφορά περιστατικών προς τις αρμόδιες αρχές. Η πλατφόρμα θα ευθυγραμμίζεται με τις απαιτήσεις του ισχύοντος και υπό αναθεώρηση νομοθετικού πλαισίου (NIS2, GDPR, DORA, eIDAS, CER) και θα υποστηρίζει τη λειτουργία του ενιαίου σημείου εισόδου (SEP) που ανατίθεται στον ENISA. Μέσω του μηχανισμού αυτού θα μειωθούν τα διοικητικά βάρη για τους φορείς, θα ενισχυθεί η αποτελεσματικότητα της διαχείρισης περιστατικών και θα προαχθεί η διαφάνεια. Επιπλέον, θα διευκολύνει τη συνεργασία μεταξύ αρχών και τη συνεκτική ανταπόκριση σε περιστατικά που εμπίπτουν σε διαφορετικά ρυθμιστικά πλαίσια.

3.ΣΤ.2: Δημιουργία Cyber hotline

Η δράση αφορά τη δημιουργία εθνικής γραμμής υποστήριξης κυβερνοασφάλειας (Cyber Hotline), η οποία θα λειτουργεί ως ενιαίο σημείο επικοινωνίας για παροχή άμεσης καθοδήγησης και τεχνικής συμβουλευτικής στο δίκτυο των SOCs, σε οργανισμούς και φορείς. Η Cyber Hotline εντάσσεται στη λειτουργία του Ενοποιημένου Κέντρου Αναφοράς Κυβερνοασφάλειας, όπως προβλέπεται στο άρθρο 31 του ν. 5002/2022, και υποστηρίζει επιχειρησιακά το EL-SOC.

Στρατηγικός Στόχος 4: Ενίσχυση κανονιστικής συμμόρφωσης και αναβάθμιση πολιτικών και μέτρων κυβερνοασφάλειας

Ο Στρατηγικός Στόχος 4 αποσκοπεί στη δημιουργία ενός σύγχρονου, συνεκτικού και αποτελεσματικού κανονιστικού πλαισίου κυβερνοασφάλειας, το οποίο διασφαλίζει ότι οι δημόσιοι και ιδιωτικοί φορείς εφαρμόζουν ουσιαστικά μέτρα προστασίας, πλήρως ευθυγραμμισμένα με το ενωσιακό δίκαιο και τις διεθνείς βέλτιστες πρακτικές. Εστιάζει στην ενίσχυση της συμμόρφωσης με το ν. 5160/2024 και συναφείς ευρωπαϊκές ρυθμίσεις, καθώς και στην αναβάθμιση των πολιτικών, προτύπων και μηχανισμών εποπτείας, με τρόπο αναλογικό, βασισμένο στον κίνδυνο και προσαρμοσμένο στις ιδιαιτερότητες των κρίσιμων τομέων.

Μέσω της ενσωμάτωσης αρχών ασφαλούς σχεδιασμού, της προστασίας των θεμελιωδών δικαιωμάτων, της ενίσχυσης της ανθεκτικότητας κρίσιμων υποδομών, της καθιέρωσης μηχανισμών υπεύθυνης γνωστοποίησης ευπαθειών και της ρύθμισης κρίσιμων αγορών και υπηρεσιών, ο στόχος αυτός λειτουργεί ως «ραχοκοκαλιά» του συστήματος διακυβέρνησης της κυβερνοασφάλειας. Συνδέει την πολιτική, τη ρύθμιση και την εποπτεία με την επιχειρησιακή πραγματικότητα, συμβάλλοντας στη σταδιακή σύγκλιση της χώρας με τα πιο ώριμα ευρωπαϊκά οικοσυστήματα κυβερνοασφάλειας.

Ειδικός Στόχος 4.Α: Διασφάλιση της Ισορροπίας μεταξύ Κυβερνοασφάλειας και Προστασίας της Ιδιωτικότητας

Ο Ειδικός Στόχος 4.Α στοχεύει στη θεσμική κατοχύρωση μιας ισορροπημένης προσέγγισης, όπου η ενίσχυση της κυβερνοασφάλειας συμβαδίζει με την αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα και των θεμελιωδών δικαιωμάτων. Προωθεί τη συστηματική ενσωμάτωση των αρχών «Privacy & Security by Design» στον σχεδιασμό και τον κύκλο ζωής ψηφιακών υπηρεσιών και υποδομών, διασφαλίζοντας ότι οι απαιτήσεις ασφάλειας και ιδιωτικότητας λαμβάνονται υπόψη εξ αρχής και όχι εκ των υστέρων.

Μέσω της ανάπτυξης εθνικού πλαισίου και κοινών προγραμμάτων επιμόρφωσης για DPOs και CISOs, ο στόχος αυτός ενισχύει τη συνεργασία μεταξύ της Εθνικής Αρχής Κυβερνοασφάλειας και της Αρχής Προστασίας Δεδομένων, καλλιεργώντας κοινή γλώσσα και κουλτούρα συμμόρφωσης. Κατ' αυτόν τον τρόπο, η χώρα υιοθετεί ένα πρότυπο διακυβέρνησης όπου η ασφάλεια και η ιδιωτικότητα αντιμετωπίζονται ως συμπληρωματικές διαστάσεις της εμπιστοσύνης στον ψηφιακό χώρο.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
4.Α: Διασφάλιση της Ισορροπίας μεταξύ Κυβερνοασφάλειας και Προστασίας της Ιδιωτικότητας	4.Α.1: Διαμόρφωση Εθνικού Πλαισίου για "Privacy & Security by Design"
	4.Α.2: Ανάπτυξη κοινού προγράμματος για DPO και CISOs: "Cybersecurity & Privacy Compliance"

4.Α.1: Διαμόρφωση Εθνικού Πλαισίου για "Privacy & Security by Design"

Η δράση αποσκοπεί στη διαμόρφωση Εθνικού Πλαισίου για την εφαρμογή των αρχών "Privacy & Security by Design", με στόχο τη συστηματική ενσωμάτωση της προστασίας της ιδιωτικότητας και της ασφάλειας ήδη από το στάδιο του σχεδιασμού ψηφιακών υπηρεσιών, πληροφοριακών συστημάτων και υποδομών.

Το πλαίσιο θα:

- Καθορίζει ενιαίες αρχές και προδιαγραφές για τη συνεκτίμηση των απαιτήσεων κυβερνοασφάλειας και προστασίας δεδομένων προσωπικού χαρακτήρα σε όλα τα στάδια του κύκλου ζωής των συστημάτων (σχεδιασμός, ανάπτυξη, λειτουργία, συντήρηση).
- Ευθυγραμμίζεται με το κανονιστικό πλαίσιο της Οδηγίας NIS2, του ν. 5160/2024 και του Κανονισμού (ΕΕ) 2016/679 (GDPR), εξασφαλίζοντας την ισορροπία μεταξύ ασφάλειας και ιδιωτικότητας.
- Παρέχει κατευθυντήριες οδηγίες και τεχνικά πρότυπα για φορείς του δημόσιου και ιδιωτικού τομέα, ώστε να ενσωματώνουν μεθοδικά μηχανισμούς ασφάλειας και προστασίας δεδομένων στις ψηφιακές τους λύσεις.
- Ενισχύει τη συνεργασία μεταξύ της Εθνικής Αρχής Κυβερνοασφάλειας και της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, προωθώντας κοινές πολιτικές και βέλτιστες πρακτικές.

4.Α.2: Ανάπτυξη κοινού προγράμματος για DPO και CISOs: "Cybersecurity & Privacy Compliance"

Η δράση στοχεύει στην ανάπτυξη κοινού προγράμματος επιμόρφωσης για Υπευθύνους Προστασίας Δεδομένων (DPOs) και Υπεύθυνους Ασφάλειας Πληροφοριών (CISOs) με αντικείμενο τη συμμόρφωση στον τομέα της κυβερνοασφάλειας και της προστασίας της ιδιωτικότητας.

Το πρόγραμμα θα:

- Ενισχύσει τη συνεργασία μεταξύ DPOs και CISOs, καλλιεργώντας κοινή κατανόηση των νομικών, τεχνικών και οργανωτικών απαιτήσεων που απορρέουν από τον ν. 5160/2024 (ενσωμάτωση της Οδηγίας NIS2) και τον Κανονισμό (ΕΕ) 2016/679 (GDPR).
- Εστιάσει σε θέματα "Cybersecurity & Privacy Compliance", όπως η διαχείριση κινδύνων, η προστασία δεδομένων εξ ορισμού και εξ αρχής (Privacy by Design), η ανταπόκριση σε περιστατικά ασφάλειας και η τεκμηρίωση συμμόρφωσης.
- Παρέχει εξειδικευμένα σεμινάρια και πρακτικές ασκήσεις, προσαρμοσμένα στις ανάγκες των επαγγελματιών που δραστηριοποιούνται στη διακυβέρνηση ασφάλειας και προστασίας δεδομένων.
- Προάγει τη διατομεακή συνεργασία μεταξύ φορέων του δημόσιου και ιδιωτικού τομέα, ενισχύοντας την ανταλλαγή γνώσεων και βέλτιστων πρακτικών.

Ειδικός Στόχος 4.Β: Ενίσχυση της Κυβερνοασφάλειας της Εφοδιαστικής Αλυσίδας

Ο Ειδικός Στόχος 4.Β αποσκοπεί στη θωράκιση της εφοδιαστικής αλυσίδας ΤΠΕ, αναγνωρίζοντας ότι οι κίνδυνοι κυβερνοασφάλειας δεν περιορίζονται στα όρια ενός οργανισμού αλλά επεκτείνονται στους προμηθευτές, συνεργάτες και παρόχους υπηρεσιών. Εστιάζει στην ανάπτυξη πλαισίου ασφαλών

προμηθειών και στη συστηματική ενσωμάτωση της διαχείρισης κινδύνων τρίτων μερών τόσο στη Δημόσια Διοίκηση όσο και στον ιδιωτικό τομέα.

Με την υιοθέτηση προτύπων, διαδικασιών αξιολόγησης προμηθευτών και μηχανισμών ελέγχου συμμόρφωσης, ο στόχος αυτός ενισχύει την ανθεκτικότητα των κρίσιμων πληροφοριακών υποδομών απέναντι σε απειλές που πηγάζουν από την εφοδιαστική αλυσίδα. Παράλληλα, προωθεί την ευθυγράμμιση με διεθνή και ευρωπαϊκά πρότυπα, συμβάλλοντας στη δημιουργία ενός πιο ασφαλούς και αξιόπιστου οικοσυστήματος προμηθειών ΤΠΕ.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
4.Β: Ενίσχυση της Κυβερνοασφάλειας της Εφοδιαστικής Αλυσίδας	4.Β.1: Διαμόρφωση πλαισίου ασφαλών προμηθειών ΤΠΕ και ασφάλεια εφοδιαστικής αλυσίδας

4.Β.1: Διαμόρφωση πλαισίου ασφαλών προμηθειών ΤΠΕ και ασφάλεια εφοδιαστικής αλυσίδας

Η δράση αποσκοπεί στη διαμόρφωση ολοκληρωμένου πλαισίου για τις ασφαλείς προμήθειες ΤΠΕ και την ενίσχυση της ασφάλειας της εφοδιαστικής αλυσίδας τόσο στη Δημόσια Διοίκηση όσο και στον ιδιωτικό τομέα. Το πλαίσιο θα περιλαμβάνει μηχανισμούς αξιολόγησης και διαχείρισης κινδύνων από προμηθευτές, καθορισμό προτύπων και πολιτικών ασφαλών προμηθειών, καθώς και εκπαιδευτικές δράσεις για την ενίσχυση των σχετικών ικανοτήτων των φορέων. Μέσω της δράσης θα προαχθεί η συμμόρφωση με διεθνή πρότυπα κυβερνοασφάλειας και θα ενισχυθεί η ανθεκτικότητα των πληροφοριακών υποδομών απέναντι σε κινδύνους που προέρχονται από την εφοδιαστική αλυσίδα.

Ειδικός Στόχος 4.Γ: Προστασία και Ενίσχυση της Ανθεκτικότητας των Κρίσιμων Τομέων

Ο Ειδικός Στόχος 4.Γ εστιάζει στην ενίσχυση της προστασίας και της ανθεκτικότητας των κρίσιμων τομέων και υποδομών, σύμφωνα με το ισχύον εθνικό και ενωσιακό πλαίσιο (συμπεριλαμβανομένης της Οδηγίας CER). Προβλέπει την ορθή και δυναμική αναγνώριση των κρίσιμων οντοτήτων, καθώς και την ανάπτυξη εξειδικευμένων προτύπων και οδηγιών ασφάλειας για βιομηχανικά συστήματα, ICS/SCADA και IIoT, όπου οι κυβερνοαπειλές συνδέονται άμεσα με τη φυσική ασφάλεια και τη συνέχεια ζωτικών λειτουργιών.

Μέσω της υιοθέτησης τεχνικών και οργανωτικών μέτρων προσαρμοσμένων στα περιβάλλοντα ΟΤ, της προώθησης προγραμμάτων αναβάθμισης ασφάλειας και της ενίσχυσης της διατομεακής συνεργασίας, ο στόχος αυτός συμβάλλει στη διασφάλιση της συνεχούς παροχής βασικών υπηρεσιών προς την κοινωνία και την οικονομία. Ταυτόχρονα, ενισχύει την ικανότητα της χώρας να ανταποκρίνεται σε σύνθετους κινδύνους που συνδυάζουν φυσικές και ψηφιακές διαστάσεις.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
4.Γ: Προστασία και Ενίσχυση της Ανθεκτικότητας των Κρίσιμων Τομέων	4.Γ.1: Καθορισμός και επικαιροποίηση καταλόγου κρίσιμων υποδομών
	4.Γ.2: Εκπόνηση ειδικών οδηγιών και προτύπων ασφαλείας για ICS/SCADA/IIoT
	4.Γ.3 Εκπόνηση τομεακής στρατηγικής και πλάνου δράσης για την κυβερνο-ανθεκτικότητα στον τομέα της Πολιτικής Αεροπορίας
	4.Γ.4 Ενίσχυση της Κυβερνοασφάλειας και της Ανθεκτικότητας των Μητρώων Ονομάτων Χώρου .gr και .ελ

4.Γ.1 Καθορισμός και επικαιροποίηση καταλόγου κρίσιμων υποδομών

Η δράση αποσκοπεί στον καθορισμό και την τακτική επικαιροποίηση του εθνικού καταλόγου κρίσιμων υποδομών, σύμφωνα με τις απαιτήσεις του ισχύοντος κανονιστικού πλαισίου και της Οδηγίας CER. Στόχος είναι η ορθή αναγνώριση των κρίσιμων τομέων και οντοτήτων, η ενίσχυση της προστασίας τους από κυβερνοαπειλές και φυσικούς κινδύνους, καθώς και η διασφάλιση της συνέχειας βασικών λειτουργιών του κράτους και της κοινωνίας, λαμβάνοντας στοχευμένες δράσεις για τις κρίσιμες οντότητες.

4.Γ.2 Εκπόνηση ειδικών οδηγιών και προτύπων ασφαλείας για ICS/SCADA/IIoT

Η δράση αποσκοπεί στην εκπόνηση ειδικών οδηγιών και προτύπων ασφάλειας για τα βιομηχανικά και αυτοματοποιημένα συστήματα ελέγχου (ICS), τα συστήματα SCADA και το Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT), με στόχο την ενίσχυση της κυβερνοανθεκτικότητας κρίσιμων υποδομών και υπηρεσιών. Οι οδηγίες θα βασιστούν σε διεθνή πρότυπα και βέλτιστες πρακτικές και θα καλύπτουν τεχνικά, οργανωτικά και λειτουργικά μέτρα προστασίας. Παράλληλα, η δράση περιλαμβάνει την προώθηση προγραμμάτων αναβάθμισης ασφάλειας, όπως εγκατάσταση συστημάτων ανίχνευσης και αποτροπής εισβολών (IDS/IPS), εφαρμογή δικτυακού διαχωρισμού σε περιβάλλοντα OT, ενισχύοντας τη φυσική και ψηφιακή ασφάλεια κρίσιμων τομέων.

4.Γ.3 Εκπόνηση τομεακής στρατηγικής και πλάνου δράσης για την κυβερνο-ανθεκτικότητα στον τομέα της Πολιτικής Αεροπορίας

Ο τομέας της πολιτικής αεροπορίας χαρακτηρίζεται από νέες κανονιστικές απαιτήσεις και προκλήσεις όσον αφορά την ασφάλεια πληροφοριών. Με την εν λόγω εμβληματική δραστηριότητα συστηματοποιείται ένα ολοκληρωμένο πλαίσιο παρεμβάσεων για την προστασία, ανίχνευση, απόκριση και ανάκαμψη από περιστατικά ασφαλείας, σε ευθυγράμμιση τόσο με τις οριζόντιες (NIS 2, ν. 5160/2024, ΚΥΑ ΕΠΑΚ), όσο και με τις τομεακές απαιτήσεις (EASA Part-IS, AVSEC R). Αποσκοπείται η εν λόγω στρατηγική να αποτελέσει πρότυπο για αντίστοιχες - τομεακές- στρατηγικές.

4.Γ.4 Ενίσχυση της Κυβερνοασφάλειας και της Ανθεκτικότητας των Μητρώων Ονομάτων Χώρου .gr και .ελ

Η δράση περιλαμβάνει την ανάπτυξη και εφαρμογή ενός ολοκληρωμένου πλαισίου κυβερνοασφάλειας, επιχειρησιακής ετοιμότητας και εποπτείας για τα μητρώα .gr και .ελ, με τις ακόλουθες βασικές συνιστώσες: 1. Θέσπιση Ελάχιστων Υποχρεωτικών Απαιτήσεων Κυβερνοασφάλειας, 2. Μηχανισμός Συνεχούς Παρακολούθησης και Αναφοράς Περιστατικών, 3. Τακτικές Ασκήσεις και Έλεγχοι Ανθεκτικότητας, 4. Πλαίσιο Διακυβέρνησης και Συνεργασίας σε εθνικό και διεθνές επίπεδο.

Ειδικός Στόχος 4.Δ: Θέσπιση Εθνικής Πολιτικής Συντονισμένης Γνωστοποίησης Ευπαθειών (CVD Policy)

Ο Ειδικός Στόχος 4.Δ αποσκοπεί στη θεσμοθέτηση μιας ώριμης, ασφαλούς και διαφανούς προσέγγισης για τη διαχείριση ευπαθειών, μέσω ενός εθνικού μηχανισμού συντονισμένης γνωστοποίησης ευπαθειών (CVD) και ενός πλαισίου κινήτρων για υπεύθυνη αποκάλυψη (Bug Bounty GR). Αναγνωρίζει τον κρίσιμο ρόλο της κοινότητας ερευνητών ασφάλειας στην έγκαιρη αναγνώριση και αντιμετώπιση αδυναμιών, και επιδιώκει να μετατρέψει αυτή τη σχέση σε θεσμική συνεργασία.

Μέσα από τυποποιημένες διαδικασίες αξιολόγησης, ενημέρωσης και αποκατάστασης ευπαθειών, καθώς και τη θέσπιση κατάλληλων κινήτρων και νομικής προστασίας, ο στόχος αυτός ενισχύει τη διαφάνεια και την εμπιστοσύνη στο εθνικό οικοσύστημα κυβερνοασφάλειας. Παράλληλα, συμβάλλει στη σημαντική μείωση του χρόνου από την ανακάλυψη έως την αντιμετώπιση κρίσιμων ευπαθειών, αυξάνοντας την ανθεκτικότητα των ψηφιακών συστημάτων σε εθνικό επίπεδο.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
4.Δ: Θέσπιση Εθνικής Πολιτικής Συντονισμένης Γνωστοποίησης Ευπαθειών (CVD Policy)	4.Δ.1 Ανάπτυξη εθνικού μηχανισμού συντονισμένης γνωστοποίησης και διαχείρισης ευπαθειών
	4.Δ.2. Ανάπτυξη Εθνικού Πλαισίου Κινήτρων για Υπεύθυνη Γνωστοποίηση Ευπαθειών (Bug Bounty GR)

4.Δ.1 Ανάπτυξη εθνικού μηχανισμού συντονισμένης γνωστοποίησης και διαχείρισης ευπαθειών

Η δράση στοχεύει στη δημιουργία ενός εθνικού μηχανισμού συντονισμένης γνωστοποίησης και διαχείρισης ευπαθειών (Coordinated Vulnerability Disclosure – CVD), που θα επιτρέπει την υπεύθυνη και ασφαλή αναφορά ευπαθειών από ερευνητές, οργανισμούς και ιδιώτες. Ο μηχανισμός θα λειτουργεί βάσει καθορισμένων διαδικασιών αξιολόγησης, κοινοποίησης και αποκατάστασης ευπαθειών, ενισχύοντας τη διαφάνεια, την εμπιστοσύνη και τη συνεργασία μεταξύ όλων των εμπλεκομένων μερών του εθνικού οικοσυστήματος κυβερνοασφάλειας. Παράλληλα, θα συμβάλει στην έγκαιρη αντιμετώπιση κινδύνων και στην αύξηση της συνολικής ανθεκτικότητας ψηφιακών συστημάτων και υπηρεσιών σε εθνικό επίπεδο.

4.Δ.2. Ανάπτυξη Εθνικού Πλαισίου Κινήτρων για Υπεύθυνη Γνωστοποίηση Ευπαθειών (Bug Bounty GR)

Η δράση αποσκοπεί στη δημιουργία και λειτουργία ενός ελεγχόμενου και θεσμικά κατοχυρωμένου Εθνικού Πλαισίου Κινήτρων για την Υπεύθυνη Γνωστοποίηση Ευπαθειών (Bug Bounty GR). Το πλαίσιο θα καθορίζει τους βασικούς κανόνες, τις προϋποθέσεις συμμετοχής και τις διαδικασίες ασφαλούς συνεργασίας μεταξύ της ΕΑΚ, των φορέων της δημόσιας διοίκησης και της κοινότητας των ερευνητών ασφάλειας (security researchers).

Στόχος της δράσης είναι η ενθάρρυνση της υπεύθυνης αποκάλυψης ευπαθειών από εξειδικευμένους ερευνητές, ακαδημαϊκούς και Subject Matter Experts, μέσα από ένα διαφανές, αξιόπιστο και ρυθμισμένο περιβάλλον, το οποίο παρέχει σαφείς κανόνες “safe-harbour”, κατάλληλα κίνητρα και εγγυήσεις νομικής προστασίας.

Ειδικός Στόχος 4.Ε: Προώθηση της Ενεργητικής Προστασίας στον Κυβερνοχώρο

Ο Ειδικός Στόχος 4.Ε επικεντρώνεται στην ανάπτυξη ενός ώριμου, αξιόπιστου και ρυθμισμένου οικοσυστήματος υπηρεσιών κυβερνοασφάλειας και πιστοποίησης, που υποστηρίζει την ενεργητική προστασία στον κυβερνοχώρο. Προβλέπει τη θέσπιση πλαισίου για Μητρώο Ενδεδειγμένων Παρόχων Υπηρεσιών Κυβερνοασφάλειας, την αναβάθμιση και επιχειρησιακή λειτουργία της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας, καθώς και την ευθυγράμμιση με το πλαίσιο του Κανονισμού (ΕΕ) 2019/881 (Cybersecurity Act).

Μέσω της καθιέρωσης σαφών απαιτήσεων ποιότητας, κριτηρίων πιστοποίησης και μηχανισμών διαπίστευσης, ο στόχος αυτός ενισχύει την εμπιστοσύνη στην αγορά λύσεων και υπηρεσιών κυβερνοασφάλειας και προάγει την υιοθέτηση πιστοποιημένων προϊόντων και υπηρεσιών από δημόσιους και ιδιωτικούς φορείς. Κατ’ αυτόν τον τρόπο, η ενεργητική προστασία στον κυβερνοχώρο αναβαθμίζεται από αποσπασματικό τεχνικό μέτρο σε δομικό στοιχείο της εθνικής πολιτικής, που ευθυγραμμίζεται με τα ευρωπαϊκά σχήματα πιστοποίησης και ενισχύει τη συλλογική κυβερνοανθεκτικότητα της χώρας.

Ειδικός Στόχος	Εμβληματικές Δραστηριότητες
4.Ε: Προώθηση της Ενεργητικής Προστασίας στον Κυβερνοχώρο)	4.Ε.1 Ανάπτυξη πλαισίου απαιτήσεων για δημιουργία μητρώου ενδεδειγμένων παρόχων Υπηρεσιών Κυβερνοασφάλειας
	4.Ε.2 Αναβάθμιση και επιχειρησιακή λειτουργία της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας
	4.Ε.3 Καθορισμός θεσμικού πλαισίου πιστοποιήσεων σε ευθυγράμμιση με το πλαίσιο του Κανονισμού (ΕΕ) 2019/881 (Cybersecurity Act)

	4.Ε.4 Ενίσχυση της Ικανότητας Κυβερνοαποτροπής στον Τομέα της Εθνικής Άμυνας

4.Ε.1 Ανάπτυξη πλαισίου απαιτήσεων για δημιουργία μητρώου ενδεδειγμένων παρόχων Υπηρεσιών Κυβερνοασφάλειας

Η δράση στοχεύει στην ανάπτυξη πλαισίου απαιτήσεων και κριτηρίων για τη δημιουργία Μητρώου Ενδεδειγμένων Παρόχων Υπηρεσιών Κυβερνοασφάλειας. Το πλαίσιο θα καθορίζει πρότυπα ποιότητας, τεχνικές προδιαγραφές και όρους πιστοποίησης, διασφαλίζοντας την αξιοπιστία και την επάρκεια των παρεχόμενων υπηρεσιών προς δημόσιους και ιδιωτικούς φορείς.

4.Ε.2 Αναβάθμιση και επιχειρησιακή λειτουργία της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας

Η δράση στοχεύει στον καθορισμό της οργανωτικής δομής, των συνεργειών καθώς και του κατάλληλου πλαισίου στελέχωσης της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας, που θα της επιτρέψει να ανταποκριθεί αποτελεσματικά στον σύνθετο ρόλο της, με απώτερο στόχο την λειτουργία της βάσει συγκεκριμένων προτύπων, πλαισίου πιστοποιήσεων και διαπίστευσης.

4.Ε.3 Καθορισμός θεσμικού πλαισίου πιστοποιήσεων σε ευθυγράμμιση με το πλαίσιο του Κανονισμού (ΕΕ) 2019/881 (Cybersecurity Act)

Η δράση αποσκοπεί στην καταγραφή και ανάπτυξη των απαιτήσεων σε όρους θεσμικού πλαισίου, λαμβάνοντας υπόψη τις πρακτικές άλλων κρατών μελών, ώστε να διασφαλιστεί η συμμόρφωση με το Ενωσιακό θεσμικό πλαίσιο πιστοποίησης της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών.

4.Ε.4 Ενίσχυση της Ικανότητας Κυβερνοαποτροπής στον Τομέα της Εθνικής Άμυνας

Η δράση αφορά την υποστήριξη της ανάπτυξης και ωρίμανσης ολοκληρωμένων ικανοτήτων Κυβερνοάμυνας, με έμφαση στην πρόληψη, την ετοιμότητα και την ενεργητική αποτροπή σύνθετων και εξελισσόμενων κυβερνοαπειλών στον τομέα της εθνικής άμυνας.

Παράρτημα: Σχέδιο Δράσης ΕΣΚ 2026 – 2030

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
1. Ανάπτυξη Ικανοτήτων & Ευαισθητοποίηση	1.Α Ενίσχυση της Κυβερνοανθεκτικότητας και της Κυβερνο-Υγιεινής του Ιδιωτικού Τομέα και των Μικρομεσαίων Επιχειρήσεων	1.Α.1 Διενέργεια μελέτης για την αναγνώριση των συγκεκριμένων αναγκών κυβερνοασφάλειας των ΜΜΕ, εκτός πεδίου εφαρμογής της Οδηγίας NIS2	-ΕΑΚ -ΥΠΑΝ/ΓΓ Βιομηχανίας & ΓΓ Εμπορίου -ΑΕΙ	Κ.1.Α.1 : % προτάσεων της μελέτης που ενσωματώνονται σε πολιτικές ή προγράμματα της ΕΑΚ και συναρμόδιων φορέων.	Μεσοπρόθεσμο (2028–2029)
		1.Α.2 Προαγωγή της εφαρμογής Ευρωπαϊκών & Διεθνών Προτύπων Κυβερνοασφάλειας από οντότητες.	-ΕΑΚ -ΥΨΗΔ -NSFPs	Κ.1.Α.2 : % οντοτήτων που εφαρμόζουν αναγνωρισμένα ευρωπαϊκά και διεθνή πρότυπα κυβερνοασφάλειας	Μακροπρόθεσμο (2030)
		1.Α.3 Εργαλειοθήκη Κυβερνοετοιμότητας για Μικρομεσαίες Επιχειρήσεις και Αυτοαπασχολούμενους	-ΕΑΚ -ΑΕΙ -ΥΠΑΝ	Κ.1.Α.3 : % ΜμΕ και αυτοαπασχολούμενων που αξιοποιούν την Εργαλειοθήκη Κυβερνοετοιμότητας.	Μεσοπρόθεσμο (2028–2029)
	1.Β Γεφύρωση του Ελλείματος Δεξιοτήτων στην Κυβερνοασφάλεια	1.Β.1 Ανάπτυξη πλατφόρμας “cyber range” για την εκπαίδευση των διαχειριστών (ασφάλειας, δικτύων, συστημάτων, εφαρμογών, βάσεων δεδομένων, κλπ.) της Αρχής και των Φορέων	-ΕΑΚ -ΑΕΙ	Κ.1.Β.1 : Πλήθος στελεχών (ΕΑΚ & Οντότητες) που εκπαιδεύονται ετησίως μέσω του cyber range.	Μακροπρόθεσμο (2030)
		1.Β.2 Εκπόνηση Εθνικού Σχεδίου Δράσης για την Εκπαίδευση και την Ευαισθητοποίηση στην Κυβερνοασφάλεια	-ΕΑΚ -ΥΠΑΙΘΑ -ΑΕΙ -ΕΛ.ΑΣ	Κ.1.Β.2 : % βαθμίδων εκπαίδευσης στις οποίες ενσωματώνεται εγκεκριμένο εκπαιδευτικό περιεχόμενο κυβερνοασφάλειας.	Μεσοπρόθεσμο (2028–2029)

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
1. Ανάπτυξη Ικανοτήτων & Ευαισθητοποίηση	1.Β Γεφύρωση του Ελλείματος Δεξιοτήτων στην Κυβερνοασφάλεια	1.Β.3 Υλοποίηση ολοκληρωμένου προγράμματος εκπαίδευσης κυβερνοασφάλειας σε στελέχη της ΔΔ	-ΕΑΚ -ΥΠΕΣ -ΕΚΔΔΑ	Κ.1.Β.3 : % στελεχών της Δημόσιας Διοίκησης που ολοκληρώνουν επιτυχώς εγκεκριμένη εκπαίδευση κυβερνοασφάλειας	Βραχυπρόθεσμο (2026–2027)
		1.Β.4 Στοχευμένα προγράμματα ενημέρωσης για ανώτατες διοικήσεις δημόσιου και ιδιωτικού τομέα	-ΕΑΚ -ΥΠΕΣ -ΥΠΑΝ -ΑΕΙ	Κ.1.Β.4 : % οργανισμών που εκπροσωπούνται από ανώτατα διοικητικά στελέχη στα προγράμματα ενημέρωσης.	Μεσοπρόθεσμο (2028–2029)
		1.Β.5 Υλοποίηση ειδικών προγραμμάτων επανειδίκευσης (reskilling) και αναβάθμισης δεξιοτήτων (upskilling) για ΥΑΣΠΕ για το δημόσιο τομέα	-ΕΑΚ -ΥΠΕΣ -ΕΚΔΔΑ	Κ.1.Β.5 : Πλήθος ΥΑΣΠΕ που ολοκληρώνουν ετήσια προγράμματα reskilling/upskilling	Μακροπρόθεσμο (2030)
	1.Γ Προώθηση των Επενδύσεων και της Καινοτομίας	1.Γ.1 Ενίσχυση του ρόλου και των λειτουργιών του Εθνικού Κέντρου Συντονισμού (NCC-EL ScaleUP)	-ΕΑΚ -ΚτΠ ΜΑΕ -ΥΨΗΔ -ΑΕΙ	Κ.1.Γ.1 : Επέκταση λειτουργιών, συνεργασιών και υπηρεσιών του NCC-EL	Βραχυπρόθεσμο (2026–2027)
		1.Γ.1 Συνέχιση ενισχυμένης συνεργασίας με ακαδημαϊκούς και ερευνητικούς φορείς σε θέματα κυβερνοασφάλειας	-ΕΑΚ -ΑΕΙ -ΕΔΥΤΕ ΑΕ -ΕΥΠ	Κ.1.Γ.1 : Πλήθος ακαδημαϊκών και ερευνητικών φορέων που συμμετέχουν σε επίσημες συνεργασίες με την ΕΑΚ	Διαρκής Δράση
		1.Γ.3 Σχεδιασμός οικονομικών κινήτρων για επένδυση σε υπηρεσίες και εργαλεία κυβερνοασφάλειας	-ΕΑΚ -ΥΨΗΔ -ΥΠΟΙΚ -ΤΥΠΑΝ -ΥΠΑΝ/ΓΓ Έρευνας και Καινοτομίας	Κ.1.Γ.3 : Πλήθος επιχειρήσεων που κάνουν χρήση των οικονομικών κινήτρων για επενδύσεις σε εργαλεία και υπηρεσίες κυβερνοασφάλειας.	Μεσοπρόθεσμο (2028–2029)
		1.Γ.4 Δημιουργία Εθνικού Μητρώου Ελλήνων Ερευνητών και Εμπειρογνωμόνων Κυβερνοασφάλειας	-ΕΑΚ -ΥΠΑΝ/ΓΓ Έρευνας και Καινοτομίας -ΑΕΙ -NSFPs	Κ.1.Γ.4 : Πλήθος εγγεγραμμένων Ελλήνων ερευνητών κυβερνοασφάλειας στο εθνικό μητρώο	Βραχυπρόθεσμο (2026–2027)

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
1. Ανάπτυξη Ικανοτήτων & Ευαισθητοποίηση	1.Γ Προώθηση των Επενδύσεων και της Καινοτομίας	1.Γ.5 Δημιουργία Παρατηρητηρίου Επενδύσεων στην Κυβερνοασφάλεια	-ΕΑΚ -NSFPs -ΑΕΙ	Κ.1.Γ.5 : % φορέων που υποβάλλουν συστηματικά δεδομένα επενδύσεων κυβερνοασφάλειας στο Παρατηρητήριο.	Βραχυπρόθεσμο (2026–2027)
		1.Γ.6 Δημιουργία Εθνικού Αποθεματικού Κυβερνοασφάλειας με σκοπό τη χρηματοδοτική υποστήριξη έργων και πρωτοβουλιών που ενισχύουν την κυβερνοανθεκτικότητα δημόσιων και ιδιωτικών οντοτήτων	-ΕΑΚ -ΥΨΗΔ -ΥΠΟΙΚ	Κ.1.Γ.6 : % ολοκλήρωσης της θεσμικής σύστασης και επιχειρησιακής λειτουργίας του Εθνικού Αποθεματικού Κυβερνοασφάλειας.	Μακροπρόθεσμο (2030)
	1.Δ Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας	1.Δ.1 Εθνικό Σχέδιο Επικοινωνίας και Ευαισθητοποίησης σε Θέματα Κυβερνοασφάλειας	-ΕΑΚ -ΥΨΗΔ -ΓΓ Επικοινωνίας & Ενημέρωσης -ΑΕΙ	Κ.1.Δ.1 : % πληθυσμού που έχει παρακολουθήσει δράσεις ευαισθητοποίησης κυβερνοασφάλειας σε εθνικό επίπεδο.	Βραχυπρόθεσμο (2026–2027)
		1.Δ.2 Ανάπτυξη ολοκληρωμένου προγράμματος διενέργειας ασκήσεων με έμφαση στην αντιμετώπιση περιστατικών και κρίσεων στο πεδίο εφαρμογής της Οδηγίας NIS2 και της CER	-ΕΑΚ -CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ -Εθνικό CERT -Υπουργείο Προστασίας του Πολίτη - Γ.Γ.Π.Κ.Ο. -NSFPs -Γενική Γραμματεία Εθνικής Ασφάλειας	Κ.1.Δ.2 : Πλήθος εθνικών και διατομεακών ασκήσεων κυβερνοασφάλειας που υλοποιούνται ετησίως. Μετρά τον αριθμό των ολοκληρωμένων ασκήσεων, ταξινομημένων ανά τύπο	Μεσοπρόθεσμο (2028–2029)
		1.Δ.3 Κατάρτιση ενημερωτικού και εκπαιδευτικού υλικού (γενικό και ανά κατηγορία Φορέα)	-ΕΑΚ -ENISA -ΑΠΔΠΧ -ΕΛ.ΑΣ -ΕΥΠ -NSFPs -ΑΕΙ	Κ.1.Δ.3 : % τομέων για τους οποίους έχει παραχθεί εξειδικευμένο υλικό.	Βραχυπρόθεσμο (2026–2027)
		1.Δ.4 Διαμόρφωση πλαισίου επικοινωνιακής διαχείρισης περιστατικών	-ΕΑΚ -ΥΨΗΔ -Εθνικό CERT -ΓΓ Επικοινωνίας & Ενημέρωσης	Κ.1.Δ.4 : % κρίσιμων φορέων που έχουν εσωτερικά επικαιροποιήσει και ευθυγραμμίσει τα σχέδια επικοινωνίας τους σύμφωνα με το εθνικό πλαίσιο.	Μακροπρόθεσμο (2030)

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
1. Ανάπτυξη Ικανοτήτων & Ευαισθητοποίηση	1.Δ Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας	1.Δ.5 Διενέργεια Δράσεων ευαισθητοποίησης σε α'βάθμια και β΄ βάθμια εκπαίδευση	-ΕΑΚ -ΥΠΑΙΘΑ -ΕΛ.ΑΣ -ΑΕΙ	Κ.1.Δ.5 : Πλήθος σχολικών μονάδων πρωτοβάθμιας και δευτεροβάθμιας που λαμβάνουν μέρος σε δράσεις ευαισθητοποίησης ετησίως.	Συνεχής Δράση
	1.Δ Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας	1.Δ.6 Βελτιστοποίηση της λειτουργίας του gSOC και των mini-SOC	-Εθνικό CERT -ΕΑΚ	Κ.1.Δ.6 : % φορέων της Κεντρικής Κυβέρνησης που παρακολουθούνται επιχειρησιακά από το gSOC ή/και mini-SOC βάσει ενιαίου πλαισίου.	Βραχυπρόθεσμο (2026–2027)
	1.Δ Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας	1.Δ.7 Εργαστήριο Αναλύσεων Δοκιμών και Μελετών Κυβερνοασφάλειας (LAB)	-ΕΑΚ -Εθνικό CERT -ΓΕΕΘΑ/ΔΙΚΥΒ -ΕΛ.ΑΣ	Κ.1.Δ.7 : Πλήθος τεχνικών αναλύσεων, δοκιμών και μελετών που εκπονεί το LAB για την υποστήριξη της ΕΑΚ	Μεσοπρόθεσμο (2028–2029)
	1.Δ Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας	1.Δ.8 Λειτουργία Ενοποιημένου Κέντρου Αναφοράς Κυβερνοασφάλειας (EL-SOC)	-ΕΑΚ	Κ.1.Δ.8 : % υπόχρεων φορέων που χρησιμοποιούν το EL-SOC ως βασικό σημείο αναφοράς και συντονισμού περιστατικών.	Μεσοπρόθεσμο (2028–2029)
	1.Δ Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας	1.Δ.9 Λειτουργία Ομάδας Απόκρισης Περιστατικών Κυβερνοασφάλειας (CSIRT)	-ΕΑΚ -Εθνικό CERT -ΓΕΕΘΑ/ΔΙΚΥΒ	Κ.1.Δ.9 : Επίπεδο επιχειρησιακής ωριμότητας της CSIRT της ΕΑΚ βάσει αναγνωρισμένου CSIRT maturity model.	Διαρκής Δράση
	1.Δ Ενίσχυση της Ετοιμότητας και της Απόκρισης σε Περιστατικά Κυβερνοασφάλειας	1.Δ.10 Διεξαγωγή Ελέγχων Τρωτότητας και Ανάλυσης Ευπαθειών	-ΕΑΚ -ΕΥΠ	Κ.1.Δ.10: % φορέων/συστημάτων υψηλής κρισιμότητας που υποβάλλονται σε ελέγχους τρωτότητας και ανάλυση ευπαθειών.	Διαρκής Δράση

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
2. Ενίσχυση της Εθνικής, Ευρωπαϊκής και Διεθνούς Συνεργασίας	2.Α Ενίσχυση των Μηχανισμών Πρόληψης και Αντιμετώπισης του Κυβερνοεγκλήματος	2.Α.1 Αξιοποίηση σύγχρονων εργαλείων, τεχνικών και μηχανισμών συνεργασίας για την πάταξη του κυβερνοεγκλήματος	-ΕΛ.ΑΣ -ΕΑΚ	Κ.2.Α.1 : Μείωση του μέσου χρόνου διερεύνησης και αύξηση του ποσοστού επιτυχούς τεκμηρίωσης υποθέσεων κυβερνοεγκλήματος.	Βραχυπρόθεσμο (2026–2027)
		2.Α.2 Ανάπτυξη και υλοποίηση προγραμμάτων εκπαίδευσης για στελέχη επιβολής του νόμου (όπως αστυνομικούς, εισαγγελείς και δικαστές) σε θέματα που αφορούν το κυβερνοέγκλημα	-Υπουργείο Δικαιοσύνης -ΕΛ.ΑΣ -ΕΑΚ	Κ.2.Α.2 : % στελεχών επιβολής του νόμου που έχουν παρακολουθήσει πιστοποιημένη εκπαίδευση σε θέματα κυβερνοεγκλήματος.	Μεσοπρόθεσμο (2028–2029)
		2.Α.3 Επικαιροποίηση πολιτικής αντιμετώπισης του Λυτρισμικού (Ransomware) για το γενικό πληθυσμό	-ΕΑΚ -ΕΛ.ΑΣ	Κ.2.Α.3 : % ενημερωμένων πολιτών και οργανισμών σχετικά με πρακτικές πρόληψης λυτρισμικού (ransomware)	Βραχυπρόθεσμο (2026–2027)
		2.Α.4 Ανάπτυξη Σχεδίου Δράσης για την Αντιμετώπιση Επιθέσεων μέσω Deepfakes	-ΥΨΗΔ -ΕΑΚ -ΕΛ.ΑΣ	Κ.2.Α.4 : Έκδοση και εφαρμογή Σχεδίου Δράσης για την αντιμετώπιση κακόβουλων deepfakes	Βραχυπρόθεσμο (2026–2027)
	2.Β Ενίσχυση της Ευρωπαϊκής και Διεθνούς Συνεργασίας	2.Β.1 Θέσπιση Στρατηγικής για τη Διεθνή Συνεργασία σε Θέματα Κυβερνοασφάλειας	-ΕΑΚ -ΥΠΕΞ -ΓΕΕΘΑ -Εθνικό CERT	Κ.2.Β.1 : % βασικών ευρωπαϊκών και διεθνών φόρουμ κυβερνοασφάλειας στα οποία η Ελλάδα συμμετέχει ενεργά	Βραχυπρόθεσμο (2026–2027)
		2.Β.2 Ενίσχυση της Εξωστρέφειας και της Διεθνούς Παρουσίας της ΕΑΚ	-ΕΑΚ	Κ.2.Β.2 : Πλήθος διεθνών συνεδρίων, φόρουμ και συναντήσεων υψηλού επιπέδου με ενεργή συμμετοχή της ΕΑΚ.	Διαρκής Δράση
		2.Β.3 Ενίσχυση Ευρωπαϊκών και Διεθνών Συνεργασιών Πολιτικής Κυβερνοασφάλειας	-ΕΑΚ	Κ.2.Β.3 : Πλήθος ευρωπαϊκών και διεθνών θεσμικών οργάνων, ομάδων εργασίας και δικτύων πολιτικής κυβερνοασφάλειας στα οποία συμμετέχει ενεργά η ΕΑΚ.	Διαρκής Δράση

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
2. Ενίσχυση της Εθνικής, Ευρωπαϊκής και Διεθνούς Συνεργασίας	2.Γ Θέσπιση Αξιόπιστων Μηχανισμών Ανταλλαγής Πληροφοριών	2.Γ.1 Πλατφόρμα διαμοιρασμού πληροφοριών περί απειλών (threat intelligence)	-ΕΑΚ -Εθνικό CERT -Λοιπά CSIRTs	Κ.2.Γ.1 : % φορέων που συμμετέχουν στον εθνικό CTI Hub.	Μεσοπρόθεσμο (2028–2029)
		2.Δ.1 Ενίσχυση Κυβερνοανθεκτικότητας ΟΤΑ	-ΕΑΚ -ΥΨΗΔ -Εθνικό CERT -ΥΠΕΣ	Κ.2.Δ.1 : % ΟΤΑ που επιτυγχάνουν βασικό επίπεδο κυβερνοωριμότητας	Μακροπρόθεσμο (2030)
3. Ένα σύστημα διακυβέρνησης της κυβερνοασφάλειας για το σύνολο της κοινωνίας	3.Α Ανάπτυξη Πλαισίων Διαχείρισης Κρίσεων Κυβερνοασφάλειας	3.Α.1 Ενίσχυση επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφές	-ΕΑΚ -ΥΠΡΟΠΟ-ΙΤ Προστασίας Κρίσιμων Οντοτήτων -Εθνικό CERT -CSIRTs -NSFPs	Κ.3.Α.1 : % οργανισμών κρίσιμων υπηρεσιών που διαθέτουν εγκεκριμένα και επικαιροποιημένα BCP και DRP.	Μεσοπρόθεσμο (2028–2029)
		3.Α.2 Εθνικός σχεδιασμός διαχείρισης κρίσεων	-ΕΑΚ -Εθνικό CERT -ΕΛ.ΑΣ -Λοιπά CSIRTs -ΥΠΡΟΠΟ-ΙΤ Προστασίας Κρίσιμων Οντοτήτων	Κ.3.Α.2 : % ολοκλήρωσης και επίσημης έγκρισης του Εθνικού Σχεδίου Διαχείρισης Κυβερνοκρίσεων	Βραχυπρόθεσμο (2026–2027)
	3.Β Ασφαλής Ψηφιακή Ταυτότητα και Εμπιστοσύνη στις Δημόσιες Ψηφιακές Υπηρεσίες	3.Β.1 Αναβάθμιση προστασίας κυβερνητικών ιστοτόπων	-ΕΑΚ -ΥΨΗΔ -ΥΠΕΣ	Κ.3.Β.1 : % κυβερνητικών ιστοτόπων που προστατεύονται από Web Application Firewall και υπηρεσίες προστασίας DDoS.	Διαρκής Δράση
	3.Γ Θέσπιση Εθνικού Πλαισίου Εκτίμησης Κινδύνων Κυβερνοασφάλειας	3.Γ.1 Εκπόνηση threat landscape reports	-ΕΑΚ -Εθνικό CERT -CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ	Κ.3.Γ.1 : % προγραμματισμένων threat landscape reports που εκδίδονται εντός του προβλεπόμενου χρονοδιαγράμματος.	Συνεχής Δράση
		3.Γ.2 Ανάπτυξη και διαχείριση μητρώου υποδομών (hardware), λογισμικού (software) και άυλων πληροφοριακών αγαθών σε κρίσιμους τομείς (δημόσιο, κρίσιμες υποδομές)	-ΕΑΚ -NSFPs	Κ.3.Γ.2 : % κρίσιμων φορέων που έχουν καταγράψει πλήρως τα πληροφοριακά τους αγαθά στο εθνικό μητρώο.	Βραχυπρόθεσμο (2026–2027)

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
3. Ένα σύστημα διακυβέρνησης της κυβερνοασφάλειας για το σύνολο της κοινωνίας	3.Γ Θέσπιση Εθνικού Πλαισίου Εκτίμησης Κινδύνων Κυβερνοασφάλειας	3.Γ.3 Εκπόνηση εθνικής εκτίμησης κινδύνων κυβερνοασφάλειας	-ΕΑΚ	Κ.3.Γ.3 : % ολοκλήρωσης και επίσημης έγκρισης της Εθνικής Εκτίμησης Κινδύνων Κυβερνοασφάλειας.	Βραχυπρόθεσμο (2026–2027)
	3.Δ Ενίσχυση της Διακυβέρνησης Κυβερνοασφάλειας	3.Δ.1 Θέσπιση Συντονιστικής Επιτροπής Κυβερνοασφάλειας για τη Δημόσια Διοίκηση	-ΕΑΚ -Εθνικό CERT -ΥΨΗΔ -ΥΠΕΣ	Κ.3.Δ.1 : Πλήθος επίσημων συνεδριάσεων της επιτροπής ετησίως	Μακροπρόθεσμο (2030)
		3.Δ.2 Ανάπτυξη και εφαρμογή ενιαίου συντονιστικού πλαισίου για τους ΥΑΣΠΕ για τη Δημόσια Διοίκηση	-ΕΑΚ -Εθνικό CERT -ΥΨΗΔ -ΥΠΕΣ -NSFPs	Κ.3.Δ.2 : % υπουργείων και εποπτευόμενων φορέων που εφαρμόζουν το ενιαίο πλαίσιο ΥΑΣΠΕ	Βραχυπρόθεσμο (2026–2027)
		3.Δ.3 Διαμόρφωση Πλαισίου Λειτουργίας Οργανικών Μονάδων Κυβερνοασφάλειας Φορέων της Κεντρικής Διοίκησης	-ΕΑΚ -Εθνικό CERT -ΥΠΕΣ -ΥΨΗΔ	Κ.3.Δ.3 : % φορέων της Κεντρικής Διοίκησης που έχουν ιδρύσει, στελεχώσει και λειτουργούν ενεργά δομή κυβερνοασφάλειας	Μακροπρόθεσμο (2030)
		3.Δ.4 Ανάπτυξη και Εφαρμογή της Δευτερογενούς Νομοθεσίας του Ν. 5160/2024 (Οδηγία NIS2)	-ΕΑΚ -ΥΨΗΔ -NSFPs	Κ.3.Δ.4 : % κανονιστικών πράξεων, τεχνικών προτύπων και οδηγιών εφαρμογής που έχουν εκδοθεί έναντι του συνολικού νομοθετικού προγράμματος.	Βραχυπρόθεσμο (2026–2027)
		3.Δ.5 Ανάπτυξη-έκδοση τομεακών πολιτικών και προτύπων κυβερνοασφάλειας	-ΕΑΚ -ΥΨΗΔ -NSFPs -Τομεακά Αρμόδια Υπουργεία	Κ.3.Δ.5 : Έκδοση τομεακών πολιτικών και προτύπων κυβερνοασφάλειας	Μεσοπρόθεσμο (2028–2029)
	3.Δ Ενίσχυση της Διακυβέρνησης Κυβερνοασφάλειας	3.Δ.6 Ανάπτυξη συστήματος ελέγχων (audit) εφαρμογής των απαιτήσεων ασφάλειας	-ΕΑΚ -ΥΨΗΔ	Κ.3.Δ.6 : % βασικών και σημαντικών οντοτήτων που υποβάλλονται σε έλεγχο συμμόρφωσης βάσει του εθνικού συστήματος audit.	Βραχυπρόθεσμο (2026–2027)

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
3. Ένα σύστημα διακυβέρνησης της κυβερνοασφάλειας για το σύνολο της κοινωνίας	3.Δ Ενίσχυση της Διακυβέρνησης Κυβερνοασφάλειας	3.Δ.7 Ανάπτυξη Εγχειριδίου Οργάνωσης Πλαισίου Διακυβέρνησης Κυβερνοασφάλειας για Δημόσιους Φορείς	-ΕΑΚ -Εθνικό CERT -ΥΠΕΣ -ΑΕΙ	Κ.3.Δ.7 : % δημόσιων φορέων που έχουν προσαρμόσει και τεκμηριώσει εσωτερικό πλαίσιο διακυβέρνησης κυβερνοασφάλειας βάσει του Εγχειριδίου.	Μεσοπρόθεσμο (2028–2029)
		3.Δ.8 Δημιουργία Πλαισίου Εκπαίδευσης και Πιστοποίησης Επιθεωρητών Κυβερνοασφάλειας	-ΕΑΚ	Κ.3.Δ.8 : Πλήθος ενεργών πιστοποιημένων Επιθεωρητών Κυβερνοασφάλειας εγγεγραμμένων στο επίσημο μητρώο.	Βραχυπρόθεσμο (2026–2027)
		3.Δ.9 Ανάπτυξη πλαισίου πολιτικών σχετικών με την ασφάλεια των υποθαλάσσιων καλωδίων επικοινωνιών	-ΕΑΚ -ΥΨΗΔ-ΙΤ Τηλεπικοινωνιών	Κ.3.Δ.9 : % υποθαλάσσιων καλωδιακών έργων (υφιστάμενων και νέων) που ευθυγραμμίζονται με το εθνικό πλαίσιο πολιτικών ασφάλειας.	Μεσοπρόθεσμο (2028–2029)
	3.Δ. Θέσπιση Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας	3.Δ.10 Θέσπιση Πλαισίου Ρύθμισης και Πιστοποίησης Παρόχων Κυβερνοασφάλισης (Cyber Insurance)	-ΕΑΚ -ΥΠΑΝ	Κ.3.Δ.10: % ολοκλήρωσης και επίσημης θέσπισης του εθνικού πλαισίου ρύθμισης και πιστοποίησης παρόχων κυβερνοασφάλισης.	Μακροπρόθεσμο (2030)
		3.Ε.1 Εφαρμογή ολοκληρωμένου πλαισίου κυβερνοασφάλειας για τα δίκτυα 5G	-ΑΔΑΕ -ΕΑΚ -ΥΠΕΞ -ΕΕΤΤ -ΕΥΠ -ΥΨΗΔ	Κ.3.Ε.1 : % μέτρων του EU 5G Toolbox που ενσωματώνονται στο εθνικό πλαίσιο	Διαρκής Δράση
		3.Ε.2 Εφαρμογή πλαισίου μέτρων και δράσεων για την Τεχνητή Νοημοσύνη & την Κυβερνοασφάλεια	-ΥΨΗΔ (ΕΓ Τεχνητής Νοημοσύνης) -ΕΑΚ -ΑΠΔΠΧ	Κ.3.Ε.2 : % ενοτήτων του εθνικού πλαισίου που συμμορφώνονται με τις απαιτήσεις του AI Act και λοιπές απαιτήσεις ΕΕ για AI security.	Βραχυπρόθεσμο (2026–2027)
		3.Ε.3 Εφαρμογή πλαισίου μέτρων και δράσεων για το Internet of Things (IoT)	-ΕΑΚ -ΥΨΗΔ	Κ.3.Ε.3 : Πλήθος σοβαρών περιστατικών κυβερνοασφάλειας που σχετίζονται με IoT συσκευές και δίκτυα	Μεσοπρόθεσμο (2028–2029)

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
3. Ένα σύστημα διακυβέρνησης της κυβερνοασφάλειας για το σύνολο της κοινωνίας	3.Ε Θέσπιση Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας	3.Ε.4 Θέσπιση αρχών ασφαλούς σχεδιασμού για νέα συστήματα ΤΠΕ του Δημόσιου Τομέα	-ΕΑΚ -ΥΨΗΔ -ΥΠΕΣ -ΑΕΙ	Κ.3.Ε.4 : % νέων έργων ΤΠΕ που τεκμηριώνουν ότι ενσωματώνουν τις αρχές ασφαλούς σχεδιασμού από τη φάση προδιαγραφών.	Μεσοπρόθεσμο (2028–2029)
	3.Ε Θέσπιση Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας	3.Ε.5 Ανάπτυξη εθνικού πλαισίου ασφαλούς μετάβασης υπηρεσιών στο Υπολογιστικό Νέφος	-ΥΨΗΔ -ΕΑΚ -ΥΠΕΣ	Κ.3.Ε.5 : % φορέων που εφαρμόζουν υποχρεωτική ταξινόμηση δεδομένων και υπηρεσιών πριν από τη μετάβαση στο cloud.	Μεσοπρόθεσμο (2028–2029)
	3.Ε Θέσπιση Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας	3.Ε.6 Διεξαγωγή Ελέγχων	-ΕΑΚ -NSFPs	Κ.3.Ε.6 : % Βασικών και Σημαντικών Οντοτήτων που υποβάλλονται σε ελέγχους κυβερνοασφάλειας εντός του ετήσιου εποπτικού κύκλου.	Βραχυπρόθεσμο (2026–2027)
	3.ΣΤ Ενίσχυση Μηχανισμών Αναφοράς Περιστατικών Κυβερνοασφάλειας	3.ΣΤ.1 Κεντρικός Μηχανισμός Συντονισμένης Αναφοράς Περιστατικών Κυβερνοασφάλειας	-ΕΑΚ -ΑΠΔΠΧ -ΑΔΑΕ -CSIRTs	Κ.3.ΣΤ.1: % υπόχρεων φορέων που πραγματοποιούν αναφορές αποκλειστικά μέσω του κεντρικού μηχανισμού.	Μακροπρόθεσμο (2030)
	3.ΣΤ Ενίσχυση Μηχανισμών Αναφοράς Περιστατικών Κυβερνοασφάλειας	3.ΣΤ.2 Δημιουργία Cyber hotline	-ΕΑΚ	Κ.3.ΣΤ.2: % SOCs και φορέων που αξιοποιούν ενεργά την Cyber Hotline για υποστήριξη σε περιστατικά κυβερνοασφάλειας.	Μεσοπρόθεσμο (2028–2029)
4. Ενίσχυση κανονιστικής συμμόρφωσης και αναβάθμιση πολιτικών και μέτρων κυβερνοασφάλειας	4.Α Διασφάλιση της Ισορροπίας μεταξύ Κυβερνοασφάλειας και Προστασίας της Ιδιωτικότητας	4.Α.1 Ανάπτυξη κοινού προγράμματος για DPO και CISOs: "Cybersecurity & Privacy Compliance"	-ΕΑΚ -ΑΠΔΠΧ -ΙΝΕΠ ΕΚΔΔΑ -ΑΕΙ	Κ.4.Α.1 : % DPOs και CISOs που έχουν ολοκληρώσει πιστοποιημένη κοινή εκπαίδευση.	Μακροπρόθεσμο (2030)
	4.Α Διασφάλιση της ισορροπίας μεταξύ Κυβερνοασφάλειας και Προστασίας της Ιδιωτικότητας	4.Α.2 Διαμόρφωση Εθνικού Πλαισίου για "Privacy & Security by Design"	-ΕΑΚ -ΑΠΔΠΧ -ΥΨΗΔ	Κ.4.Α.2 : % νέων ψηφιακών έργων/συστημάτων που εφαρμόζουν τεκμηριωμένα τις αρχές Privacy & Security by Design.	Μεσοπρόθεσμο (2028–2029)

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
4. Ενίσχυση κανονιστικής συμμόρφωσης και αναβάθμιση πολιτικών και μέτρων κυβερνοασφάλειας	4.Β Ενίσχυση της Κυβερνοασφάλειας της Εφοδιαστικής Αλυσίδας	4.Β.1 Διαμόρφωση πλαισίου ασφαλών προμηθειών ΤΠΕ και ασφάλεια εφοδιαστικής αλυσίδας	-ΕΑΚ -ΥΨΗΔ -ΥΠΕΣ -ΥΠΑΝ -ΕΑΑΔΗΣΥ	Κ.4.Β.1 : Πλήθος σοβαρών περιστατικών κυβερνοασφάλειας που σχετίζονται με αδυναμίες της εφοδιαστικής αλυσίδας ΤΠΕ.	Μεσοπρόθεσμο (2028–2029)
	4.Γ Προστασία και Ενίσχυση της Ανθεκτικότητας των Κρίσιμων Τομέων	4.Γ.1 Καθορισμός και επικαιροποίηση καταλόγου κρίσιμων υποδομών	-Υπουργείο Προστασίας του Πολίτη - Γ.Γ.Π.Κ.Ο. -ΕΑΚ -ΥΨΗΔ -NSFPs -ΕΥΠ	Κ.4.Γ.1 : % κρίσιμων οντοτήτων του καταλόγου που καλύπτονται από στοχευμένα μέτρα προστασίας και ανθεκτικότητας	Μεσοπρόθεσμο (2028–2029)
		4.Γ.2 Εκπόνηση ειδικών οδηγιών και προτύπων ασφαλείας για ICS/SCADA/IIoT	-ΕΑΚ -ΥΠΑΝ (ΓΓ Βιομηχανίας) -Υπουργείο Προστασίας του Πολίτη - Γ.Γ.Π.Κ.Ο. -NSFPs	Κ.4.Γ.2 : % βασικών οντοτήτων που εφαρμόζουν τα εθνικά πρότυπα ICS/SCADA/IIoT.	Μεσοπρόθεσμο (2028–2029)
		4.Γ.3 Εκπόνηση τομεακής στρατηγικής και πλάνου δράσης για την κυβερνο-ανθεκτικότητα στον τομέα της Πολιτικής Αεροπορίας	-ΑΠΑ -ΕΑΚ	Κ.4.Γ.3 : % ολοκλήρωσης και θεσμικής έγκρισης της τομεακής στρατηγικής και του πλάνου δράσης κυβερνοανθεκτικότητας Πολιτικής Αεροπορίας.	Βραχυπρόθεσμο (2026–2027)
		4.Γ.4 Ενίσχυση της Κυβερνοασφάλειας και της Ανθεκτικότητας των Μητρώων Ονομάτων Χώρου .gr και .ελ	-ΕΕΤΤ -ΕΑΚ -ΙΤΕ	Κ.4.Γ.4 : % περιστατικών ασφάλειας των μητρώων .gr και .ελ που ανιχνεύονται και αναφέρονται έγκαιρα μέσω του μηχανισμού συνεχούς παρακολούθησης.	Μεσοπρόθεσμο (2028–2029)
	4.Δ Θέσπιση Εθνικής Πολιτικής Συντονισμένης Γνωστοποίησης Ευπαθειών (CVD Policy)	4.Δ.1 Ανάπτυξη εθνικού μηχανισμού συντονισμένης γνωστοποίησης και διαχείρισης ευπαθειών	-ΕΑΚ -Εθνικό CERT -Λοιπά CSIRTs	Κ.4.Δ.1 : % ευπαθειών που αξιολογούνται και οδηγούνται σε αποκατάσταση.	Μεσοπρόθεσμο (2028–2029)
		4.Δ.2 Ανάπτυξη Εθνικού Πλαισίου Κινήτρων για Υπεύθυνη Γνωστοποίηση Ευπαθειών (Bug Bounty GR)	-ΕΑΚ	Κ.4.Δ.2 : % δημόσιων φορέων που συμμετέχουν ενεργά στο πλαίσιο Bug Bounty GR.	Μακροπρόθεσμο (2030)

ΣΤΡΑΤΗΓΙΚΟΣ ΣΤΟΧΟΣ	ΕΙΔΙΚΟΣ ΣΤΟΧΟΣ	ΕΜΒΛΗΜΑΤΙΚΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑ	ΒΑΣΙΚΟΙ ΕΜΠΛΕΚΟΜΕΝΟΙ ΦΟΡΕΙΣ	ΒΑΣΙΚΟΣ ΚΡΙ	ΟΡΟΣΗΜΟ
4. Ενίσχυση κανονιστικής συμμόρφωσης και αναβάθμιση πολιτικών και μέτρων κυβερνοασφάλειας	4.Ε Προώθηση της Ενεργητικής Προστασίας στον Κυβερνοχώρο	4.Ε.1 Ανάπτυξη πλαισίου απαιτήσεων για δημιουργία Μητρώου Ενδεδειγμένων Παρόχων Υπηρεσιών Κυβερνοασφάλειας	-ΕΑΚ -Εθνικό CERT -NSFPs	Κ.4.Ε.1 : % φορέων που χρησιμοποιούν το Μητρώο για επιλογή παρόχων υπηρεσιών κυβερνοασφάλειας.	Βραχυπρόθεσμο (2026–2027)
		4.Ε.2 Αναβάθμιση και επιχειρησιακή λειτουργία της Εθνικής Αρχής Πιστοποίησης Κυβερνοασφάλειας	-ΕΑΚ -ΕΣΥΔ	Κ.4.Ε.2 : Πλήθος σχημάτων πιστοποίησης κυβερνοασφάλειας που υποστηρίζονται επιχειρησιακά από την Αρχή.	Μεσοπρόθεσμο (2028–2029)
		4.Ε.3 Καθορισμός θεσμικού πλαισίου πιστοποιήσεων σε ευθυγράμμιση με το πλαίσιο του Κανονισμού (ΕΕ) 2019/881 (Cybersecurity Act)		Κ.4.Ε.3 : % ολοκλήρωσης και επίσημης θέσπισης του εθνικού θεσμικού πλαισίου πιστοποιήσεων σε ευθυγράμμιση με τον Κανονισμό (ΕΕ) 2019/881.	Μεσοπρόθεσμο (2028–2029)
		4.Ε.4 Ενίσχυση της Ικανότητας Κυβερνοαποτροπής στον Τομέα της Εθνικής Άμυνας	-CSIRT ΓΕΕΘΑ/ΔΙΚΥΒ	Κ.4.Ε.4 : Θέσπιση και Εφαρμογή Επιχειρησιακού Σχεδίου	Μεσοπρόθεσμο (2028–2029)